(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2020 년 2 월 20 일 (20.02.2020)

WIPO | PCT

(10) 국제공개번호
WO 2020/036401 A1

(51) 국제특허분류:
H04W 48/02 (2009.01) *H04W 8/20* (2009.01)
H04W 48/18 (2009.01) *H04W 60/00* (2009.01)

(21) 국제출원번호: PCT/KR2019/010265

(22) 국제출원일: 2019 년 8 월 13 일 (13.08.2019)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2018-0094572 2018 년 8 월 13 일 (13.08.2018) KR
10-2018-0113871 2018 년 9 월 21 일 (21.09.2018) KR

(71) 출원인: 삼성전자 주식회사 (**SAMSUNG ELECTRONICS CO., LTD.**) [KR/KR]; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

(72) 발명자: **백영교 (BAEK, Youngkyo)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **문상준 (MOON, Sangjun)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **박중신 (PARK, Jungshin)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR). **이지철 (LEE, Jicheol)**; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

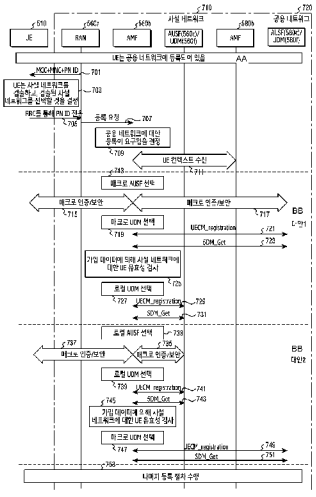
(74) 대리인: **권혁록 등 (KWON, Hyuk-Rok** et al.); 03175 서울시 종로구 경희궁길 28, 2층, Seoul (KR).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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,

(54) **Title:** APPARATUS AND METHOD FOR REGISTRATION ON NETWORK IN WIRELESS COMMUNICATION SYSTEM

(54) **발명의 명칭:** 무선 통신 시스템에서 네트워크에 등록하기 위한 장치 및 방법



703 ... UE detects private network and determines to select detected private network
705 ... Transmit PN ID through RRC
707 ... Registration request
709 ... Determine that registration on public network is required
710 ... Private network
711 ... Receive UE context
713 ... Select macro AUSF
715, 717, 735, 737 ... Macro authentication/security
719, 747 ... Select macro UDM
720 ... Public network
721, 729, 741, 749 ... UECM_registration
723, 743 ... SDM_Get
725, 745 ... Test for validity of UE for private network according to subscription data
727, 739 ... Select local UDM
731, 751 ... SDM_Get
733 ... Select local AUSF
753 ... Perform remaining registration procedures
AA ... UE has been registered on public network
BB ... Alternative procedure 1/2

(57) **Abstract:** The present disclosure relates to a 5th generation (5G) or pre-5G communication system for supporting a higher data transfer rate beyond a 4th generation (4G) communication system such as Long Term Evolution (LTE). According to various embodiments of the present disclosure, a method for the operation of a core network entity in a wireless communication system may comprise the steps of: acquiring identification information of a private network from a registration request message obtained from a user equipment (UE); selecting an authentication server function (AUSF) supporting authentication of the UE on the basis of the identification information of the private network; selecting a unified data management (UDM), which manages subscription information and registration information of the UE, in response to a procedure of the authentication of the UE and the AUSF; obtaining, from the UDM, subscription information of the UE to the private network; performing a test for the validity of the UE for the private network on the basis of the subscription information of the UE; and registering the UE on the private network on the basis of results obtained from the validity test and the authentication procedure.

(57) **요약서:** 본 개시는 LTE(Long Term Evolution)와 같은 4G(4th generation) 통신 시스템 이후 보다 높은 데이터 전송률을 지원하기 위한 5G(5th generation) 또는 pre-5G 통신 시스템에 관련된 것이다. 본 개시의 다양한 실시 예들에 따르면, 무선 통신 시스템에서 코어 네트워크 객체(core network entity)의 동작 방법은, 사용자 장치(user equipment)로부터 획득된 등록 요청 메시지에서 사설 네트워크의 식별 정보를 획득하는 과정과, 상기 사설 네트워크의 식별 정보에 기반하여, 상기 UE에 대한 인증을 지원하는 AUSF(authentication server function)를 선택하는 과정과, 상기 AUSF 및 상기 UE에 대한 인증 절차를 수행함에 대응하여, 상기 UE의 가입 정보 및 등록 정보를 관리하는 UDM(unified data management)을 선택하는 과정과, 상기 UDM으로부터 상기 사설 네트워크에 대한 상기 UE의 가입 정보를 획득하는 과정과, 상기 UE의 가입 정보에 기반하여, 상기 사설 네트워크에 대한 상기 UE의 유효성(validity) 검사를 수행하는 과정과, 상기 인증 절차 및 상기 유효성 검사의 결과에 기반하여, 상기 UE를 상기 사설 네트워크에 등록하는 과정을 포함할 수 있다.

WO 2020/036401 A1

[다음 쪽 계속]

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 제21조(3))

— 청구범위 보정 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

명세서

발명의 명칭: 무선 통신 시스템에서 네트워크에 등록하기 위한 장치 및 방법

기술분야

[1] 본 개시는 일반적으로 무선 통신 시스템에 관한 것으로, 보다 구체적으로 무선 통신 시스템에서 네트워크에 등록하기 위한 장치 및 방법에 관한 것이다.

배경기술

[2] 4G(4th generation) 통신 시스템 상용화 이후 증가 추세에 있는 무선 데이터 트래픽 수요를 충족시키기 위해, 개선된 5G(5th generation) 통신 시스템 또는 pre-5G 통신 시스템을 개발하기 위한 노력이 이루어지고 있다. 이러한 이유로, 5G 통신 시스템 또는 pre-5G 통신 시스템은 4G 네트워크 이후(Beyond 4G Network) 통신 시스템 또는 LTE(Long Term Evolution) 시스템 이후(Post LTE) 시스템이라 불리어지고 있다.

[3] 높은 데이터 전송률을 달성하기 위해, 5G 통신 시스템은 초고주파(mmWave) 대역(예를 들어, 60기가(60GHz) 대역과 같은)에서의 구현이 고려되고 있다. 초고주파 대역에서의 전파의 경로손실 완화 및 전파의 전달 거리를 증가시키기 위해, 5G 통신 시스템에서는 빔포밍(beamforming), 거대 배열 다중 입출력(massive MIMO), 전차원 다중입출력(Full Dimensional MIMO, FD-MIMO), 어레이 안테나(array antenna), 아날로그 빔형성(analog beam-forming), 및 대규모 안테나(large scale antenna) 기술들이 논의되고 있다.

[4] 또한 시스템의 네트워크 개선을 위해, 5G 통신 시스템에서는 진화된 소형 셀, 개선된 소형 셀(advanced small cell), 클라우드 무선 액세스 네트워크(cloud radio access network, cloud RAN), 초고밀도 네트워크(ultra-dense network), 기기 간 통신(Device to Device communication, D2D), 무선 백홀(wireless backhaul), 이동 네트워크(moving network), 협력 통신(cooperative communication), CoMP(Coordinated Multi-Points), 및 수신 간섭제거(interference cancellation) 등의 기술 개발이 이루어지고 있다.

[5] 이 밖에도, 5G 시스템에서는 진보된 코딩 변조(Advanced Coding Modulation, ACM) 방식인 FQAM(Hybrid Frequency Shift Keying and Quadrature Amplitude Modulation) 및 SWSC(Sliding Window Superposition Coding)과, 진보된 접속 기술인 FBMC(Filter Bank Multi Carrier), NOMA(Non Orthogonal Multiple Access), 및 SCMA(Sparse Code Multiple Access) 등이 개발되고 있다.

[6] 무선 통신 시스템에서 단말은 다양한 네트워크들로부터 서비스를 제공받을 수 있다. 서비스를 제공받기 위해, 단말은 네트워크에 등록될 것이 요구된다.

발명의 상세한 설명

기술적 과제

[7] 상술한 바와 같은 논의를 바탕으로, 본 개시(disclosure)는 무선 통신 시스템에서 네트워크에 등록하기 위한 장치 및 방법을 제공한다.

[8] 또한, 본 개시는 단말이 사설 네트워크를 발견하고, 발견된 사설 네트워크를 선택할 경우 단말이 사설 네트워크에 접속하기 위한 장치 및 방법을 제공한다.

[9] 또한, 본 개시는 사설 네트워크를 이용하고자 하는 단말이 사설 네트워크를 발견한 경우, 사설 네트워크의 유형 및/또는 사설 네트워크와 단말이 가입된 공용 네트워크 사이의 관계에 기반하여 사설 네트워크에 접속하기 위한 장치 및 방법을 제공한다.

과제 해결 수단

[10] 본 개시의 다양한 실시 예들에 따르면, 무선 통신 시스템에서 코어 네트워크 객체(core network entity)의 동작 방법은, 사용자 장치(user equipment)로부터 획득된 등록 요청 메시지에서 사설 네트워크의 식별 정보를 획득하는 과정과, 상기 사설 네트워크의 식별 정보에 기반하여, 상기 UE에 대한 인증을 지원하는 AUSF(authentication server function)를 선택하는 과정과, 상기 AUSF 및 상기 UE에 대한 인증 절차를 수행함에 대응하여, 상기 UE의 가입 정보 및 등록 정보를 관리하는 UDM(unified data management)을 선택하는 과정과, 상기 UDM으로부터 상기 사설 네트워크에 대한 상기 UE의 가입 정보를 획득하는 과정과, 상기 UE의 가입 정보에 기반하여, 상기 사설 네트워크에 대한 상기 UE의 유효성(validity) 검사를 수행하는 과정과, 상기 인증 절차 및 상기 유효성 검사의 결과에 기반하여, 상기 UE를 상기 사설 네트워크에 등록하는 과정을 포함할 수 있다.

[11] 무선 통신 시스템에서 코어 네트워크 객체(core network entity)의 장치는, 송수신기와, 상기 송수신기와 기능적으로 결합되고, 상기 송수신기를 제어하는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 사용자 장치(user equipment)로부터 획득된 등록 요청 메시지에서 사설 네트워크의 식별 정보를 획득하고, 상기 사설 네트워크의 식별 정보에 기반하여, 상기 UE에 대한 인증을 지원하는 AUSF(authentication server function)를 선택하고, 상기 AUSF 및 상기 UE에 대한 인증 절차를 수행함에 대응하여, 상기 UE의 가입 정보 및 등록 정보를 관리하는 UDM(unified data management)을 선택하고, 상기 UDM으로부터 상기 사설 네트워크에 대한 상기 UE의 가입 정보를 획득하고, 상기 UE의 가입 정보에 기반하여, 상기 사설 네트워크에 대한 상기 UE의 유효성(validity) 검사를 수행하고, 상기 인증 절차 및 상기 유효성 검사의 결과에 기반하여, 상기 UE를 상기 사설 네트워크에 등록하도록 구성된다.

발명의 효과

[12] 본 개시의 다양한 실시 예들에 따른 장치 및 방법은, 단말이 효과적으로 사설 네트워크에 접속하게 할 수 있게 한다.

[13] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술

분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[14] 도 1은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템을 도시한다.

[15] 도 2는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 기지국의 구성을 도시한다.

[16] 도 3은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말의 구성을 도시한다.

[17] 도 4는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 코어 네트워크 객체의 구성을 도시한다.

[18] 도 5a는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 유형 B 사설 네트워크의 구조를 도시한다.

[19] 도 5b는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 유형 A 사설 네트워크의 구조를 도시한다.

[20] 도 6은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 코어 네트워크 객체의 흐름도를 도시한다.

[21] 도 7은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 공용 네트워크에 등록된 경우 단말이 유형 A 사설 네트워크에 등록하기 위한 신호 흐름을 도시한다.

[22] 도 8은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 공용 네트워크에 등록되지 않은 경우 단말이 유형 A 사설 네트워크에 등록하기 위한 신호 흐름을 도시한다.

[23] 도 9는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 공용 네트워크에 등록되어 있지 아니한 경우 단말이 유형 A 사설 네트워크에 등록하기 위한 신호 흐름을 도시한다.

[24] 도 10은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 공용 네트워크에 가입되어 있지 않은 경우 단말이 유형 A 사설 네트워크에 등록하기 위한 신호 흐름을 도시한다.

[25] 도 11은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 유형 B 사설 네트워크에 등록하기 위한 신호 흐름을 도시한다.

[26] 도 12는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 유형 A 사설 네트워크에 초기 등록하기 위한 신호 흐름을 도시한다.

발명의 실시를 위한 최선의 형태

[27] 본 개시에서 사용되는 용어들은 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 다른 실시 예의 범위를 한정하려는 의도가 아닐 수 있다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다.
기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 용어들은 본 개시에 기재된 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과

동일한 의미를 가질 수 있다. 본 개시에 사용된 용어들 중 일반적인 사전에 정의된 용어들은, 관련 기술의 문맥상 가지는 의미와 동일 또는 유사한 의미로 해석될 수 있으며, 본 개시에서 명백하게 정의되지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다. 경우에 따라서, 본 개시에서 정의된 용어일지라도 본 개시의 실시 예들을 배제하도록 해석될 수 없다.

[28] 이하에서 설명되는 본 개시의 다양한 실시 예들에서는 하드웨어적인 접근 방법을 예시로서 설명한다. 하지만, 본 개시의 다양한 실시 예들에서는 하드웨어와 소프트웨어를 모두 사용하는 기술을 포함하고 있으므로, 본 개시의 다양한 실시 예들이 소프트웨어 기반의 접근 방법을 제외하는 것은 아니다.

[29] 이하 본 개시는 무선 통신 시스템에서 네트워크에 등록하기 위한 장치 및 방법에 관한 것이다. 구체적으로, 본 개시는 무선 통신 시스템에서 단말이 사설 네트워크(private network)에 등록하기 위한 기술을 설명한다.

[30] 이하 설명에서 사용되는 신호를 지칭하는 용어, 채널을 지칭하는 용어, 제어 정보를 지칭하는 용어, 네트워크 객체(network entity)들을 지칭하는 용어, 장치의 구성 요소를 지칭하는 용어 등은 설명의 편의를 위해 예시된 것이다. 따라서, 본 개시가 후술되는 용어들에 한정되는 것은 아니며, 동등한 기술적 의미를 가지는 다른 용어가 사용될 수 있다.

[31] 또한, 본 개시는, 일부 통신 규격(예: 3GPP(3rd Generation Partnership Project))에서 사용되는 용어들을 이용하여 다양한 실시 예들을 설명하지만, 이는 설명을 위한 예시일 뿐이다. 본 개시의 다양한 실시 예들은, 다른 통신 시스템에서도, 용이하게 변형되어 적용될 수 있다.

[32] 도 1은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템을 도시한다.

[33] 도 1을 참고하면, 무선 통신 시스템은 무선 접속 네트워크(radio access network, RAN) 102 및 코어 네트워크(core network, CN) 104를 포함한다.

[34] 무선 접속 네트워크 102는 사용자 장치, 예를 들어, 단말 120과 직접 연결되는 네트워크로서, 단말 120에게 무선 접속을 제공하는 인프라스트럭쳐(infrastructure)이다. 무선 접속 네트워크 102는 기지국 110을 포함하는 복수의 기지국들의 집합을 포함하며, 복수의 기지국들은 상호 간 형성된 인터페이스를 통해 통신을 수행할 수 있다. 복수의 기지국들 간 인터페이스들 중 적어도 일부는 유선이거나 무선일 수 있다. 기지국 110은 CU(central unit) 및 DU(distributed unit)으로 분리된 구조를 가질 수 있다. 이 경우, 하나의 CU가 복수의 DU들을 제어할 수 있다. 기지국 110은 기지국(base station) 외에 '액세스 포인트(access point, AP)', 'gNB(next generation node B)', '5G 노드(5th generation node)', '무선 포인트(wireless point)', '송수신 포인트(transmission/reception point, TRP)', 또는 이와 동등한 기술적 의미를 가지는 다른 용어로 지칭될 수 있다. 단말 120은 무선 접속 네트워크 102에 접속하고, 기지국 110과 무선 채널을 통해 통신을 수행한다. 단말 120은 단말(terminal) 외 '사용자 장비(user equipment, UE)', '이동국(mobile station)',

'가입자국(subscriber station)', '원격 단말(remote terminal)', '무선 단말(wireless terminal)', 또는 '사용자 장치(user device)' 또는 이와 동등한 기술적 의미를 가지는 다른 용어로 지칭될 수 있다.

[35] 코어 네트워크 104는 전체 시스템을 관리하는 네트워크로서, 무선 접속 네트워크 102을 제어하고, 무선 접속 네트워크 102를 통해 송수신되는 단말 120에 대한 데이터 및 제어 신호들을 처리한다. 코어 네트워크 104는 사용자 플랜(user plane) 및 제어 플랜(control plane)의 제어, 이동성(mobility)의 처리, 가입자 정보의 관리, 과금, 다른 종류의 시스템(예: LTE(long term evolution) 시스템)과의 연동 등 다양한 기능들을 수행한다. 상술한 다양한 기능들을 수행하기 위해, 코어 네트워크 104은 서로 다른 NF(network function)들을 가진 기능적으로 분리된 다수의 객체(entity)들을 포함할 수 있다. 예를 들어, 코어 네트워크 104는 AMF(access and mobility management function) 130a, SMF(session management function) 130b, UPF(user plane function) 130c, UDM(unified data management) 130d, 및 AUSF(authentication server function) 130e를 포함할 수 있다.

[36] AMF 130a는 NAS(non access stratum) 시그널링을 종료하고, NAS 암호화(ciphering), 및/또는 무결성(integrity) 보호, 등록 관리, 연결 관리, 이동성 관리, 접속 인증, 보안 컨텍스트(context) 관리를 수행할 수 있다. 예를 들어, AMF 130a는 EPC(evolved packet core)에서 MME(mobility management entity)의 기능의 전부 또는 일부를 수행할 수 있다.

[37] SMF 130b는 세션 관리(예: 세션 설정, 변경, 해제), 단말 120에 대한 IP(internet protocol) 주소 할당 및 관리, 세션 관리와 관련된 NAS 시그널링의 종료, 하향링크 데이터 알림, 적절한 트래픽 라우팅을 위해 UPF 130c에 대한 트래픽 조절(steering)을 수행할 수 있다.

[38] UPF 130c는 패킷 라우팅 및 포워딩, 패킷 검사, QoS(quality of service) 관리를 수행할 수 있다. UPF 130c는 데이터 네트워크와 상호 연결을 위한 외부 PDU(protocol data unit) 세션 포인트로서 동작할 수 있다. 또한, UPF 130c는 서로 다른 RAT(radio access technology)들간 이동 또는 동일한 RAT 내부에서 이동을 위한 앵커(anchor) 포인트로서 동작할 수 있다. UPF 130c는 EPC에서 S-GW(serving gateway) 및/또는 P-GW(packet data network gateway)의 기능의 전부 또는 일부를 수행할 수 있다.

[39] UDM 130d는 인증 및 키 합의(authentication and key agreement) 크레덴셜(credential)을 생성하고, 사용자 식별 정보를 처리하고, 액세스 인증, 가입 관리를 수행할 수 있다. UDM 130d는 EPC에서 HSS(home subscriber server)의 기능의 전부 또는 일부를 수행할 수 있다

[40] AUSF 130e는 인증 서버로서 동작할 수 있다. 예를 들어, AUSF 130e는 EPC에서 HSS(home subscriber server)의 기능의 전부 또는 일부를 수행할 수 있다.

[41] 도 1에 도시된 코어 네트워크 104의 객체들은 예시적인 것이고, 코어 네트워크 104는 다른 객체들을 더 포함할 수 있다. 예를 들어, 코어 네트워크 104는

PCF(policy control function), NSSF(network slice selection function), NEF(network exposure function), NRF(NF repository function), 및 AF(application function)와 같은 객체들 중 적어도 하나를 더 포함할 수 있다.

[42] 도 1에 도시된 코어 네트워크 104의 객체들 각각은 독립된 하드웨어 장치일 수 있으나, 가상화된 자원을 이용하여 각 노드의 기능을 수행하는 범용 서버 장치의 논리적 영역 또는 하드웨어 영역일 수 있다. 예를 들어, 도 1에 도시된 객체들 중 적어도 두 개의 기능들은 동일한 서버 장치에 의해 수행될 수 있다.

[43] 다양한 실시 예들에서, 코어 네트워크 104 및/또는 무선 접속 네트워크 102를 중 적어도 하나를 포함하는 셀룰러 네트워크(cellular network)가 정의될 수 있다. 다시 말해서, 셀룰러 네트워크는 코어 네트워크 104 및/또는 무선 접속 네트워크 102 중 적어도 하나를 포함할 수 있다.

[44] 다양한 실시 예들에서, 셀룰러 네트워크는 사설 셀룰러 네트워크(private cellular network) 또는 공용 셀룰러 네트워크(public cellular network)일 수 있다. 사설 셀룰러 네트워크는 특정 기관(예: 기업, 학교)에 의해 구축(construct)된 네트워크로서, 제한된 사용자들에게 접속이 허용되는 네트워크일 수 있다. 공용 셀룰러 네트워크는 통신 사업자(operator)에 의해 구축된 네트워크로서, 어떠한 가입 사용자(any subscribed user)들에게도 접속이 허용되는 네트워크일 수 있다. 다양한 실시 예들에서, 사설 셀룰러 네트워크는 사설 네트워크(private network)로 지칭될 수 있고, 공용 셀룰러 네트워크는 공용 네트워크(public network)로 지칭될 수 있다.

[45] 다양한 실시 예들에 따르면, 사설 네트워크는 사설 네트워크의 유형(type)에 따라 유형 A의 사설 네트워크와, 유형 B의 사설 네트워크로 구분될 수 있다. 유형 A의 사설 네트워크는 공용 네트워크와 연동(associated with)되고, 공용 네트워크의 사업자에 의해 운영되는 사설 네트워크일 수 있다. 유형 B의 사설 네트워크는 공용 네트워크에 연동되지 아니하고 독립적으로 운영되는 사설 네트워크일 수 있다. 다양한 실시 예들에서, 유형 A의 사설 네트워크는 '유형 A 사설 네트워크' 또는 '사설 네트워크 유형 A'로 지칭될 수 있고, 유형 B의 사설 네트워크는 '유형 B 사설 네트워크' 또는 '사설 네트워크 유형 B"로 지칭될 수 있다.

[46] 도 2는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 기지국의 구성을 도시한다. 도 2에 예시된 구성은 기지국 110의 구성으로서 이해될 수 있다. 이하 사용되는 '~부', '~기' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어, 또는, 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[47] 도 2를 참고하면, 기지국은 무선통신부 210, 백홀통신부 220, 저장부 230, 제어부 240를 포함한다.

[48] 무선통신부 210은 무선 채널을 통해 신호를 송수신하기 위한 기능들을 수행한다. 예를 들어, 무선통신부 210은 시스템의 물리 계층 규격에 따라

기저대역 신호 및 비트열 간 변환 기능을 수행한다. 예를 들어, 데이터 송신 시, 무선통신부 210은 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성한다. 또한, 데이터 수신 시, 무선통신부 210은 기저대역 신호를 복조 및 복호화를 통해 수신 비트열을 복원한다.

[49] 또한, 무선통신부 210은 기저대역 신호를 RF(radio frequency) 대역 신호로 상향변환한 후 안테나를 통해 송신하고, 안테나를 통해 수신되는 RF 대역 신호를 기저대역 신호로 하향변환한다. 이를 위해, 무선통신부 210은 송신 필터, 수신 필터, 증폭기, 믹서(mixer), 오실레이터(oscillator), DAC(digital to analog convertor), ADC(analog to digital convertor) 등을 포함할 수 있다. 또한, 무선통신부 210은 다수의 송수신 경로(path)들을 포함할 수 있다. 나아가, 무선통신부 210은 다수의 안테나 요소들(antenna elements)로 구성된 적어도 하나의 안테나 어레이(antenna array)를 포함할 수 있다.

[50] 하드웨어의 측면에서, 무선통신부 210은 디지털 유닛(digital unit) 및 아날로그 유닛(analog unit)으로 구성될 수 있으며, 아날로그 유닛은 동작 전력, 동작 주파수 등에 따라 다수의 서브 유닛(sub-unit)들로 구성될 수 있다. 디지털 유닛은 적어도 하나의 프로세서(예: DSP(digital signal processor))로 구현될 수 있다.

[51] 무선통신부 210은 상술한 바와 같이 신호를 송신 및 수신한다. 이에 따라, 무선통신부 210의 전부 또는 일부는 '송신부(transmitter)', '수신부(receiver)' 또는 '송수신부(transceiver)'로 지칭될 수 있다. 또한, 이하 설명에서, 무선 채널을 통해 수행되는 송신 및 수신은 무선통신부 210에 의해 상술한 바와 같은 처리가 수행되는 것을 포함하는 의미로 사용된다.

[52] 백홀통신부 220은 네트워크 내 다른 노드들과 통신을 수행하기 위한 인터페이스를 제공한다. 즉, 백홀통신부 220은 기지국에서 다른 노드, 예를 들어, 다른 접속 노드, 다른 기지국, 상위 노드, 코어 네트워크 등으로 송신되는 비트열을 물리적 신호로 변환하고, 다른 노드로부터 수신되는 물리적 신호를 비트열로 변환한다.

[53] 저장부 230은 기지국의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보 등의 데이터를 저장한다. 저장부 230은 휘발성 메모리, 비휘발성 메모리 또는 휘발성 메모리와 비휘발성 메모리의 조합으로 구성될 수 있다. 그리고, 저장부 230은 제어부 240의 요청에 따라 저장된 데이터를 제공한다.

[54] 제어부 240은 기지국의 전반적인 동작들을 제어한다. 예를 들어, 제어부 240은 무선통신부 210를 통해 또는 백홀통신부 220을 통해 신호를 송신 및 수신한다. 또한, 제어부 240은 저장부 230에 데이터를 기록하고, 읽는다. 그리고, 제어부 240은 통신 규격에서 요구하는 프로토콜 스택(protocol stack)의 기능들을 수행할 수 있다. 다른 구현 예에 따라, 프로토콜 스택은 무선통신부 210에 포함될 수 있다. 이를 위해, 제어부 240은 적어도 하나의 프로세서(processor)를 포함할 수 있다. 다양한 실시 예들에 따라, 제어부 240은 기지국이 후술하는 다양한 실시 예들에 따른 동작들을 수행하도록 제어할 수 있다.

[55] 도 3은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말의 구성을 도시한다. 도 3에 예시된 구성은 단말 120의 구성으로서 이해될 수 있다. 이하 사용되는 '~부', '~기' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어, 또는, 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[56] 도 3을 참고하면, 단말은 통신부 310, 저장부 320, 제어부 330를 포함한다.

[57] 통신부 310은 무선 채널을 통해 신호를 송수신하기 위한 기능들을 수행한다. 예를 들어, 통신부 310은 시스템의 물리 계층 규격에 따라 기저대역 신호 및 비트열 간 변환 기능을 수행한다. 예를 들어, 데이터 송신 시, 통신부 310은 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성한다. 또한, 데이터 수신 시, 통신부 310은 기저대역 신호를 복조 및 복호화를 통해 수신 비트열을 복원한다. 또한, 통신부 310은 기저대역 신호를 RF 대역 신호로 상향변환한 후 안테나를 통해 송신하고, 안테나를 통해 수신되는 RF 대역 신호를 기저대역 신호로 하향변환한다. 예를 들어, 통신부 310은 송신 필터, 수신 필터, 증폭기, 믹서, 오실레이터, DAC, ADC 등을 포함할 수 있다.

[58] 또한, 통신부 310은 다수의 송수신 경로(path)들을 포함할 수 있다. 나아가, 통신부 310은 다수의 안테나 요소들로 구성된 적어도 하나의 안테나 어레이를 포함할 수 있다. 하드웨어의 측면에서, 통신부 310은 디지털 회로 및 아날로그 회로(예: RFIC(radio frequency integrated circuit))로 구성될 수 있다. 여기서, 디지털 회로 및 아날로그 회로는 하나의 패키지로 구현될 수 있다. 또한, 통신부 310은 다수의 RF 체인들을 포함할 수 있다. 나아가, 통신부 310은 빔포밍을 수행할 수 있다.

[59] 통신부 310은 상술한 바와 같이 신호를 송신 및 수신한다. 이에 따라, 통신부 310의 전부 또는 일부는 '송신부', '수신부' 또는 '송수신부'로 지칭될 수 있다. 또한, 이하 설명에서 무선 채널을 통해 수행되는 송신 및 수신은 통신부 310에 의해 상술한 바와 같은 처리가 수행되는 것을 포함하는 의미로 사용된다.

[60] 저장부 320은 단말의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보 등의 데이터를 저장한다. 저장부 320은 휘발성 메모리, 비휘발성 메모리 또는 휘발성 메모리와 비휘발성 메모리의 조합으로 구성될 수 있다. 그리고, 저장부 320은 제어부 330의 요청에 따라 저장된 데이터를 제공한다.

[61] 제어부 330은 단말의 전반적인 동작들을 제어한다. 예를 들어, 제어부 330은 통신부 310를 통해 신호를 송신 및 수신한다. 또한, 제어부 330은 저장부 320에 데이터를 기록하고, 읽는다. 그리고, 제어부 330은 통신 규격에서 요구하는 프로토콜 스택의 기능들을 수행할 수 있다. 이를 위해, 제어부 330은 적어도 하나의 프로세서 또는 마이크로(micro) 프로세서를 포함하거나, 또는, 프로세서의 일부일 수 있다. 또한, 통신부 310의 일부 및 제어부 330은 CP(communication processor)라 지칭될 수 있다. 다양한 실시 예들에 따라, 제어부 330은 단말이 후술하는 다양한 실시 예들에 따른 동작들을 수행하도록 제어할

수 있다.

[62] 도 4은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 코어 네트워크 객체의 구성을 도시한다. 도 4에 예시된 구성 130은 도 1의 AMF 130a, SMF 130b, UPF 130c, UDM 130d 및 AUSF 130e 중 적어도 하나의 기능을 가지는 장치의 구성으로서 이해될 수 있다. 이하 사용되는 '...부', '...기' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어, 또는, 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[63] 상기 도 4를 참고하면, 코어 네트워크 객체는 통신부 410, 저장부 420, 제어부 430를 포함하여 구성된다.

[64] 통신부 410은 네트워크 내 다른 장치들과 통신을 수행하기 위한 인터페이스를 제공한다. 즉, 통신부 410은 코어 네트워크 객체에서 다른 장치로 송신되는 비트열을 물리적 신호로 변환하고, 다른 장치로부터 수신되는 물리적 신호를 비트열로 변환한다. 즉, 통신부 410은 신호를 송신 및 수신할 수 있다. 이에 따라, 통신부 410은 모뎀(modem), 송신부(transmitter), 수신부(receiver) 또는 송수신부(transceiver)로 지칭될 수 있다. 이때, 통신부 410은 코어 네트워크 객체가 백홀 연결(예: 유선 백홀 또는 무선 백홀)을 거쳐 또는 네트워크를 거쳐 다른 장치들 또는 시스템과 통신할 수 있도록 한다.

[65] 저장부 420은 코어 네트워크 객체의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보 등의 데이터를 저장한다. 저장부 420은 휘발성 메모리, 비휘발성 메모리 또는 휘발성 메모리와 비휘발성 메모리의 조합으로 구성될 수 있다. 그리고, 저장부 420은 제어부 430의 요청에 따라 저장된 데이터를 제공한다.

[66] 제어부 430은 코어 네트워크 객체의 전반적인 동작들을 제어한다. 예를 들어, 제어부 430은 통신부 410를 통해 신호를 송수신한다. 또한, 제어부 430은 저장부 420에 데이터를 기록하고, 읽는다. 이를 위해, 제어부 430은 적어도 하나의 프로세서(processor)를 포함할 수 있다.

[67] 다양한 실시 예들에 따라, 제어부 430는 UE로부터 획득된 등록 요청 메시지에서 사설 네트워크의 식별 정보를 획득하고, 사설 네트워크의 식별 정보에 기반하여, UE에 대한 인증을 지원하는 AUSF를 선택하고, 코어 네트워크 객체는 AUSF 및 UE에 대한 인증 절차를 수행함에 대응하여, UE의 가입 정보 및 등록 정보를 관리하는 UDM을 선택하고, UDM으로부터 사설 네트워크에 대한 UE의 가입 정보를 획득하고, UE의 가입 정보에 기반하여, 사설 네트워크에 대한 UE의 유효성 검사를 수행하고, 인증 절차 및 유효성 검사의 결과에 기반하여, UE를 사설 네트워크에 등록하도록 제어할 수 있다. 예를 들어, 제어부 430은 코어 네트워크 객체가 후술하는 다양한 실시 예들에 따른 동작들을 수행하도록 제어할 수 있다.

[68] 도 5a는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 유형 B 사설 네트워크의 구조를 도시한다.

[69] 도 5a를 참고하면, 유형 B 사설 네트워크 520의 구조는 공용 네트워크의 구조와 유사할 수 있다. 다시 말해서, UE 510은 RAN 530a를 통해 유형 B 사설 네트워크 520의 코어 네트워크에 접속하고, 유형 B 사설 네트워크 520의 코어 네트워크는 UE 510의 이동성 관리 mobility management)와 등록 관리(registration management)를 위한 기능을 수행하는 AMF 530b, UE 510의 인증을 위한 기능을 수행하는 AUSF 530c, UE 510의 가입(subscription)을 관리하는 UDM 530f, 세션 관리(session management)를 위한 기능을 수행하는 SMF 530d, 및 사용자 데이터의 포워딩을 위한 기능을 수행하는 UPF 530e를 포함할 수 있다. 그러나, 유형 B 사설 네트워크 520에서 UE 510의 식별 및/또는 UE 510의 인증을 위해 사용되는 방식은, 공용 네트워크에서와 상이할 수 있다.

[70] 다양한 실시 예들에서, 유형 B 사설 네트워크 520는 인터넷 540에 연결될 수 있고, 외부의 접속으로부터 안전을 제공하기 위해 유형 B 사설 네트워크 520 및 인터넷 540 사이에 방화벽이 설치(install)될 수 있다.

[71] 다양한 실시 예들에서, 유형 B 사설 네트워크 520은 코어 네트워크 104 및 무선 접속 네트워크 102를 포함할 수 있다. 이 경우, 유형 B 사설 네트워크 520의 코어 네트워크는 코어 네트워크 104에 대응할 수 있고, 각각의 AMF 530b, AUSF 530c, SMF 530d, UPF 530e, 및 UDM 530f는 각각의 AMF 130a, AUSF 130e, SMF 130b, UPF 130c, 및 UDM 130d에 대응할 수 있다. 또한, RAN 530a는 무선 접속 네트워크 102에 대응할 수 있고, 기지국 110을 포함할 수 있다.

[72] 도 5b는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 유형 A 사설 네트워크의 구조를 도시한다.

[73] 도 5b를 참고하면, 유형 A 사설 네트워크 550은 공용 네트워크 590과 연동(associated with)될 수 있고, 공용 네트워크 590의 통신 사업자와 동일한 통신 사업자에 의해 관리될 수 있다. UE 510은 무선 접속 네트워크 560a를 통해서 유형 A 사설 네트워크의 코어 네트워크에 접속할 수 있고, 유형 A 사설 네트워크의 코어 네트워크는 단말의 이동성 관리(mobility management) 및/또는 등록 관리(registration management)를 위한 기능을 수행하는 AMF 560b, UE 510의 인증을 위한 기능을 수행하는 AUSF 560c, UE 510의 가입(subscription)과 관련된(related to) 정보를 관리하는 UDM 560f, 세션 관리(session management)를 위한 기능을 수행하는 SMF 560d, 및 사용자 데이터를 포워딩하기 위한 기능을 수행하는 UPF 560e를 포함할 수 있다.

[74] 유형 A 사설 네트워크 550은 공용 네트워크 590과 연동될 수 있기 때문에, 유형 A 사설 네트워크 550과 공용 네트워크 590 사이의 연동은 로밍 네트워크(roaming network)와 유사할 수 있다. 따라서, 유형 A 사설 네트워크 550에 대한 접속을 시도하는 UE 510이 공용 네트워크 590에 가입된 경우, 유형 A 사설 네트워크 550에서 UE 510의 식별 및/또는 UE 510의 인증을 위해 사용되는 방식은, 공용 네트워크 590에서와 동일할 수 있다. 다른 예로, 유형 A 사설 네트워크 550에 대한 접속을 시도하는 UE 510이 공용 네트워크 590에 가입된 경우에도, 유형 A

사설 네트워크 550에서 UE 510의 식별 및/또는 UE 510의 인증을 위해 사용되는 방식은, 공용 네트워크 590에서와 상이할 수 있다.

[75] 반면, 유형 A 사설 네트워크 550에 대한 접속을 시도하는 UE 510이 공용 네트워크 590에 가입되어 있지 않은 경우, 유형 A 사설 네트워크 550에서 UE 510의 식별 및/또는 UE 510의 인증을 위해 사용되는 방식은, 유형 B 사설 네트워크 520의 경우와 같이 공용 네트워크 590에서와 상이할 수 있다.

[76] 다양한 실시 예들에서, 유형 B 사설 네트워크 520은 코어 네트워크 104 및 무선 접속 네트워크 102를 포함할 수 있다. 이 경우, 유형 B 사설 네트워크 520의 코어 네트워크는 코어 네트워크 104에 대응할 수 있고, 각각의 AMF 530b, AUSF 530c, SMF 530d, UPF 530e, 및 UDM 530f는 각각의 AMF 130a, AUSF 130e, SMF 130b, UPF 130c, 및 UDM 130d에 대응할 수 있다. 또한, RAN 530a는 무선 접속 네트워크 102에 대응할 수 있고, 기지국 110을 포함할 수 있다.

[77] 단말이 공용 네트워크를 통해 통신 서비스를 이용하는 경우, 단말은 MCC(mobile country code), MNC(mobile network code) 및/또는 PLMN(public land mobile network) 식별자(identifier, ID)를 이용하여 셀룰러 네트워크를 식별할 수 있다. 단말이 유형 A의 사설 네트워크에 등록하기 위해, 유형 A의 사설 네트워크와 연동된 공용 네트워크의 정보뿐만 아니라, 사업자가 할당한 사설 네트워크의 ID(예: PN ID(private network ID) 또는 NID(network ID), 본 개시에서는 PN ID 및 NID가 동일한 의미로 사용됨)와 같은 추가 정보가 네트워크 식별을 위해 사용된다. 단말이 유형 B의 사설 네트워크에 등록하기 위해, 유형 B의 사설 네트워크는 공용 네트워크와 별도로 운영되므로, 사설 네트워크 전용의 MCC 또는 MNC, 즉 사설 네트워크임을 나타낼 수 있는 PLMN ID와 함께 상술한 사설 네트워크의 ID가 네트워크 식별을 위해 사용된다.

[78] 따라서, 본 개시의 다양한 실시 예들은 사설 네트워크를 이용하고자 하는 단말이 사설 네트워크를 발견할 경우, 사설 네트워크의 유형 및/또는 사설 네트워크와 단말이 가입된 공용 네트워크 사이의 관계에 기반하여 사설 네트워크에 접속하기 위한 장치 및 방법을 제공한다.

[79] 나아가, 사설 네트워크의 유형에 따라 단말이 사설 네트워크를 발견하고 선택하는 방법과 사설 네트워크에 등록하는 절차가 달라질 수 있으므로, 본 개시의 다양한 실시 예들은 단말이 사설 네트워크를 발견하고, 발견된 사설 네트워크를 선택할 경우 단말이 사설 네트워크에 접속하기 위한 장치 및 방법을 제공한다.

[80] 도 6은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 코어 네트워크 객체의 흐름도를 도시한다. 도 6은 코어 네트워크 객체 130의 동작 방법을 예시한다.

[81] 도 6을 참고하면, 601 단계에서, 코어 네트워크 객체는 UE로부터 획득된 등록 요청 메시지에서 사설 네트워크의 식별 정보를 획득한다. 등록 요청 메시지는 사설 네트워크의 식별 정보뿐만 아니라, 등록 유형, UE의 식별자(identifier, ID),

사설 네트워크 접속 지시자, 사설 네트워크 UD ID 중 적어도 하나를 더 포함할 수 있다. 사설 네트워크의 식별 정보는 MCC, MNC, 및 PN ID의 조합으로 표현될 수 있다.

[82] 603 단계에서, 코어 네트워크 객체는 사설 네트워크의 식별 정보에 기반하여, UE에 대한 인증을 지원하는 AUSF를 선택한다. 다양한 실시 예들에서, 공용 네트워크의 AUSF를 선택하거나, 사설 네트워크의 AUSF를 선택할 수 있다.

[83] 605 단계에서, 코어 네트워크 객체는 AUSF 및 UE에 대한 인증 절차를 수행함에 대응하여, UE의 가입 정보 및 등록 정보를 관리하는 UDM을 선택한다. AUSF가 속한 셀룰러 네트워크가 사설 네트워크인지 또는 공용 네트워크인지에 따라, 코어 네트워크 객체는 공용 네트워크의 UDM을 선택하거나, 사설 네트워크의 UDM을 선택할 수 있다.

[84] 607 단계에서, 코어 네트워크 객체는 UDM으로부터 사설 네트워크에 대한 UE의 가입 정보를 획득한다. 코어 네트워크 객체는 UECM 등록 절차를 통해 UE의 등록 정보를 UDM에 갱신하고, SDM 등록 절차를 통해 UDM으로부터 UE의 가입 정보를 가져올 수 있다.

[85] 609 단계에서, 코어 네트워크 객체는 UE의 가입 정보에 기반하여, 사설 네트워크에 대한 UE의 유효성 검사를 수행한다. 다양한 실시 예들에서, 유효성 검사는 UE가 사설 네트워크에 등록되는 것이 허가되는지를 검사하기 위한 허가 절차를 포함할 수 있다.

[86] 611 단계에서, 코어 네트워크 객체는 인증 절차 및 유효성 검사의 결과에 기반하여, UE를 사설 네트워크에 등록한다. 예를 들어, 코어 네트워크 객체는 허가 및 인증이 성공적인 경우, UE가 사설 네트워크에 성공적으로 등록되었음을 지시하는 정보를 포함하는 등록 승인 메시지를 UE로 전달할 수 있다. 도시되지 아니하였으나, UE가 공용 네트워크에도 성공적으로 등록된 경우, 등록 승인 메시지는 UE가 공용 네트워크에 성공적으로 등록되었음을 지시하는 정보를 더 포함할 수 있다.

[87] 다양한 실시 예들에서, 사설 네트워크는 공용 네트워크와 연동된 유형 A 사설 네트워크를 포함할 수 있다.

[88] 사설 네트워크가 공용 네트워크와 연동된 유형 A 사설 네트워크를 포함하는 경우, AUSF 및 UDM은 공용 네트워크에 포함될 수 있고, 코어 네트워크 객체는 사설 네트워크에 포함된 로컬 UDM을 선택하고, 로컬 UDM으로부터 사설 네트워크에 대한 UE의 가입 정보를 획득할 수 있다. 코어 네트워크 객체는 UDM으로부터 획득된 UE의 가입 정보와, 로컬 UDM으로부터 획득된 UE의 가입 정보에 기반하여 사설 네트워크에 대한 UE의 유효성 검사를 수행할 수 있다.

[89] 사설 네트워크가 공용 네트워크와 연동된 유형 A 사설 네트워크를 포함하는 경우, AUSF 및 UDM은 사설 네트워크에 포함될 수 있고, 코어 네트워크 객체는 공용 네트워크에 포함된 매크로 UDM을 선택하고, 매크로 UDM으로부터 사설 네트워크에 대한 UE의 가입 정보를 획득하고, UDM으로부터 획득된 UE의 가입

정보와, 로컬 UDM으로부터 획득된 UE의 가입 정보에 기반하여, 사설 네트워크에 대한 UE의 유효성 검사를 수행할 수 있다.

[90] 사설 네트워크가 공용 네트워크와 연동된 유형 A 사설 네트워크를 포함하는 경우, 등록 요청 메시지는, UE의 공용 네트워크에 대한 접속이 완료된 후 미리 설정된 시간 이내에 송신될 수 있다. 예를 들어, 미리 설정된 시간은 등록 팔로온 타이머일 수 있다.

[91] 사설 네트워크가 공용 네트워크와 연동된 유형 A 사설 네트워크를 포함하는 경우, 코어 네트워크 객체는 등록 요청 메시지에 포함된 UE의 식별자(identifier, ID) 및 사설 네트워크의 식별 정보 중 적어도 하나에 기반하여 공용 네트워크에 대한 UE의 등록이 허용되지 아니함을 결정하고, UE의 사설 네트워크에 대한 초기 등록을 트리거하기 위해, UE의 이동성 등록에 대한 등록 거절 메시지를 UE로 전달할 수 있다.

[92] 사설 네트워크가 공용 네트워크와 연동된 유형 A 사설 네트워크를 포함하는 경우, 코어 네트워크 객체는 공용 네트워크에 대한 UE의 등록이 허용되지 아니함을 결정하고, 사설 네트워크에 대한 UE의 식별자(identifier, ID)를 UE에 요청하고, UE로부터 UE의 ID를 획득할 수 있다.

[93] 다양한 실시 예들에서, 사설 네트워크는 공용 네트워크와 연동되지 아니한 유형 B 사설 네트워크를 포함할 수 있다.

[94] 사설 네트워크가 공용 네트워크와 연동되지 아니한 유형 B 사설 네트워크를 포함하는 경우, 코어 네트워크 객체는 등록 메시지에 포함된 사설 네트워크의 식별 정보에 기반하여, 유형 B 사설 네트워크를 식별하고, 식별에 대응하여, 공용 네트워크에 대한 UE의 등록이 허용되지 아니함을 결정하고, UE의 사설 네트워크에 대한 초기 등록을 트리거하기 위해, UE의 이동성 등록에 대한 등록 거절 메시지를 UE로 전달할 수 있다.

[95] 도 7은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 공용 네트워크에 등록된 경우 단말이 유형 A 사설 네트워크에 등록하기 위한 신호 흐름을 도시한다. 도 7에서, UE 510은 공용 네트워크 720에 등록되었음이 가정되고, 사설 네트워크 710은 유형 A 사설 네트워크를 포함할 수 있다.

[96] 도 7을 참고하면, 701 단계에서, 사설 네트워크 710의 기지국(RAN 560a에 포함됨)은 UE 510으로 MCC, MNC 및 PN ID(private network ID)를 송신한다. 예를 들어, 기지국은 기지국이 서비스하는 사설 네트워크 710의 식별 정보(즉, MCC, MNC 및 PN ID)를 SIB(system information block) 메시지를 통해 방송할 수 있고, UE 510은 SIB 메시지에 포함된 MCC, MNC 및 PN ID를 식별할 수 있다.

[97] 703 단계에서, UE 510은 사설 네트워크 710을 검출하고, 검출된 사설 네트워크 710을 선택할 것을 결정할 수 있다. UE 510은 UE 510이 가입된 사설 네트워크 710을 발견(discover)하고, 사설 네트워크 710의 식별 정보들(즉, MCC, MNC, 및 PN ID) 중 적어도 하나에 기반하여 사설 네트워크 710이 UE 510이 접속된 공용 네트워크 720의 사업자에 의해 관리되는 유형 A 사설 네트워크임을 식별하고,

사설 네트워크 710을 선택할 것을 결정할 수 있다.

[98] 705 단계에서, UE 510은 등록 요청(registration request) 메시지를 기지국으로 송신한다. 다시 말해서, 사설 네트워크 710을 선택한 단말은 사설 네트워크 710에 접속하기 위해 등록 절차를 수행할 수 있다. 예를 들어, UE 510 및 기지국은 RRC(radio resource control) 연결 설정(RRC connection setup)을 수행하고, UE 510은 RRC를 통해 등록 요청 메시지를 기지국으로 송신할 수 있다. UE 510은 등록 요청 메시지에서 등록 유형(registration type)을 이동성 등록(mobility registration)으로 설정할 수 있고, 등록 요청 메시지는 사설 네트워크 710에 대한 등록을 지시하기 위해 사설 네트워크 710의 식별 정보 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다. 예를 들어, 사설 네트워크 710의 식별 정보는 MCC, MNC 및 PN ID의 조합으로 표현될 수 있다. 다른 예로, 등록 요청 메시지는 사설 네트워크 710의 식별 정보 대신 UE 510이 사설 네트워크 710에 대한 접속을 시도함을 지시하는 사설 네트워크 접속 지시자(private network access indicator)를 포함할 수 있다. UE 510의 ID는, 예를 들어, 공용 네트워크 720에 의해 할당된 임시 ID(예: GUTI(globally unique temporary identifier))일 수 있다. 다양한 실시 예들에서, 등록 요청 메시지는 사설 네트워크 710의 가입자에 대해 할당된 가입자 ID인 사설 네트워크 UE ID(private network UE ID)를 더 포함할 수 있다. 다양한 실시 예들에서, UE 510이 사설 네트워크 710뿐만 아니라 공용 네트워크 720에도 등록해야 함을 AMF 560b에 알리기 위해, UE 510은 등록 요청 메시지에서 등록 유형을 '통합 등록(combined registration)'으로 설정할 수 있다. 통합 등록은, UE 510이 사설 네트워크 710 및 공용 네트워크 720 모두에 등록하는 것이 요구됨을 지시할 수 있고, 이러한 지시를 위한 지시자를 포함할 수 있다. 다른 예로, UE 510이 사설 네트워크 710뿐만 아니라 공용 네트워크 720에도 등록해야 함을 AMF 560b에 알리기 위해, 등록 요청 메시지는 사설 네트워크 710 및 공용 네트워크 720에 대한 등록이 요구됨을 지시하기 위해 사설 네트워크 710의 식별 정보 및 공용 네트워크 720의 식별 정보를 포함할 수 있다. 다시 말해서, 등록 요청 메시지는 등록에 대한 타겟(target) 네트워크의 식별 정보로서, 사설 네트워크 710의 식별 정보와, 공용 네트워크 720의 식별 정보를 포함할 수 있다.

[99] 707 단계에서, 기지국은 등록 요청 메시지를 AMF 560b로 전달한다. 기지국은 UE 510으로부터 수신된 등록 요청 메시지로부터 사설 네트워크 710의 식별 정보를 식별하고, 식별 정보에 대응하는 사설 네트워크 710의 코어 네트워크에 포함된 AMF 560b로 전달할 수 있다. 기지국은 N2 메시지를 통해 등록 요청 메시지를 AMF 560b로 전달할 수 있고, 전달되는 메시지는 등록 유형이 이동성 등록임을 지시하는 정보, 사설 네트워크 710의 식별 정보, 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다.

[100] 709 단계에서, AMF 560b는 공용 네트워크 720에 대한 등록이 요구됨을 결정한다. AMF 560b는 UE 510에 대한 접속 관리가 사설 네트워크 710에서 뿐만

아니라 공용 네트워크 720에서도 수행되어야 하는지를 결정할 수 있다. AMF 560b는 등록 요청 메시지에 포함된 식별 정보들(즉, 등록 유형이 이동성 등록임을 지시하는 정보, 사설 네트워크 710의 식별 정보, 및 UE 510의 ID) 중 적어도 하나에 기반하여 UE 510이 접속을 시도하는 사설 네트워크 710이 UE 510가 접속된 공용 네트워크 720의 사업자에 의해 관리됨을 식별할 수 있고, 이 경우 AMF 560b는 UE 510에 대한 접속 관리가 사설 네트워크 710에서 뿐만 아니라 공용 네트워크 720에서도 수행되어야 함을 결정(즉, 공용 네트워크 720에 대한 등록이 요구됨을 결정)할 수 있다. 다양한 실시 예들에서, 등록 요청 메시지에 사설 네트워크 710 및 공용 네트워크 720에 대한 UE 510의 등록이 요구됨을 지시하는 지시자가 포함된 경우(또는, 등록 요청 메시지에서 등록 유형이 '통합 등록'으로 설정되거나, 등록 요청 메시지에 등록에 대한 타겟 네트워크의 식별 정보로서 사설 네트워크 710의 식별 정보 및 공용 네트워크 720의 식별 정보가 모두 포함된 경우), AMF 560b는 UE 510에 대한 접속 관리가 사설 네트워크 710에서 뿐만 아니라 공용 네트워크 720에서도 수행되어야 함을 결정할 수 있다.

[101] 711 단계에서, AMF 560b는 UE 컨텍스트(context)를 수신한다. AMF 560b는 등록 요청 메시지에 포함된 UE 510의 ID(예: GUTI)를 이용하여, 공용 네트워크 720의 AMF 580b로부터 공용 네트워크 720에 이미 등록된 UE 컨텍스트 정보를 가져올 수(retrieve) 있다.

[102] 711 단계가 수행된 후, 대안(alternative) 1로서 713 내지 731 단계들이 수행되거나, 대안 2로서 733 단계 내지 751 단계들이 수행될 수 있다. 대안 1에서, AMF 560b는 등록 프로세스의 인증(authentication) 및 허가(authorization) 프로세스를 수행하기 위해, 공용 네트워크 720의 AUSF 580c 및/또는 UDM 580f를 통해 UE 510의 사설 네트워크 710에 대한 인증을 수행하고, UE 510의 사설 네트워크 510의 이용에 대한 가입 정보를 공용 네트워크 720의 UDM 580f 또는 사설 네트워크 710의 UDM 560f로부터 획득하여 UE 510의 사설 네트워크 510의 이용에 대한 유효성(validity)을 검사하는 허가 절차를 수행하고, 사설 네트워크 710의 UDM 560f 또는 공용 네트워크 720의 UDM 580f에 UE 510의 등록 정보를 갱신(update)할 수 있다. 대안 2에서, AMF 560b는 UE 510의 사설 네트워크 710에 대한 인증을 수행하고, 사설 네트워크 710의 UDM 560f를 통해 UE의 사설 네트워크 710의 이용에 대한 가입 정보를 획득하여 UE 510의 사설 네트워크 510의 이용에 대한 유효성을 검사하는 허가 절차를 수행하고, 사설 네트워크 710의 UDM 560f에 UE 510의 등록 정보를 갱신할 수 있다.

[103] 대안 1과 관련된 단계들은 하기와 같다.

[104] 713 단계에서, AMF 560b는 매크로(macro) AUSF를 선택한다. 다양한 실시 예들에서, 매크로 AUSF는 공용 네트워크 720의 AUSF(예: AUSF 580c)일 수 있다. UE 510에 대한 접속 관리가 사설 네트워크 710에서 뿐만 아니라 공용 네트워크 720의 UDM 580f에서도 수행되어야 함을 결정한 AMF 560b는,

추가적인 인증이 필요한 경우, 매크로 AUSF를 선택할 수 있다. 예를 들어, 사설 네트워크 710의 이용을 위한 별도의(separate) 인증이 요구되는 경우, AMF 560b는 공용 네트워크 720의 AUSF들 중에서 사설 네트워크 710에 가입된 UE에 대한 인증을 지원하는 AUSF를 사설 네트워크 710의 식별 정보를 이용하여 선택할 수 있다.

[105] 715 단계에서, AMF 560b는 UE 510에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 717 단계에서, AMF 560b는 매크로 AUSF에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 다양한 실시 예들에서, 715 단계는 717 단계보다 먼저 수행되거나, 나중에 수행되거나, 또는 동시에 수행될 수 있다. 사설 네트워크 710의 정책(policy)에 따라, 715 단계 및/또는 717 단계는 생략될 수 있다.

[106] 719 단계에서, AMF 560b는 매크로 UDM을 선택한다. 다양한 실시 예들에서, 매크로 UDM은 공용 네트워크 720의 UDM(예: 580f)일 수 있다. 예를 들어, AMF 560b는 공용 네트워크 720에서 UE 510의 가입 정보 및/또는 등록 정보를 관리하는 UDM 580f를 선택할 수 있다.

[107] 721 단계에서, AMF 560b는 UECM(UE context management) 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 580f에 갱신할 수 있다.

[108] 723 단계에서, AMF 560b는 SDM(subscriber data management) 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 580f로부터 UE 510의 가입 정보를 가져올 수 있다. 예를 들어, AMF 560b는 UE 510이 등록을 시도하는 사설 네트워크 710의 식별 정보를 UDM 580f에 전달하여, 사설 네트워크 710에 대한 UE 510의 가입 정보를 획득할 수 있다.

[109] 725 단계에서, AMF 560b는 공용 네트워크 720으로부터 획득된 가입 데이터에 의해 사설 네트워크 710에 대한 UE 510의 유효성(validity)을 검사한다. 공용 네트워크 720의 UDM 580f로부터 사설 네트워크 710에 대한 UE 510의 가입 정보를 획득한 AMF 560b는 가입 정보에 기반하여 사설 네트워크 710의 이용에 대한 유효성을 검사하는 허가 절차를 수행할 수 있다.

[110] 727 단계에서, AMF 560b는 로컬 UDM을 선택한다. 다양한 실시 예들에서, 로컬 UDM은 사설 네트워크 710의 UDM(예: UDM 560f)일 수 있다. AMF 560b는 허가된 UE 510에 대해 사설 네트워크 710의 UDM을 검색하고, 검색된 UDM(예: UDM 560f)을 선택할 수 있다.

[111] 729 단계에서, AMF 560b는 UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 560f에 갱신할 수 있다.

[112] 731 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 560f로부터 UE 510에 대한 사설 네트워크 710의 가입 정보를 가져올 수 있다. 도시되지 아니하였으나, 723 단계에서 UDM 580f로부터 획득된 가입 정보가 731 단계에서 UDM 560f로부터 획득된 가입 정보와 상이할 경우,

사업자의 정책에 따라 UDM 580f로부터 획득된 정보가 우선순위가 더 높거나, UDM 560f로부터 획득된 정보가 우선 순위가 더 높을 수 있다.

[113] 도 7에서, 유효성 검사 단계(725 단계)가 UDM 560f로부터 사설 네트워크 710의 가입 정보를 획득하는 단계(731 단계) 이전에 수행되는 것으로 도시되었으나, 이는 예시적인 것이고, 유효성 검사는 AMF 560b가 UDM 580f로부터 UE 510의 가입 정보와, UDM 560f로부터 UE 510의 가입 정보를 획득한 후 수행될 수 있다. 다시 말해서, 725 단계는 731 단계 이후에 수행될 수 있다.

[114] 상술한 대안 1과 관련된 단계들의 순서는 예시적인 것이고, 다양한 변형이 가능하다. 예를 들어, AMF 560b는 717 단계에서 공용 네트워크 720의 AUSF 580c와 함께 UE 510에 대한 추가적인 인증 절차를 수행한 후, 사설 네트워크 710의 UDM 560f를 검색하여 검색된 UDM 560f에 UE 510의 등록 정보를 갱신(update)하고, UDM 560f로부터 사설 네트워크 710에서 UE 510에 대한 가입 정보를 수신할 수 있다. AMF 560b가 사설 네트워크 710의 UDM 560f를 검색하기 위해, AMF 560b는 사설 네트워크 710의 식별 정보를 이용할 수 있다. 다시 말해서, AMF 560b는 사설 네트워크 710의 식별 정보를 이용하여 사설 네트워크 710에 적합한(suitable for) UDM 560f를 검색할 수 있다. 다양한 실시 예들에서, 사설 네트워크 710의 식별 정보는 MCC, MNC 및 PN ID 중 적어도 하나, 또는 MCC, MNC 및 PN ID 중 적어도 둘의 조합으로 표현될 수 있다. 사설 네트워크 710의 UDM 560c를 선택한 AMF 560b는 사설 네트워크 710의 UDM 560f로부터 사설 네트워크 710에 대한 UE 510의 가입 정보를 획득하고, 가입 정보에 기반하여 UE 510의 사설 네트워크 710의 이용에 대한 유효성을 체크하는 허가 절차를 수행할 수 있다. 또한, AMF 560b는 공용 네트워크 720에 대한 등록을 유지하기 위해, 공용 네트워크 720에서 UE 510의 가입 정보 및 등록 정보를 관리하는 UDM 580f를 선택하고, 선택된 UDM 580f에 UE 510의 등록 정보를 갱신하고, UDM 580f로부터 UE 510의 가입 정보를 수신할 수 있다.

[115] 대안 2와 관련된 단계들은 하기와 같다.

[116] 709 단계에서 UE 510에 대한 접속 관리가 사설 네트워크 710에서 뿐만 아니라 공용 네트워크 720에서도 수행되어야 함을 결정한 AMF 560b는, 733 단계에서, 로컬 AUSF를 선택한다. 다양한 실시 예들에서, 로컬 AUSF는 사설 네트워크 710의 AUSF(예: AUSF 560c)일 수 있다. 사설 네트워크 710에서 UE 510에 대한 인증이 필요한 경우, AMF 560b는 AUSF 560c를 선택할 수 있다. 예를 들어, 사설 네트워크 710의 이용을 위한 별도의 인증이 요구되는 경우, AMF 560b는 사설 네트워크 710의 AUSF들 중에서 사설 네트워크 710에 가입된 UE에 대한 인증을 지원하는 AUSF를 선택할 수 있다.

[117] 735 단계에서, AMF 560b는 선택된 AUSF 560c에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 737 단계에서, AMF 560b는 UE 510에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 다양한 실시 예들에서, 737 단계는 735 단계보다 먼저 수행되거나, 나중에 수행되거나, 또는 동시에 수행될 수 있다.

사설 네트워크 710의 정책에 따라, 735 단계 및/또는 737 단계는 생략되거나, 공용 네트워크 720을 통한 인증으로 대치될(replaced for) 수 있다. 735 단계 및 737 단계와 같이 사설 네트워크 710에 대한 UE 510의 인증 과정이 공용 네트워크 720을 통한 인증으로 대치되는 경우, 733 단계 및 739 단계 대산 713 단계 및 719 단계가 수행될 수 있고, 공용 네트워크 720에 대한 인증을 통과한 UE 510은 사설 네트워크 710에 대한 인증 또한 통과한 것으로 간주될 수 있다.

[118] 739 단계에서, AMF 560b는 로컬 UDM(예: UDM 560f)을 선택한다. AMF 560b는 사설 네트워크 710에서 UE의 가입 정보 및/또는 등록 정보를 관리하는 UDM 560f를 선택할 수 있다.

[119] 709 단계에서 UE 510에 대한 접속 관리가 사설 네트워크 710에서 뿐만 아니라 공용 네트워크 720에서도 수행되어야 함을 결정한 AMF 560b는, 741 단계에서, UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 560f에 갱신할 수 있다.

[120] 743 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 560f로부터 UE 510에 대한 사설 네트워크 710의 가입 정보를 가져올 수 있다.

[121] 745 단계에서, AMF 560b는 가입 데이터에 의해 사설 네트워크 710에 UE 510의 유효성을 검사한다. 다시 말해서, AMF 560b는 사설 네트워크 710으로부터 획득된 가입 데이터에 기반하여 사설 네트워크 710에 대한 UE 510의 유효성을 검사할 수 있다. UDM 560f로부터 사설 네트워크 710에 대한 UE 510의 가입 정보를 획득한 AMF 560b는 가입 정보에 기반하여 사설 네트워크 710의 이용에 대한 유효성을 검사하는 허가 절차를 수행할 수 있다.

[122] 747 단계에서, AMF 560b는 매크로 UDM(예: UDM 580f)을 선택한다. AMF 560b는 허가된 UE 510에 대해 공용 네트워크 720의 UDM 580f를 검색하고, 검색된 UDM 580f를 선택할 수 있다.

[123] 749 단계에서, AMF 560b는 UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 580f에 갱신할 수 있다.

[124] 751 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 580f로부터 UE 510에 대한 사설 네트워크 710의 가입 정보를 가져올 수 있다. 예를 들어, AMF 560b는 UE 510이 등록을 시도하는 사설 네트워크 710의 식별 정보를 UDM 580f에 전달하여, 사설 네트워크 710에 대한 UE 510의 가입 정보를 획득할 수 있다. 도시되지 아니하였으나, 741 단계에서 UDM 560f로부터 획득된 가입 정보가 751 단계에서 UDM 580f로부터 획득된 가입 정보와 상이할 경우, 사업자의 정책에 따라 UDM 580f로부터 획득된 정보가 우선순위가 더 높거나, UDM 560f로부터 획득된 정보가 우선 순위가 더 높을 수 있다.

[125] 도 7에서, 유효성 검사 단계(745 단계)가 UDM 580f로부터 사설 네트워크 710의 가입 정보를 획득하는 단계(751 단계) 이전에 수행되는 것으로 도시되었으나,

이는 예시적인 것이고, 유효성 검사는 AMF 560b가 UDM 560f로부터 UE 510의 가입 정보와, UDM 580f로부터 UE 510의 가입 정보를 획득한 후 수행될 수 있다. 다시 말해서, 745 단계는 751 단계 이후에 수행될 수 있다.

[126] 753 단계에서, AMF 560b는 나머지 등록 절차를 수행한다. 예를 들어, AMF 560b는 UE 510의 등록을 위한 허가 및 인증 절차를 수행한 후, 허가 및 인증의 결과에 따라 UE 510에 등록 승인(registration accept) 메시지를 전달할 수 있다(허가 및 인증이 성공적인 경우). 등록 승인 메시지는 UE 510이 사설 네트워크 710에 성공적으로 등록되었음을 지시하는 정보와, 공용 네트워크 720에 성공적으로 등록되었음을 지시하는 정보를 포함할 수 있다. 예를 들어, 등록 승인 메시지는 '등록 결과="공용 네트워크 및 사설 네트워크 모두에 등록됨"(registration result = "registered to both public and private network")'과 같이 표현되는 정보를 포함할 수 있다.

[127] 다양한 실시 예들에 따르면, 도 7에 예시된 것과 같은, UE 510이 사설 네트워크 710에 등록하기 위한 절차들 및/또는 단계들은, UE 510이 가입되지는 아니하였으나, UE 510이 가입된 공용 네트워크의 사업자와 로밍 협약이 되어 있는 공용 네트워크(이하, 로밍 네트워크로 지칭된다)의 사업자에 의해 관리되는 유형 A 사설 네트워크(이하, 로밍 네트워크에 연계된 유형 A 사설 네트워크로 지칭된다)에 UE 510이 등록하는 경우에도 적용될 수 있다. 예를 들어, UE 510이 로밍 네트워크에 연계된 유형 A 사설 네트워크에 등록하는 절차는 하기와 같다.

[128] UE 510은 사설 네트워크를 발견하고, 사설 네트워크의 식별 정보에 기반하여 사설 네트워크가 UE 510이 직접 가입되지 아니하였으나 로밍 네트워크에 연계된 사설 네트워크임을 식별하고, 식별된 사설 네트워크를 선택할 것을 결정하고, 사설 네트워크에 접속하기 위해 UE 510이 도 7에서 설명된 사설 네트워크 710에 등록하기 위한 절차들 및/또는 단계들과 같은 등록 과정을 수행할 수 있다.

[129] 도 8은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 공용 네트워크에 등록되지 않은 경우 단말이 유형 A 사설 네트워크에 등록하기 위한 신호 흐름을 도시한다. 도 7에서, UE 510은 공용 네트워크 820에 등록되어 있지 않음이 가정되고, 네트워크 810은 유형 A 사설 네트워크를 포함할 수 있다.

[130] 도 8을 참고하면, 801 단계에서, 사설 네트워크 810의 기지국(RAN 560a에 포함됨)은 UE 510으로 MCC, MNC 및 PN ID를 송신한다. 예를 들어, 기지국은 기지국이 서비스하는 사설 네트워크 810의 식별 정보(즉, MCC, MNC 및 PN ID)를 SIB 메시지를 통해 방송할 수 있고, UE 510은 SIB 메시지에 포함된 MCC, MNC 및 PN ID를 식별할 수 있다.

[131] 803 단계에서, UE 510은 사설 네트워크 810을 검출하고, 검출된 사설 네트워크 810을 선택할 것을 결정할 수 있다. UE 510은 UE 510이 가입된 사설 네트워크 810을 발견하고, 사설 네트워크 810의 식별 정보들(즉, MCC, MNC, 및 PN ID) 중 적어도 하나에 기반하여 사설 네트워크 810이 UE 510이 가입된 공용 네트워크

820의 사업자에 의해 관리되는 유형 A 사설 네트워크임을 식별하고, 사설 네트워크 810을 선택할 것을 결정할 수 있다.

[132] 805 단계에서, UE 510은 등록 요청 메시지를 기지국으로 송신한다. 다시 말해서, 사설 네트워크 810을 선택한 단말은 사설 네트워크 810에 접속하기 위해 등록 절차를 수행할 수 있다. 예를 들어, UE 510 및 기지국은 RRC 연결 설정을 수행하고, UE 510은 RRC를 통해 등록 요청 메시지를 기지국으로 송신할 수 있다. UE 510은 등록 요청 메시지에서 등록 유형을 초기 등록(initial registration)으로 설정할 수 있고, 등록 요청 메시지는 사설 네트워크 810에 대한 등록을 지시하기 위해 사설 네트워크 810의 식별 정보 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다. 예를 들어, 사설 네트워크 810의 식별 정보는 MCC, MNC 및 PN ID의 조합으로 표현될 수 있다. 다른 예로, 등록 요청 메시지는 사설 네트워크 810의 식별 정보 대신 UE 510이 사설 네트워크 810에 대한 접속을 시도함을 지시하는 사설 네트워크 접속 지시자(private network access indicator)를 포함할 수 있다. UE 510의 ID는, 예를 들어, 공용 네트워크 820에 의해 할당된 임시 ID(예: GUTI(globally unique temporary identifier))이거나, 공용 네트워크 820에 의해 할당된 가입자 ID(예: SUTI(subscriber unique temporary identifier))일 수 있다. 다양한 실시 예들에서, 등록 요청 메시지는 사설 네트워크 810의 가입자에 대해 할당된 가입자 ID인 사설 네트워크 UE ID를 더 포함할 수 있다. 다양한 실시 예들에서, UE 510이 사설 네트워크 810뿐만 아니라 공용 네트워크 820에도 등록해야 함을 AMF 560b에 알리기 위해, UE 510은 등록 요청 메시지에서 등록 유형을 '통합 등록'으로 설정할 수 있다. 통합 등록은, UE 510이 사설 네트워크 810 및 공용 네트워크 820 모두에 등록하는 것이 요구됨을 지시할 수 있고, 이러한 지시를 위한 지시자를 포함할 수 있다. 다른 예로, UE 510이 사설 네트워크 810뿐만 아니라 공용 네트워크 820에도 등록해야 함을 AMF 560b에 알리기 위해, 등록 요청 메시지는 사설 네트워크 810 및 공용 네트워크 820에 대한 등록이 요구됨을 지시하기 위해 사설 네트워크 810의 식별 정보 및 공용 네트워크 820의 식별 정보를 포함할 수 있다. 다시 말해서, 등록 요청 메시지는 등록에 대한 타겟(target) 네트워크의 식별 정보로서, 사설 네트워크 810의 식별 정보와, 공용 네트워크 820의 식별 정보를 포함할 수 있다.

[133] 807 단계에서, 기지국은 등록 요청 메시지를 AMF 560b로 전달한다. 기지국은 UE 510으로부터 수신된 등록 요청 메시지로부터 사설 네트워크 810의 식별 정보를 식별하고, 식별 정보에 대응하는 사설 네트워크 810의 코어 네트워크에 포함된 AMF 560b로 전달할 수 있다. 기지국은 N2 메시지를 통해 등록 요청 메시지를 AMF 560b로 전달할 수 있고, 전달되는 메시지는 등록 유형이 초기 등록임을 지시하는 정보, 사설 네트워크 810의 식별 정보, 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다.

[134] 809 단계에서, AMF 560b는 공용 네트워크 820에 대한 등록이 요구됨을 결정한다. AMF 560b는 UE 510에 대한 접속 관리가 사설 네트워크 810에서 뿐만

아니라 공용 네트워크 820에서도 수행되어야 하는지를 결정할 수 있다. AMF 560b는 등록 요청 메시지에 포함된 식별 정보들(즉, 등록 유형이 초기 등록임을 지시하는 정보, 사설 네트워크 810의 식별 정보, UE 510의 ID 및/또는 사설 네트워크 UE ID) 중 적어도 하나에 기반하여 UE 510이 접속을 시도하는 사설 네트워크 810이 UE 510가 가입된 공용 네트워크 820의 사업자에 의해 관리됨을 식별할 수 있고, 이 경우 AMF 560b는 UE 510에 대한 접속 관리가 사설 네트워크 810에서 뿐만 아니라 공용 네트워크 820에서도 수행되어야 함을 결정(즉, 공용 네트워크 820에 대한 등록이 요구됨을 결정)할 수 있다. 다양한 실시 예들에서, 등록 요청 메시지에 사설 네트워크 810 및 공용 네트워크 820에 대한 UE 510의 등록이 요구됨을 지시하는 지시자가 포함된 경우(또는, 등록 요청 메시지에서 등록 유형이 '통합 등록'으로 설정되거나, 등록 요청 메시지에 등록에 대한 타겟 네트워크의 식별 정보로서 사설 네트워크 810의 식별 정보 및 공용 네트워크 720의 식별 정보가 모두 포함된 경우), AMF 560b는 UE 510에 대한 접속 관리가 사설 네트워크 810에서 뿐만 아니라 공용 네트워크 820에서도 수행되어야 함을 결정할 수 있다.811 단계에서, AMF 560b는 UE 컨텍스트(context)를 수신한다. AMF 560b는 등록 요청 메시지에 포함된 UE 510의 ID(예: GUTI 및/또는 SUTI)를 이용하여, 공용 네트워크 820의 AMF 580b로부터 공용 네트워크 820에 이미 등록된 UE 컨텍스트 정보를 가져올 수(retrieve) 있다.

[135] 811 단계가 수행된 후, 대안 1로서 813 내지 831 단계들이 수행되거나, 대안 2로서 833 단계 내지 851 단계들이 수행될 수 있다. 대안 1에서, AMF 560b는 등록 프로세스의 인증 및 허가 프로세스를 수행하기 위해, 공용 네트워크 820의 AUSF 580c 및/또는 UDM 580f를 통해 UE 510의 사설 네트워크 810에 대한 인증을 수행하고, UE 510의 사설 네트워크 510의 이용에 대한 가입 정보를 공용 네트워크 820의 UDM 580f 또는 사설 네트워크 810의 UDM 560f로부터 획득하여 UE 510의 사설 네트워크 510의 이용에 대한 유효성을 검사하는 허가 절차를 수행하고, 사설 네트워크 810의 UDM 560f 또는 공용 네트워크 820의 UDM 580f에 UE 510의 등록 정보를 갱신(update)할 수 있다. 대안 2에서, AMF 560b는 사설 네트워크 810의 AUSF 560c 및/또는 UDM 560f를 통해 UE 510의 사설 네트워크 810에 대한 인증을 수행하고, 사설 네트워크 810의 UDM 560f를 통해 UE의 사설 네트워크 810의 이용에 대한 가입 정보를 획득하여 UE 510의 사설 네트워크 510의 이용에 대한 유효성을 검사하는 허가 절차를 수행하고, 사설 네트워크 810의 UDM 560f에 UE 510의 등록 정보를 갱신할 수 있다.

[136] 대안 1과 관련된 단계들은 하기와 같다.

[137] 813 단계에서, AMF 560b는 매크로 AUSF를 선택한다. 다양한 실시 예들에서, 매크로 AUSF는 공용 네트워크 820의 AUSF(예: AUSF 580c)일 수 있다. UE 510에 대한 접속 관리가 사설 네트워크 810에서 뿐만 아니라 공용 네트워크 820의 UDM 580f에서도 수행되어야 함을 결정한 AMF 560b는, 추가적인 인증이 필요한 경우, 매크로 AUSF를 선택할 수 있다. 예를 들어, 사설 네트워크 810의 이용을

위한 별도의(separate) 인증이 요구되는 경우, AMF 560b는 공용 네트워크 820의 AUSF들 중에서 사설 네트워크 810에 가입된 UE에 대한 인증을 지원하는 AUSF를 사설 네트워크 810의 식별 정보를 이용하여 선택할 수 있다.

[138] 815 단계에서, AMF 560b는 UE 510에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 817 단계에서, AMF 560b는 매크로 AUSF에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 다양한 실시 예들에서, 815 단계는 817 단계보다 먼저 수행되거나, 나중에 수행되거나, 또는 동시에 수행될 수 있다. 사설 네트워크 810의 정책에 따라, 815 단계 및/또는 817 단계는 생략될 수 있다.

[139] 819 단계에서, AMF 560b는 매크로 UDM을 선택한다. 다양한 실시 예들에서, 매크로 UDM은 공용 네트워크 820의 UDM(예: 580f)일 수 있다. 예를 들어, AMF 560b는 공용 네트워크 820에서 UE 510의 가입 정보 및/또는 등록 정보를 관리하는 UDM 580f를 선택할 수 있다.

[140] 821 단계에서, AMF 560b는 UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 580f에 갱신할 수 있다.

[141] 823 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 580f로부터 UE 510의 가입 정보를 가져올 수 있다. 예를 들어, AMF 560b는 UE 510이 등록을 시도하는 사설 네트워크 810의 식별 정보를 UDM 580f에 전달하여, 사설 네트워크 810에 대한 UE 510의 가입 정보를 획득할 수 있다.

[142] 825 단계에서, AMF 560b는 공용 네트워크 820으로부터 획득된 가입 데이터에 의해 사설 네트워크 810에 대한 UE 510의 유효성을 검사한다. 공용 네트워크 820의 UDM 580f로부터 사설 네트워크 810에 대한 UE 510의 가입 정보를 획득한 AMF 560b는 가입 정보에 기반하여 사설 네트워크 810의 이용에 대한 유효성을 검사하는 허가 절차를 수행할 수 있다.

[143] 827 단계에서, AMF 560b는 로컬 UDM을 선택한다. 다양한 실시 예들에서, 로컬 UDM은 사설 네트워크 810의 UDM(예: UDM 560f)일 수 있다. AMF 560b는 허가된 UE 510에 대해 사설 네트워크 810의 UDM을 검색하고, 검색된 UDM(예: UDM 560f)을 선택할 수 있다.

[144] 829 단계에서, AMF 560b는 UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 560f에 갱신할 수 있다.

[145] 831 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 560f로부터 UE 510에 대한 사설 네트워크 810의 가입 정보를 가져올 수 있다. 도시되지 아니하였으나, 823 단계에서 UDM 580f로부터 획득된 가입 정보가 831 단계에서 UDM 560f로부터 획득된 가입 정보와 상이할 경우, 사업자의 정책에 따라 UDM 580f로부터 획득된 정보가 우선순위가 더 높거나, UDM 560f로부터 획득된 정보가 우선 순위가 더 높을 수 있다.

[146] 도 8에서, 유효성 검사 단계(825 단계)가 UDM 560f로부터 사설 네트워크 810의 가입 정보를 획득하는 단계(831 단계) 이전에 수행되는 것으로 도시되었으나,

이는 예시적인 것이고, 유효성 검사는 AMF 560b가 UDM 580f로부터 UE 510의 가입 정보와, UDM 560f로부터 UE 510의 가입 정보를 획득한 후 수행될 수 있다. 다시 말해서, 825 단계는 831 단계 이후에 수행될 수 있다.

[147] 상술한 대안 1과 관련된 단계들의 순서는 예시적인 것이고, 다양한 변형이 가능하다. 예를 들어, AMF 560b는 817 단계에서 공용 네트워크 820의 AUSF 580c와 함께 UE 510에 대한 추가적인 인증 절차를 수행한 후, 사설 네트워크 810의 UDM 560f를 검색하여 검색된 UDM 560f에 UE 510의 등록 정보를 갱신(update)하고, UDM 560f로부터 사설 네트워크 810에서 UE 510에 대한 가입 정보를 수신할 수 있다. AMF 560b가 사설 네트워크 810의 UDM 560f를 검색하기 위해, AMF 560b는 사설 네트워크 810의 식별 정보를 이용할 수 있다. 다시 말해서, AMF 560b는 사설 네트워크 810의 식별 정보를 이용하여 사설 네트워크 810에 적합한(suitable for) UDM 560f를 검색할 수 있다. 다양한 실시 예들에서, 사설 네트워크 810의 식별 정보는 MCC, MNC 및 PN ID 중 적어도 하나, 또는 MCC, MNC 및 PN ID 중 적어도 둘의 조합으로 표현될 수 있다. 사설 네트워크 810의 UDM 560c를 선택한 AMF 560b는 사설 네트워크 810의 UDM 560f로부터 사설 네트워크 810에 대한 UE 510의 가입 정보를 획득하고, 가입 정보에 기반하여 UE 510의 사설 네트워크 810의 이용에 대한 유효성을 체크하는 허가 절차를 수행할 수 있다. 또한, AMF 560b는 공용 네트워크 820에 대한 등록을 유지하기 위해, 공용 네트워크 820에서 UE 510의 가입 정보 및 등록 정보를 관리하는 UDM 580f를 선택하고, 선택된 UDM 580f에 UE 510의 등록 정보를 갱신하고, UDM 580f로부터 UE 510의 가입 정보를 수신할 수 있다. 대안 2와 관련된 단계들은 하기와 같다.

[148] 809 단계에서 UE 510에 대한 접속 관리가 사설 네트워크 810에서 뿐만 아니라 공용 네트워크 820에서도 수행되어야 함을 결정한 AMF 560b는, 833 단계에서, 로컬 AUSF를 선택한다. 다양한 실시 예들에서, 로컬 AUSF는 사설 네트워크 810의 AUSF(예: AUSF 560c)일 수 있다. 사설 네트워크 810에서 UE 510에 대한 인증이 필요한 경우, AMF 560b는 AUSF 560c를 선택할 수 있다. 예를 들어, 사설 네트워크 810의 이용을 위한 별도의 인증이 요구되는 경우, AMF 560b는 사설 네트워크 810의 AUSF들 중에서 사설 네트워크 810에 가입된 UE에 대한 인증을 지원하는 AUSF를 선택할 수 있다.

[149] 835 단계에서, AMF 560b는 선택된 AUSF 560c에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 837 단계에서, AMF 560b는 UE 510에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 다양한 실시 예들에서, 837 단계는 835 단계보다 먼저 수행되거나, 나중에 수행되거나, 또는 동시에 수행될 수 있다. 사설 네트워크 810의 정책에 따라, 835 단계 및/또는 837 단계는 생략되거나, 공용 네트워크 820을 통한 인증으로 대치될(replaced for) 수 있다. 835 단계 및 837 단계와 같이 사설 네트워크 810에 대한 UE 510의 인증 과정이 공용 네트워크 820을 통한 인증으로 대치되는 경우, 833 단계 및 839 단계 대산 813 단계 및 819

단계가 수행될 수 있고, 공용 네트워크 820에 대한 인증을 통과한 UE 510은 사설 네트워크 810에 대한 인증 또한 통과한 것으로 간주될 수 있다.

[150] 839 단계에서, AMF 560b는 로컬 UDM(예: UDM 560f)을 선택한다. AMF 560b는 사설 네트워크 810에서 UE의 가입 정보 및/또는 등록 정보를 관리하는 UDM 560f를 선택할 수 있다.

[151] 809 단계에서 UE 510에 대한 접속 관리가 사설 네트워크 810에서 뿐만 아니라 공용 네트워크 820에서도 수행되어야 함을 결정한 AMF 560b는, 841 단계에서, UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 560f에 갱신할 수 있다.

[152] 843 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 560f로부터 UE 510에 대한 사설 네트워크 810의 가입 정보를 가져올 수 있다.

[153] 845 단계에서, AMF 560b는 가입 데이터에 의해 사설 네트워크 810에 UE 510의 유효성을 검사한다. 다시 말해서, AMF 560b는 사설 네트워크 810으로부터 획득된 가입 데이터에 기반하여 사설 네트워크 810에 대한 UE 510의 유효성을 검사할 수 있다. UDM 560f로부터 사설 네트워크 810에 대한 UE 510의 가입 정보를 획득한 AMF 560b는 가입 정보에 기반하여 사설 네트워크 810의 이용에 대한 유효성을 검사하는 허가 절차를 수행할 수 있다.

[154] 847 단계에서, AMF 560b는 매크로 UDM(예: UDM 580f)을 선택한다. AMF 560b는 허가된 UE 510에 대해 공용 네트워크 820의 UDM 580f를 검색하고, 검색된 UDM 580f를 선택할 수 있다.

[155] 849 단계에서, AMF 560b는 UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 580f에 갱신할 수 있다.

[156] 851 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 580f로부터 UE 510에 대한 사설 네트워크 810의 가입 정보를 가져올 수 있다. 예를 들어, AMF 560b는 UE 510이 등록을 시도하는 사설 네트워크 810의 식별 정보를 UDM 580f에 전달하여, 사설 네트워크 810에 대한 UE 510의 가입 정보를 획득할 수 있다. 도시되지 아니하였으나, 841 단계에서 UDM 560f로부터 획득된 가입 정보가 851 단계에서 UDM 580f로부터 획득된 가입 정보와 상이할 경우, 사업자의 정책에 따라 UDM 580f로부터 획득된 정보가 우선순위가 더 높거나, UDM 560f로부터 획득된 정보가 우선 순위가 더 높을 수 있다.

[157] 도 8에서, 유효성 검사 단계(845 단계)가 UDM 580f로부터 사설 네트워크 810의 가입 정보를 획득하는 단계(851 단계) 이전에 수행되는 것으로 도시되었으나, 이는 예시적인 것이고, 유효성 검사는 AMF 560b가 UDM 560f로부터 UE 510의 가입 정보와, UDM 580f로부터 UE 510의 가입 정보를 획득한 후 수행될 수 있다. 다시 말해서, 845 단계는 851 단계 이후에 수행될 수 있다.

[158] 853 단계에서, AMF 560b는 나머지 등록 절차를 수행한다. 예를 들어, AMF

560b는 UE 510의 등록을 위한 허가 및 인증 절차를 수행한 후, 허가 및 인증의 결과에 따라 UE 510에 등록 승인(registration accept) 메시지를 전달할 수 있다(허가 및 인증이 성공적인 경우). 등록 승인 메시지는 UE 510이 사설 네트워크 810에 성공적으로 등록되었음을 지시하는 정보와, 공용 네트워크 820에 성공적으로 등록되었음을 지시하는 정보를 포함할 수 있다. 예를 들어, 등록 승인 메시지는 '등록 결과="공용 네트워크 및 사설 네트워크 모두에 등록됨"(registration result = "registered to both public and private network")'과 같이 표현되는 정보를 포함할 수 있다.

[159] 다양한 실시 예들에 따르면, 도 8에 예시된 것과 같은, UE 510이 사설 네트워크 810에 등록하기 위한 절차들 및/또는 단계들은, UE 510이 가입되지는 아니하였으나, UE 510이 가입된 공용 네트워크의 사업자와 로밍 협약이 되어 있는 공용 네트워크(즉, 로밍 네트워크)의 사업자에 의해 관리되는 유형 A 사설 네트워크(즉, 로밍 네트워크에 연계된 유형 A 사설 네트워크로 지칭된다)에 UE 510이 등록하는 경우에도 적용될 수 있다. 예를 들어, UE 510이 로밍 네트워크에 연계된 유형 A 사설 네트워크에 등록하는 절차는 하기와 같다.

[160] UE 510은 사설 네트워크를 발견하고, 사설 네트워크의 식별 정보에 기반하여 사설 네트워크가 UE 510이 직접 가입되지 아니하였으나 로밍 네트워크에 연계된 사설 네트워크임을 식별하고, 식별된 사설 네트워크를 선택할 것을 결정하고, 사설 네트워크에 접속하기 위해 UE 510이 도 8에서 설명된 사설 네트워크 810에 등록하기 위한 절차들 및/또는 단계들과 같은 등록 과정을 수행할 수 있다.

[161] 도 9는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 공용 네트워크에 등록되어 있지 아니한 경우 단말이 유형 A 사설 네트워크에 등록하기 위한 신호 흐름을 도시한다. 도 9에서, 사설 네트워크 910은 유형 A 사설 네트워크를 포함할 수 있다.

[162] 도 9를 참고하면, 901 단계에서, 사설 네트워크 910의 기지국(RAN 560a에 포함됨)은 UE 510으로 MCC, MNC 및 PN ID를 송신한다. 예를 들어, 기지국은 기지국이 서비스하는 사설 네트워크 910의 식별 정보(즉, MCC, MNC 및 PN ID)를 SIB 메시지를 통해 방송할 수 있고, UE 510은 SIB 메시지에 포함된 MCC, MNC 및 PN ID를 식별할 수 있다.

[163] 903 단계에서, UE 510은 사설 네트워크 910을 검출하고, 검출된 사설 네트워크 910을 선택할 것을 결정할 수 있다. UE 510은 UE 510이 가입된 사설 네트워크 910을 발견하고, 사설 네트워크 910의 식별 정보들(즉, MCC, MNC, 및 PN ID) 중 적어도 하나에 기반하여 사설 네트워크 910이 UE 510이 가입된 공용 네트워크 920의 사업자에 의해 관리되는 유형 A 사설 네트워크임을 식별하고, 사설 네트워크 910을 선택할 것을 결정할 수 있다.

[164] 905 단계에서, UE 510가 공용 네트워크 920에 등록되지 않았을 경우, UE 510은 공용 네트워크 920에 등록하기 위한 절차를 수행한다. UE 510은 UE 510이 공용

네트워크 920에 접속 및/또는 등록되어 있지 아니하고, 공용 네트워크 920을 통해 서비스되지 아니하는 상황에 있으므로, UE 510은 일반적인 등록 절차(예: 3GPP TS23.502에서 기술되는(specified) 등록 절차)에 따라 공용 네트워크 920에 등록할 수 있다.

[165] 907 단계에서, UE 510은 등록 요청 메시지를 기지국으로 송신한다. 예를 들어, UE 510 및 기지국은 RRC 연결 설정을 수행하고, UE 510은 RRC를 통해 등록 요청 메시지를 기지국으로 송신할 수 있다. UE 510의 공용 네트워크 920에 대한 접속이 완료된 후, UE 510은 사설 네트워크 910에 대한 추가 등록이 필요함을 지시하는 등록 팔로온 타이머(registration follow-on timer)가 종료되기 전 사설 네트워크 910에 대한 이동성 등록을 수행할 수 있고, 이동성 등록을 위해 등록 요청 메시지를 기지국으로 송신할 수 있다. 등록 팔로온 타이머는 UE 510이 사설 네트워크 910에 등록하기로 결정한 시점부터 시작하거나, UE 510이 공용 네트워크 920에 대한 등록을 완료한 시점부터 시작할 수 있다. UE 510은 등록 요청 메시지에서 등록 유형을 이동성 등록으로 설정할 수 있고, 등록 요청 메시지는 사설 네트워크 910에 대한 등록을 지시하기 위해 사설 네트워크 910의 식별 정보 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다. 예를 들어, 사설 네트워크 910의 식별 정보는 MCC, MNC 및 PN ID의 조합으로 표현될 수 있다. 다른 예로, 등록 요청 메시지는 사설 네트워크 910의 식별 정보 대신 UE 510이 사설 네트워크 910에 대한 접속을 시도함을 지시하는 사설 네트워크 접속 지시자를 포함할 수 있다. UE 510의 ID는, 예를 들어, 공용 네트워크 920에 의해 할당된 임시 ID(예: GUTI)이거나, 공용 네트워크 920에 의해 할당된 가입자 ID(예: SUTI)일 수 있다. 다양한 실시 예들에서, 등록 요청 메시지는 사설 네트워크 910의 가입자에 대해 할당된 가입자 ID인 사설 네트워크 UE ID를 더 포함할 수 있다. 다양한 실시 예들에서, UE 510이 사설 네트워크 910뿐만 아니라 공용 네트워크 920에도 등록해야 함을 AMF 560b에 알리기 위해, UE 510은 등록 요청 메시지에서 등록 유형을 '통합 등록'으로 설정할 수 있다. 통합 등록은, UE 510이 사설 네트워크 910 및 공용 네트워크 920 모두에 등록하는 것이 요구됨을 지시할 수 있고, 이러한 지시를 위한 지시자를 포함할 수 있다. 다른 예로, UE 510이 사설 네트워크 910뿐만 아니라 공용 네트워크 920에도 등록해야 함을 AMF 560b에 알리기 위해, 등록 요청 메시지는 사설 네트워크 910 및 공용 네트워크 920에 대한 등록이 요구됨을 지시하기 위해 사설 네트워크 910의 식별 정보 및 공용 네트워크 920의 식별 정보를 포함할 수 있다. 다시 말해서, 등록 요청 메시지는 등록에 대한 타겟(target) 네트워크의 식별 정보로서, 사설 네트워크 910의 식별 정보와, 공용 네트워크 920의 식별 정보를 포함할 수 있다.

[166] 909 단계에서, 기지국은 등록 요청 메시지를 AMF 560b로 전달한다. 기지국은 UE 510으로부터 수신된 등록 요청 메시지로부터 사설 네트워크 910의 식별 정보를 식별하고, 식별 정보에 대응하는 사설 네트워크 910의 코어 네트워크에 포함된 AMF 560b로 전달할 수 있다. 기지국은 N2 메시지를 통해 등록 요청

메시지를 AMF 560b로 전달할 수 있고, 전달되는 메시지는 등록 유형이 초기 등록임을 지시하는 정보, 사설 네트워크 910의 식별 정보, 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다.

[167] 911 단계에서, AMF 560b는 공용 네트워크 920에 대한 등록이 요구됨을 결정한다. AMF 560b는 UE 510에 대한 접속 관리가 사설 네트워크 910에서 뿐만 아니라 공용 네트워크 920에서도 수행되어야 하는지를 결정할 수 있다. AMF 560b는 등록 요청 메시지에 포함된 식별 정보들(즉, 등록 유형이 초기 등록임을 지시하는 정보, 사설 네트워크 910의 식별 정보, UE 510의 ID 및/또는 사설 네트워크 UE ID) 중 적어도 하나에 기반하여 UE 510이 접속을 시도하는 사설 네트워크 910이 UE 510가 가입된 공용 네트워크 920의 사업자에 의해 관리됨을 식별할 수 있고, 이 경우 AMF 560b는 UE 510에 대한 접속 관리가 사설 네트워크 910에서 뿐만 아니라 공용 네트워크 920에서도 수행되어야 함을 결정(즉, 공용 네트워크 920에 대한 등록이 요구됨을 결정)할 수 있다.

[168] 911 단계 이후의 단계들은 도 7의 709 단계 이후의 단계들과 동일하다.

[169] 도 10은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 가입되어 있지 않고, 단말에 대한 로밍 네트워크가 아닌 공용 네트워크와 연동된 유형 A 사설 네트워크에 단말이 등록하기 위한 신호 흐름을 도시한다. 도 9에서, UE 510은 공용 네트워크 1020에 접속 및/또는 등록되어 공용 네트워크 1020에 의해 서비스되거나, 공용 네트워크 1020에 접속되어 있지 않음이 가정되고, 사설 네트워크 1010은 유형 A 사설 네트워크를 포함할 수 있다.

[170] 도 10을 참고하면, 1001 단계에서, 사설 네트워크 1010의 기지국(RAN 560a에 포함됨)은 UE 510으로 MCC, MNC 및 PN ID를 송신한다. 예를 들어, 기지국은 기지국이 서비스하는 사설 네트워크 1010의 식별 정보(즉, MCC, MNC 및 PN ID)를 SIB 메시지를 통해 방송할 수 있고, UE 510은 SIB 메시지에 포함된 MCC, MNC 및 PN ID를 식별할 수 있다.

[171] 1003 단계에서, UE 510은 사설 네트워크 1010을 검출하고, 검출된 사설 네트워크 1010을 선택할 것을 결정할 수 있다. UE 510은 UE 510이 가입된 사설 네트워크 1010을 발견하고, 사설 네트워크 1010의 식별 정보들(즉, MCC, MNC, 및 PN ID) 중 적어도 하나에 기반하여 사설 네트워크 1010이 UE 510이 가입되지 아니한 공용 네트워크 820의 사업자에 의해 관리되는 유형 A 사설 네트워크임을 식별하고, 사설 네트워크 1010을 선택할 것을 결정할 수 있다.

[172] 1005 단계에서, UE 510은 등록 요청 메시지를 기지국으로 송신한다. 다시 말해서, 사설 네트워크 1010을 선택한 단말은 사설 네트워크 1010에 접속하기 위해 등록 절차를 수행할 수 있다. 예를 들어, UE 510 및 기지국은 RRC 연결 설정을 수행하고, UE 510은 RRC를 통해 등록 요청 메시지를 기지국으로 송신할 수 있다. UE 510은 등록 요청 메시지에서 등록 유형을 초기 등록 또는 이동성 등록으로 설정할 수 있고, 등록 요청 메시지는 사설 네트워크 1010에 대한 등록을 지시하기 위해 사설 네트워크 1010의 식별 정보 및 UE 510의 ID 중

적어도 하나를 포함할 수 있다. 예를 들어, 사설 네트워크 1010의 식별 정보는 MCC, MNC 및 PN ID의 조합으로 표현될 수 있다. 다른 예로, 등록 요청 메시지는 사설 네트워크 1010의 식별 정보 대신 UE 1010이 사설 네트워크 1010에 대한 접속을 시도함을 지시하는 사설 네트워크 접속 지시자를 포함할 수 있다. UE 510의 ID는, 예를 들어, 공용 네트워크 1020에 의해 할당된 임시 ID(예: GUTI)이거나, 공용 네트워크 1020에 의해 할당된 가입자 ID(예: SUTI)일 수 있다. 다양한 실시 예들에서, 등록 요청 메시지는 사설 네트워크 1010의 가입자에 대해 할당된 가입자 ID인 사설 네트워크 UE ID를 더 포함하거나, 임시 ID 대신 포함할 수 있다. 다양한 실시 예들에서, 사설 네트워크 UE ID 대신, UE 510이 가입된 공용 네트워크에서 할당된 가입자 ID인 SUPI로서, 암호화되지 아니한 SUPI가 UE 510의 ID로 사용될 수 있다. 뿐만 아니라, UE 510과 사설 네트워크 1010 사이에서 공유되는 암호화 규칙에 따라 UE 510이 가입된 공용 네트워크에서 할당된 가입자 ID인 SUPI로서, 암호화된 SUPI가 UE 510의 ID로 사용될 수 있다.

[173] 1007 단계에서, 기지국은 등록 요청 메시지를 AMF 560b로 전달한다. 기지국은 UE 510으로부터 수신된 등록 요청 메시지로부터 사설 네트워크 1010의 식별 정보를 식별하고, 식별 정보에 대응하는 사설 네트워크 1010의 코어 네트워크에 포함된 AMF 560b로 전달할 수 있다. 기지국은 N2 메시지를 통해 등록 요청 메시지를 AMF 560b로 전달할 수 있고, 전달되는 메시지는 등록 유형이 초기 등록 또는 이동성 등록임을 지시하는 정보, 사설 네트워크 1010의 식별 정보, 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다.

[174] 1009 단계에서, AMF 560b는 공용 네트워크 1020에 대한 등록이 허용되지 아니함을 결정한다. AMF 560b는 UE 510에 대한 접속 관리가 사설 네트워크 1010에서 뿐만 아니라 공용 네트워크 1020에서도 수행되어야 하는지를 결정할 수 있다. AMF 560b는 등록 요청 메시지에 포함된 식별 정보들(즉, 등록 유형이 이동성 등록 또는 초기 등록임을 지시하는 정보, 사설 네트워크 1010의 식별 정보, UE 510의 ID 및/또는 사설 네트워크 UE ID) 중 적어도 하나에 기반하여 UE 510이 접속을 시도하는 사설 네트워크 1010이 UE 510가 가입되지 아니한 공용 네트워크 1020의 사업자에 의해 관리됨을 식별하고, 공용 네트워크 1020이 로밍 네트워크도 아닌 경우, AMF 560b는 UE 510의 사설 네트워크 1010에 대한 등록이 요구되고, UE 510이 가입되어 있지 아니한 공용 네트워크 1020에 대한 등록은 허용되지 아니함을 결정할 수 있다.

[175] 사설 네트워크 1010과 사업자가 동일한 공용 네트워크 1020에 대해 접속이 허용되지 아니할 경우, 1011 단계 및 1013단계가 수행될 수 있다.

[176] 1011 단계에서, AMF 560b는 이동성 등록에 대한 등록 거절(registration reject) 메시지를 UE 510으로 전달한다. 예를 들어, AMF 560b는 UE 510이 이동성 등록을 시도한 경우, UE 510에 '이유= "공용 네트워크에 대한 접속이 허용되지 아니함"(cause= "access to the public network is not allowed")'와 같이 표현되는 정보를 포함하는 등록 거절 메시지를 전달할 수 있다. UE 510이 등록 거절

메시지를 수신한 후, UE 510은 사설 네트워크 1010에 대한 초기 등록을 시도하도록 트리거(trigger)될 수 있다.

[177] 1013 단계에서, AMF 560b는 UE 510에 사설 네트워크 1010에 대한 UE 510의 ID를 요청하고, 그에 대한 응답으로 UE 510으로부터 UE 510의 ID를 수신할 수 있다. 예를 들어, AMF 560b는 UE 510으로부터 UE 510이 사설 네트워크 1010에서 사용할 수 있는 UE 510의 ID를 등록 메시지를 통해 획득하지 아니한 경우, AMF 560b는 UE 510에 사설 네트워크 1010에 대한 UE 510의 ID를 요청하고, 그에 대한 응답으로 UE 510으로부터 UE 510의 ID를 수신할 수 있다. UE 510의 ID를 요청하기 위한 요청 메시지는 사설 네트워크 1010에 대한 ID가 요청됨을 지시하기 위해 사설 네트워크 1010의 식별 정보를 포함할 수 있다.

[178] 도시되지 아니하였으나, 1011 단계 및 1013는 선택적으로 수행될 수 있다. 다시 말해서, 1011 단계 또는 1013 단계는 생략될 수 있다.

[179] 1015 단계에서, AMF 560b는 UE 컨텍스트를 수신한다. AMF 560b는 등록 요청 메시지에 포함된 UE 510의 ID(예: GUTI 및/또는 SUTI)를 이용하여, 공용 네트워크 1020의 AMF 580b로부터 공용 네트워크 1020에 이미 등록된 UE 컨텍스트 정보를 가져올 수 있다.

[180] AMF 560b는 UE 510의 사설 네트워크 1010에 대한 인증을 수행하고, 사설 네트워크 1010의 UDM 560f를 통해 UE의 사설 네트워크 1010의 이용에 대한 가입 정보를 획득하여 UE 510의 사설 네트워크 1010의 이용에 대한 유효성을 검사하는 허가 절차를 수행하고, 사설 네트워크 1010의 UDM 560f에 UE 510의 등록 정보를 갱신할 수 있다. 이를 위한 AMF 560b의 동작들은 후술하는 단계들을 통해 수행될 수 있다.

[181] 1017 단계에서, AMF 560b는 로컬 AUSF를 선택한다. 다양한 실시 예들에서, 로컬 AUSF는 사설 네트워크 1010의 AUSF(예: AUSF 560c)일 수 있다. AMF 560b가 사설 네트워크 1010에서 UE 510에 대한 인증을 수행할 때, AMF 560b는 AUSF 560c를 선택할 수 있다. 예를 들어, AMF 560b가 사설 네트워크 1010의 이용을 위한 별도의 인증을 수행하는 경우, AMF 560b는 사설 네트워크 1010의 AUSF들 중에서 사설 네트워크 1010에 가입된 UE에 대한 인증을 지원하는 AUSF를 선택할 수 있다.

[182] 1019 단계에서, AMF 560b는 선택된 AUSF 560c에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 1021 단계에서, AMF 560b는 UE 510에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 다양한 실시 예들에서, 1019 단계는 1021 단계보다 먼저 수행되거나, 나중에 수행되거나, 또는 동시에 수행될 수 있다.

[183] 1023 단계에서, AMF 560b는 로컬 UDM(예: UDM 560f)을 선택한다. AMF 560b는 사설 네트워크 1010에서 UE의 가입 정보 및/또는 등록 정보를 관리하는 UDM 560f를 선택할 수 있다.

[184] 1025 단계에서, AMF 560b는 UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 560f에 갱신할 수 있다.

[185] 1027 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 560f로부터 UE 510에 대한 사설 네트워크 1010의 가입 정보를 가져올 수 있다.

[186] 1029 단계에서, AMF 560b는 가입 데이터에 의해 사설 네트워크 1010에 UE 510의 유효성을 검사한다. 다시 말해서, AMF 560b는 사설 네트워크 1010으로부터 획득된 가입 데이터에 기반하여 사설 네트워크 1010에 대한 UE 510의 유효성을 검사할 수 있다. UDM 560f로부터 사설 네트워크 1010에 대한 UE 510의 가입 정보를 획득한 AMF 560b는 가입 정보에 기반하여 사설 네트워크 1010의 이용에 대한 유효성을 검사하는 허가 절차를 수행할 수 있다.

[187] 1031 단계에서, AMF 560b는 매크로 UDM(예: UDM 580f)을 선택한다. AMF 560b는 허가된 UE 510에 대해 UE 510이 가입된 공용 네트워크 1020의 UDM 580f를 검색하고, 검색된 UDM 580f를 선택할 수 있다.

[188] 1033 단계에서, AMF 560b는 UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 560b는 UE 510의 등록 정보를 UDM 580f에 갱신할 수 있다.

[189] 1035 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 UDM 580f로부터 UE 510에 대한 사설 네트워크 1010의 가입 정보를 가져올 수 있다.

[190] 1037 단계에서, AMF 560b는 나머지 등록 절차를 수행한다. 예를 들어, AMF 560b는 UE 510의 등록을 위한 허가 및 인증 절차를 수행한 후, 허가 및 인증의 결과에 따라 UE 510에 등록 승인 메시지를 전달할 수 있다(허가 및 인증이 성공적인 경우). 등록 승인 메시지는 UE 510이 사설 네트워크 1010에 성공적으로 등록되었음을 지시하는 정보와, 공용 네트워크 1020에 성공적으로 등록되었음을 지시하는 정보를 포함할 수 있다. 예를 들어, 등록 승인 메시지는 '등록 결과="공용 네트워크 및 사설 네트워크 모두에 등록됨"(registration result = "registered to both public and private network")'과 같이 표현되는 정보를 포함할 수 있다. 다양한 실시 예들에서, 등록 승인 메시지는 UE 510이 사설 네트워크 1010에 성공적으로 등록되었음을 지시하는 정보를 포함할 수 있다. 예를 들어, 등록 승인 메시지는 '등록 결과="사설 네트워크에만 등록됨"(registration result = "registered to private network only")'과 같이 표현되는 정보를 포함할 수 있다.

[191] 도 11은 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 유형 B 사설 네트워크에 등록하기 위한 신호 흐름을 도시한다. 도 11에서, UE 510은 공용 네트워크 1120에 접속 및/또는 등록되어 공용 네트워크 1120에 의해 서비스되거나, 공용 네트워크 1120에 접속되어 있지 않음이 가정되고, 사설 네트워크 1110은 유형 B 사설 네트워크를 포함할 수 있다.

[192] 도 11을 참고하면, 1101 단계에서, 사설 네트워크 1110의 기지국(RAN 530a에 포함됨)은 UE 510으로 MCC, MNC 및 PN ID를 송신한다. 예를 들어, 기지국은 기지국이 서비스하는 사설 네트워크 1110의 식별 정보(즉, MCC, MNC 및 PN ID)를 SIB 메시지를 통해 방송할 수 있고, UE 510은 SIB 메시지에 포함된 MCC,

MNC 및 PN ID를 식별할 수 있다.

[193] 1103 단계에서, UE 510은 사설 네트워크 1110을 검출하고, 검출된 사설 네트워크 1110을 선택할 것을 결정할 수 있다. UE 510은 UE 510이 가입된 사설 네트워크 1110을 발견하고, 사설 네트워크 1110의 식별 정보들(즉, MCC, MNC, 및 PN ID) 중 적어도 하나에 기반하여 사설 네트워크 1110이 유형 B 사설 네트워크임을 식별하고, 사설 네트워크 1110을 선택할 것을 결정할 수 있다.

[194] 1105 단계에서, UE 510은 등록 요청 메시지를 기지국으로 송신한다. 다시 말해서, 사설 네트워크 1110을 선택한 단말은 사설 네트워크 1110에 접속하기 위해 등록 절차를 수행할 수 있다. 예를 들어, UE 510 및 기지국은 RRC 연결 설정을 수행하고, UE 510은 RRC를 통해 등록 요청 메시지를 기지국으로 송신할 수 있다. UE 510은 등록 요청 메시지에서 등록 유형을 초기 등록으로 설정할 수 있고, 등록 요청 메시지는 사설 네트워크 1110에 대한 등록을 지시하기 위해 사설 네트워크 1110의 식별 정보 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다. 예를 들어, 사설 네트워크 1110의 식별 정보는 MCC, MNC 및 PN ID의 조합으로 표현될 수 있다. 다른 예로, 등록 요청 메시지는 사설 네트워크 1110의 식별 정보 대신 UE 510이 사설 네트워크 1110에 대한 접속을 시도함을 지시하는 사설 네트워크 접속 지시자를 포함할 수 있다. UE 510의 ID는 사설 네트워크 1110의 가입자에 대해 할당된 가입자 ID인 사설 네트워크 UE ID를 포함할 수 있다. 다양한 실시 예들에서, 사설 네트워크 UE ID 대신, UE 510이 가입된 공용 네트워크에서 할당된 가입자 ID인 SUPI로서, 암호화되지 아니한 SUPI가 UE 510의 ID로 사용될 수 있다. 뿐만 아니라, UE 510과 사설 네트워크 1110 사이에서 공유되는 암호화 규칙에 따라 UE 510이 가입된 공용 네트워크에서 할당된 가입자 ID인 SUPI로서, 암호화된 SUPI가 UE 510의 ID로 사용될 수 있다.

[195] 1107 단계에서, 기지국은 등록 요청 메시지를 AMF 530b로 전달한다. 기지국은 UE 510으로부터 수신된 등록 요청 메시지로부터 사설 네트워크 1110의 식별 정보를 식별하고, 식별 정보에 대응하는 사설 네트워크 1110의 코어 네트워크에 포함된 AMF 530b로 전달할 수 있다. 기지국은 N2 메시지를 통해 등록 요청 메시지를 AMF 530b로 전달할 수 있고, 전달되는 메시지는 등록 유형이 초기 등록임을 지시하는 정보, 사설 네트워크 1110의 식별 정보, 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다.

[196] 1109 단계에서, AMF 530b는 공용 네트워크 1120에 대한 등록이 허용되지 아니함을 결정한다. AMF 530b는 UE 510에 대한 접속 관리가 사설 네트워크 1110에서 뿐만 아니라 공용 네트워크 1120에서도 수행되어야 하는지를 결정할 수 있다. AMF 530b는 UE 510이 접속을 시도하는 사설 네트워크 1110이 유형 B 사설 네트워크임을 식별하고, 이 경우 AMF 530b는 UE 510의 사설 네트워크 1110에 대한 등록이 요구되고, 공용 네트워크 1120에 대한 등록은 허용되지 아니함을 결정할 수 있다.

[197] 1111 단계에서, AMF 530b는 이동성 등록에 대한 등록 거절 메시지를 UE

510으로 전달한다. 예를 들어, AMF 530b는 UE 510이 이동성 등록을 시도한 경우, UE 510에 '이유= "공용 네트워크에 대한 접속이 허용되지 아니함"(cause= "access to the public network is not allowed")'와 같이 표현되는 정보를 포함하는 등록 거절 메시지를 전달할 수 있다. UE 510이 등록 거절 메시지를 수신한 후, UE 510은 사설 네트워크 1110에 대한 초기 등록을 시도하도록 트리거될 수 있다.

[198] AMF 530b는 UE 510의 사설 네트워크 1110에 대한 인증을 수행하고, 사설 네트워크 1110의 UDM 530f를 통해 UE의 사설 네트워크 1110의 이용에 대한 가입 정보를 획득하여 UE 510의 사설 네트워크 1110의 이용에 대한 유효성을 검사하는 허가 절차를 수행할 수 있다. 이를 위한 AMF 530b의 동작들은 후술하는 단계들을 통해 수행될 수 있다.

[199] 1113 단계에서, AMF 530b는 로컬 AUSF를 선택한다. 다양한 실시 예들에서, 로컬 AUSF는 사설 네트워크 1110의 AUSF(예: AUSF 530c)일 수 있다. AMF 530b가 사설 네트워크 1110에서 UE 510에 대한 인증을 수행할 때, AMF 530b는 AUSF 530c를 선택할 수 있다. 예를 들어, AMF 530b가 사설 네트워크 1110의 이용을 위한 별도의 인증을 수행하는 경우, AMF 530b는 사설 네트워크 1110의 AUSF들 중에서 사설 네트워크 1110에 가입된 UE에 대한 인증을 지원하는 AUSF를 선택할 수 있다.

[200] 1115 단계에서, AMF 530b는 선택된 AUSF 530c에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 1117 단계에서, AMF 530b는 UE 510에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 다양한 실시 예들에서, 1115 단계는 1117 단계보다 먼저 수행되거나, 나중에 수행되거나, 또는 동시에 수행될 수 있다.

[201] 1119 단계에서, AMF 530b는 로컬 UDM(예: UDM 530f)을 선택한다. AMF 530b는 사설 네트워크 1110에서 UE의 가입 정보 및/또는 등록 정보를 관리하는 UDM 530f를 선택할 수 있다.

[202] 1121 단계에서, AMF 530b는 UECM 등록 절차를 수행한다. UECM 등록 절차에서, AMF 530b는 UE 510의 등록 정보를 UDM 530f에 갱신할 수 있다.

[203] 1123 단계에서, AMF 530b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 530b는 UDM 530f로부터 UE 510에 대한 사설 네트워크 1110의 가입 정보를 가져올 수 있다.

[204] 1125 단계에서, AMF 530b는 가입 데이터에 의해 사설 네트워크 1110에 UE 510의 유효성을 검사한다. 다시 말해서, AMF 530b는 사설 네트워크 1110으로부터 획득된 가입 데이터에 기반하여 사설 네트워크 1110에 대한 UE 510의 유효성을 검사할 수 있다. UDM 530f로부터 사설 네트워크 1110에 대한 UE 510의 가입 정보를 획득한 AMF 530b는 가입 정보에 기반하여 사설 네트워크 1110의 이용에 대한 유효성을 검사하는 허가 절차를 수행할 수 있다.

[205] 1127 단계에서, AMF 530b는 나머지 등록 절차를 수행한다. 예를 들어, AMF 530b는 UE 510의 등록을 위한 허가 및 인증 절차를 수행한 후, 허가 및 인증의 결과에 따라 UE 510에 등록 승인메시지를 전달할 수 있다(허가 및 인증이

성공적인 경우).

[206] 도 12는 본 개시의 다양한 실시 예들에 따른 무선 통신 시스템에서 단말이 유형 A 사설 네트워크에 초기 등록하기 위한 신호 흐름을 도시한다. 도 12에서, 사설 네트워크 1210은 유형 A 사설 네트워크를 포함할 수 있다.

[207] 도 12를 참고하면, 1201 단계에서, 사설 네트워크 1210의 기지국(RAN 560a에 포함됨)은 UE 510으로 MCC, MNC 및 PN ID를 송신한다. 예를 들어, 기지국은 기지국이 서비스하는 사설 네트워크 1210의 식별 정보(즉, MCC, MNC 및 PN ID)를 SIB 메시지를 통해 방송할 수 있고, UE 510은 SIB 메시지에 포함된 MCC, MNC 및 PN ID를 식별할 수 있다.

[208] 1203 단계에서, UE 510은 사설 네트워크 1210을 검출하고, 검출된 사설 네트워크 1210을 선택할 것을 결정할 수 있다. UE 510은 UE 510이 가입된 사설 네트워크 1210을 발견하고, 사설 네트워크 1210의 식별 정보들(즉, MCC, MNC, 및 PN ID) 중 적어도 하나에 기반하여 사설 네트워크 1210이 UE 510이 가입된 공용 네트워크 1220의 사업자에 의해 관리되는 유형 A 사설 네트워크임을 식별하고, 사설 네트워크 1210을 선택할 것을 결정할 수 있다.

[209] 1205 단계에서, UE 510은 등록 요청 메시지를 기지국으로 송신한다. 다시 말해서, 사설 네트워크 1210을 선택한 단말은 사설 네트워크 1210에 접속하기 위해 등록 절차를 수행할 수 있다. 예를 들어, UE 510 및 기지국은 RRC 연결 설정을 수행하고, UE 510은 RRC를 통해 등록 요청 메시지를 기지국으로 송신할 수 있다. UE 510은 등록 요청 메시지에서 등록 유형을 초기 등록으로 설정할 수 있고, 등록 요청 메시지는 사설 네트워크 1210에 대한 등록을 지시하기 위해 사설 네트워크 1210의 식별 정보 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다. 예를 들어, 사설 네트워크 1210의 식별 정보는 MCC, MNC 및 PN ID의 조합으로 표현될 수 있다. 다른 예로, 등록 요청 메시지는 사설 네트워크 1210의 식별 정보 대신 UE 510이 사설 네트워크 1210에 대한 접속을 시도함을 지시하는 사설 네트워크 접속 지시자를 포함할 수 있다. UE 510의 ID는, 예를 들어, 공용 네트워크 1220에 의해 할당된 임시 ID(예: GUTI(globally unique temporary identifier))이거나, 공용 네트워크 1220에 의해 할당된 가입자 ID(예: SUTI(subscriber unique temporary identifier))일 수 있다. 다양한 실시 예들에서, 등록 요청 메시지는 사설 네트워크 1210의 가입자에 대해 할당된 가입자 ID인 사설 네트워크 UE ID를 더 포함할 수 있다.

[210] 1207 단계에서, 기지국은 등록 요청 메시지를 AMF 560b로 전달한다. 기지국은 UE 510으로부터 수신된 등록 요청 메시지로부터 사설 네트워크 1210의 식별 정보를 식별하고, 식별 정보에 대응하는 사설 네트워크 1210의 코어 네트워크에 포함된 AMF 560b로 전달할 수 있다. 기지국은 N2 메시지를 통해 등록 요청 메시지를 AMF 560b로 전달할 수 있고, 전달되는 메시지는 등록 유형이 초기 등록임을 지시하는 정보, 사설 네트워크 1210의 식별 정보, 및 UE 510의 ID 중 적어도 하나를 포함할 수 있다.

[211] 1209 단계에서, AMF 560b는 공용 네트워크 1220의 AUSF 580c에 의해 인증이 수행될 수 있음을 결정한다. 다시 말해서, 등록 요청 메시지를 수신한 AMF 560b는, UE 510에 대한 인증이 공용 네트워크 1220의 AUSF 580c 및/또는 UDM 580f를 통해 수행될 수 있는지 여부를 결정한다. 예를 들어, UE 510이 접속을 시도하는 사설 네트워크 1210의 관리가 UE 510의 SUPI를 할당한 공용 네트워크 1220를 통해 수행됨을 AMF 560b가 UE 510으로부터의 등록 요청 메시지에 포함된 UE 510의 ID 및/또는 사설 네트워크 1210의 식별 정보에 기반하여 식별하거나, UE 510의 SUPI를 할당한 공용 네트워크 1220와 사설 네트워크 1210을 관리하는 공용 네트워크간 로밍 협약이 되어 있는 경우, AMF 560b는 UE 510에 대한 인증이 공용 네트워크 1220의 AUSF 580c 및/또는 UDM 580f를 통해 수행될 수 있다고 결정한다.

[212] 1211 단계에서, AMF 560b는 UE 컨텍스트(context)를 수신한다. AMF 560b는 등록 요청 메시지에 포함된 UE 510의 ID(예: GUTI 및/또는 SUTI)를 이용하여, 공용 네트워크 1220의 AMF 580b로부터 공용 네트워크 1220에 이미 등록된 UE 컨텍스트 정보를 가져올 수(retrieve) 있다.

[213] 다양한 실시 예들에서, AMF 560b는 등록 절차를 수행하는 동안, UE 510에 대한 인증이 공용 네트워크 1220의 AUSF 580c 및/또는 UDM 580f를 통해 수행될 수 있다고 결정한 경우, AMF 560b는 공용 네트워크의 AUSF 580c 및/또는 UDM 580f를 선택하고, 선택된 AUSF 580c 및/또는 UDM 580f을 통해 UE 510의 사설 네트워크 1210에 대한 인증을 수행한다.

[214] 즉, 1209 단계에서 UE 510에 대한 인증이 공용 네트워크의 AUSF 580c 및/또는 UDM 560f를 통해 수행될 수 있다고 결정한 AMF 560b는, 1213 단계에서, 매크로 AUSF를 선택한다. 다양한 실시 예들에서, 매크로 AUSF는 공용 네트워크 1220의 AUSF(예: AUSF 580c)일 수 있다. 예를 들어, 사설 네트워크 1210의 이용을 위한 인증이 요구되는 경우, AMF 560b는 공용 네트워크 1220의 AUSF들 중에서 사설 네트워크 810에 가입된 UE에 대한 인증을 지원하는 AUSF를 사설 네트워크 1210의 식별 정보를 이용하여 선택할 수 있다. 사설 네트워크 1210의 식별 정보는, MCC, MNC 및 PN ID 중 적어도 하나, 또는 MCC, MNC 및 PN ID 중 적어도 둘의 조합으로 표현될 수 있다. 또는, AMF 560b는 UE 510과 같이 공용 네트워크 1220에 적합한(suitable for) AUSF를 검색하기 위해, 공용 네트워크 1220의 식별 정보(즉, MCC, MNC 중 적어도 하나)를 이용할 수 있다.

[215] 1215 단계에서, AMF 560b는 UE 510에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 1217 단계에서, AMF 560b는 매크로 AUSF 580c에 대한 인증 절차 및/또는 보안 절차를 수행할 수 있다. 다양한 실시 예들에서, 815 단계는 817 단계보다 먼저 수행되거나, 나중에 수행되거나, 또는 동시에 수행될 수 있다. 사설 네트워크 1210의 정책에 따라, 1215 단계 및/또는 1217 단계는 생략될 수 있다.

[216] 다양한 실시 예들에서, 사설 네트워크 1210의 이용에 대한 가입 정보가 공용

네트워크 1220의 UDM 580f에서 관리되는지(대안 1), 또는 사설 네트워크 1210의 UDM 560f에서 관리되는지(대안 2)는 사설 네트워크 1210을 관리하는 공용 네트워크 1220의 사업자 정책에 따라 결정될 수 있다. 따라서, AMF 560이 인증을 위한 UDM을 검색하는 경우, AMF 560b는 사설 네트워크 1210의 식별 정보를 참고할 수 있다. 다시 말해서, AMF 560b는 사설 네트워크 1210의 식별 정보(즉, MCC, MNC, PN IO 중 적어도 하나 또는 적어도 둘의 조합)에 기반하여, 인증을 위한 UDM을 검색할 수 있다.

[217] 대안 1과 같이, 사설 네트워크 1210의 이용에 대한 가입 정보가 공용 네트워크 1220의 UDM 580f에서 관리되는 경우, 1219 단계에서, AMF 560b는 매크로 UDM을 선택한다. 다양한 실시 예들에서, 매크로 UDM은 공용 네트워크 1220의 UDM(예: UDM 580f)일 수 있다. AMF 560b는 사설 네트워크 1210의 식별 정보에 기반하여, 사설 네트워크 1210에 대한 가입 정보를 관리하는 UDM 580f를 검색하고, 이를 선택할 수 있다.

[218] 1221 단계에서, AMF 560b는 UECM 등록 절차를 수행한다. 사설 네트워크 1210의 이용에 대한 가입 정보를 공용 네트워크 1220의 UDM 580f가 관리하는 경우, UECM 등록 절차에서, AMF 560b는 공용 네트워크 1220의 UDM 580f에 UE 510의 등록 정보를 갱신할 수 있다.

[219] 1223 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 공용 네트워크 1220의 UDM 580f로부터 사설 네트워크 1210에 대한 UE 510의 가입 정보를 획득할 수 있다.

[220] 대안 2과 같이, 사설 네트워크 1210의 이용에 대한 가입 정보가 사설 네트워크 1210의 UDM 560f에서 관리되는 경우, 1225 단계에서, AMF 560b는 로컬 UDM을 선택한다. 다양한 실시 예들에서, 로컬 UDM은 사설 네트워크 810의 UDM(예: UDM 560f)일 수 있다. AMF 560b는 사설 네트워크 1210의 식별 정보에 기반하여, 사설 네트워크 1210에 대한 가입 정보를 관리하는 UDM 560f를 검색하고, 이를 선택할 수 있다.

[221] 1227 단계에서, AMF 560b는 UECM 등록 절차를 수행한다. 사설 네트워크 1210의 이용에 대한 가입 정보를 사설 네트워크 1210의 UDM 560f가 관리하는 경우, UECM 등록 절차에서, AMF 560b는 사설 네트워크 1210의 UDM 560f에 UE 510의 등록 정보를 갱신할 수 있다.

[222] 1229 단계에서, AMF 560b는 SDM 획득 절차를 수행한다. SDM 획득 절차에서, AMF 560b는 사설 네트워크 1220의 UDM 560f로부터 사설 네트워크 1210에 대한 UE 510의 가입 정보를 획득할 수 있다.

[223] 1231 단계에서, AMF 560b는 가입 데이터에 의해 사설 네트워크 1210에 대한 UE 유효성 검사를 수행한다. AMF 560b는 사설 네트워크 1210의 이용에 대한 가입 정보를 공용 네트워크 1220의 UDM 580f로부터 획득하거나(대안 1), 사설 네트워크 1210의 UDM 560f로부터 획득하여(대안 2), UE 510의 사설 네트워크 1210의 이용에 대한 유효성을 체크하는 허가(authorization) 절차를 수행할 수

있다

[224] 1233 단계에서, AMF 560b는 나머지 등록 절차를 수행한다. 예를 들어, AMF 560b는 UE 510의 등록을 위한 허가 및 인증 절차를 수행한 후, 허가 및 인증의 결과에 따라 UE 510에 등록 승인(registration accept) 메시지를 전달할 수 있다(허가 및 인증이 성공적인 경우). 등록 승인 메시지는 UE 510이 사설 네트워크 810에 성공적으로 등록되었음을 지시하는 정보와, 공용 네트워크 820에 성공적으로 등록되었음을 지시하는 정보를 포함할 수 있다. 예를 들어, 등록 승인 메시지는 '등록 결과="공용 네트워크 및 사설 네트워크 모두에 등록됨"(registration result = "registered to both public and private network")'과 같이 표현되는 정보를 포함할 수 있다.

[225] 본 개시의 청구항 또는 명세서에 기재된 실시 예들에 따른 방법들은 하드웨어, 소프트웨어, 또는 하드웨어와 소프트웨어의 조합의 형태로 구현될(implemented) 수 있다.

[226] 소프트웨어로 구현하는 경우, 하나 이상의 프로그램(소프트웨어 모듈)을 저장하는 컴퓨터 판독 가능 저장 매체가 제공될 수 있다. 컴퓨터 판독 가능 저장 매체에 저장되는 하나 이상의 프로그램은, 전자 장치(device) 내의 하나 이상의 프로세서에 의해 실행 가능하도록 구성된다(configured for execution). 하나 이상의 프로그램은, 전자 장치로 하여금 본 개시의 청구항 또는 명세서에 기재된 실시 예들에 따른 방법들을 실행하게 하는 명령어(instructions)를 포함한다.

[227] 이러한 프로그램(소프트웨어 모듈, 소프트웨어)은 랜덤 액세스 메모리 (random access memory), 플래시(flash) 메모리를 포함하는 불휘발성(non-volatile) 메모리, 롬(read only memory, ROM), 전기적 삭제가능 프로그램가능 롬(electrically erasable programmable read only memory, EEPROM), 자기 디스크 저장 장치(magnetic disc storage device), 컴팩트 디스크 롬(compact disc-ROM, CD-ROM), 디지털 다목적 디스크(digital versatile discs, DVDs) 또는 다른 형태의 광학 저장 장치, 마그네틱 카세트(magnetic cassette)에 저장될 수 있다. 또는, 이들의 일부 또는 전부의 조합으로 구성된 메모리에 저장될 수 있다. 또한, 각각의 구성 메모리는 다수 개 포함될 수도 있다.

[228] 또한, 프로그램은 인터넷(Internet), 인트라넷(Intranet), LAN(local area network), WAN(wide area network), 또는 SAN(storage area network)과 같은 통신 네트워크, 또는 이들의 조합으로 구성된 통신 네트워크를 통하여 접근(access)할 수 있는 부착 가능한(attachable) 저장 장치(storage device)에 저장될 수 있다. 이러한 저장 장치는 외부 포트를 통하여 본 개시의 실시 예를 수행하는 장치에 접속할 수 있다. 또한, 통신 네트워크상의 별도의 저장장치가 본 개시의 실시 예를 수행하는 장치에 접속할 수도 있다.

[229] 상술한 본 개시의 구체적인 실시 예들에서, 개시에 포함되는 구성 요소는 제시된 구체적인 실시 예에 따라 단수 또는 복수로 표현되었다. 그러나, 단수 또는 복수의 표현은 설명의 편의를 위해 제시한 상황에 적합하게 선택된

것으로서, 본 개시가 단수 또는 복수의 구성 요소에 제한되는 것은 아니며, 복수로 표현된 구성 요소라 하더라도 단수로 구성되거나, 단수로 표현된 구성 요소라 하더라도 복수로 구성될 수 있다.

[230] 한편 본 개시의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 개시의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 개시의 범위는 설명된 실시 예에 국한되어 정해져서는 아니 되며 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

청구범위

[청구항 1] 무선 통신 시스템에서 코어 네트워크 객체(core network entity)의 동작 방법에 있어서,
사용자 장치(user equipment)로부터 획득된 등록 요청 메시지에서 사설 네트워크의 식별 정보를 획득하는 과정과,
상기 사설 네트워크의 식별 정보에 기반하여, 상기 UE에 대한 인증을 지원하는 AUSF(authentication server function)를 선택하는 과정과,
상기 AUSF 및 상기 UE에 대한 인증 절차를 수행함에 대응하여, 상기 UE의 가입 정보 및 등록 정보를 관리하는 UDM(unified data management)을 선택하는 과정과,
상기 UDM으로부터 상기 사설 네트워크에 대한 상기 UE의 가입 정보를 획득하는 과정과,
상기 UE의 가입 정보에 기반하여, 상기 사설 네트워크에 대한 상기 UE의 유효성(validity) 검사를 수행하는 과정과,
상기 인증 절차 및 상기 유효성 검사의 결과에 기반하여, 상기 UE를 상기 사설 네트워크에 등록하는 과정을 포함하는 방법.

[청구항 2] 청구항 1에 있어서, 상기 사설 네트워크는, 공용 네트워크(public network)와 연동된 유형 A 사설 네트워크를 포함하는 방법.

[청구항 3] 청구항 2에 있어서, 상기 AUSF 및 상기 UDM은 상기 공용 네트워크에 포함되고,
상기 사설 네트워크에 포함된 로컬 UDM을 선택하는 과정과,
상기 로컬 UDM으로부터 상기 사설 네트워크에 대한 상기 UE의 가입 정보를 획득하는 과정을 더 포함하고,
상기 사설 네트워크에 대한 상기 UE의 유효성 검사를 수행하는 과정은,
상기 UDM으로부터 획득된 상기 UE의 가입 정보와, 상기 로컬 UDM으로부터 획득된 상기 UE의 가입 정보에 기반하여 상기 사설 네트워크에 대한 상기 UE의 유효성 검사를 수행하는 과정을 포함하는 방법.

[청구항 4] 청구항 2에 있어서, 상기 AUSF 및 상기 UDM은 상기 사설 네트워크에 포함되고,
상기 공용 네트워크에 포함된 매크로 UDM을 선택하는 과정과,
상기 매크로 UDM으로부터 상기 사설 네트워크에 대한 상기 UE의 가입 정보를 획득하는 과정을 더 포함하고,
상기 사설 네트워크에 대한 상기 UE의 유효성 검사를 수행하는 과정은,
상기 UDM으로부터 획득된 상기 UE의 가입 정보와, 상기 로컬 UDM으로부터 획득된 상기 UE의 가입 정보에 기반하여, 상기 사설 네트워크에 대한 상기 UE의 유효성 검사를 수행하는 과정을 포함하는

방법.

[청구항 5] 청구항 2에 있어서, 상기 등록 요청 메시지는, 상기 UE의 상기 공용 네트워크에 대한 접속이 완료된 후 미리 설정된 시간 이내에 송신되는 방법.

[청구항 6] 청구항 2에 있어서, 상기 등록 요청 메시지에 포함된 상기 UE의 식별자(identifier, ID) 및 상기 사설 네트워크의 식별 정보 중 적어도 하나에 기반하여 상기 공용 네트워크에 대한 상기 UE의 등록이 허용되지 아니함을 결정하는 과정과,
상기 UE의 상기 사설 네트워크에 대한 초기 등록을 트리거하기 위해, 상기 UE의 이동성 등록에 대한 등록 거절 메시지를 상기 UE로 전달하는 과정을 더 포함하는 방법.

[청구항 7] 청구항 2에 있어서, 상기 공용 네트워크에 대한 상기 UE의 등록이 허용되지 아니함을 결정하는 과정과,
상기 사설 네트워크에 대한 상기 UE의 식별자(identifier, ID)를 상기 UE에 요청하는 과정과,
상기 UE로부터 상기 UE의 ID를 획득하는 과정을 더 포함하는 방법.

[청구항 8] 청구항 1에 있어서, 상기 사설 네트워크는, 공용 네트워크(public network)와 연동되지 아니한 유형 B 사설 네트워크를 포함하고,
상기 등록 메시지에 포함된 상기 사설 네트워크의 식별 정보에 기반하여, 상기 유형 B 사설 네트워크를 식별하는 과정과,
상기 식별에 대응하여, 상기 공용 네트워크에 대한 상기 UE의 등록이 허용되지 아니함을 결정하는 과정과,
상기 UE의 상기 사설 네트워크에 대한 초기 등록을 트리거하기 위해, 상기 UE의 이동성 등록에 대한 등록 거절 메시지를 상기 UE로 전달하는 과정을 더 포함하는 방법.

[청구항 9] 무선 통신 시스템에서 코어 네트워크 객체(core network entity)의 장치에 있어서,
송수신기와,
상기 송수신기와 기능적으로 결합되고, 상기 송수신기를 제어하는 적어도 하나의 프로세서를 포함하고,
상기 적어도 하나의 프로세서는,
사용자 장치(user equipment)로부터 획득된 등록 요청 메시지에서 사설 네트워크의 식별 정보를 획득하고,
상기 사설 네트워크의 식별 정보에 기반하여, 상기 UE에 대한 인증을 지원하는 AUSF(authentication server function)를 선택하고,
상기 AUSF 및 상기 UE에 대한 인증 절차를 수행함에 대응하여, 상기 UE의 가입 정보 및 등록 정보를 관리하는 UDM(unified data management)을 선택하고,

상기 UDM으로부터 상기 사설 네트워크에 대한 상기 UE의 가입 정보를 획득하고,
상기 UE의 가입 정보에 기반하여, 상기 사설 네트워크에 대한 상기 UE의 유효성(validity) 검사를 수행하고,
상기 인증 절차 및 상기 유효성 검사의 결과에 기반하여, 상기 UE를 상기 사설 네트워크에 등록하도록 구성된 장치.

[청구항 10] 청구항 9에 있어서, 상기 사설 네트워크는, 공용 네트워크(public network)와 연동된 유형 A 사설 네트워크를 포함하는 장치.

[청구항 11] 청구항 10에 있어서, 상기 AUSF 및 상기 UDM은 상기 공용 네트워크에 포함되고,
상기 적어도 하나의 프로세서는, 상기 사설 네트워크에 포함된 로컬 UDM을 선택하고, 상기 로컬 UDM으로부터 상기 사설 네트워크에 대한 상기 UE의 가입 정보를 획득하고, 상기 UDM으로부터 획득된 상기 UE의 가입 정보와, 상기 로컬 UDM으로부터 획득된 상기 UE의 가입 정보에 기반하여 상기 사설 네트워크에 대한 상기 UE의 유효성 검사를 수행하도록 구성된 장치.

[청구항 12] 청구항 10에 있어서, 상기 AUSF 및 상기 UDM은 상기 사설 네트워크에 포함되고,
상기 적어도 하나의 프로세서는, 상기 공용 네트워크에 포함된 매크로 UDM을 선택하고, 상기 매크로 UDM으로부터 상기 사설 네트워크에 대한 상기 UE의 가입 정보를 획득하고, 상기 UDM으로부터 획득된 상기 UE의 가입 정보와, 상기 로컬 UDM으로부터 획득된 상기 UE의 가입 정보에 기반하여, 상기 사설 네트워크에 대한 상기 UE의 유효성 검사를 수행하도록 구성된 장치.

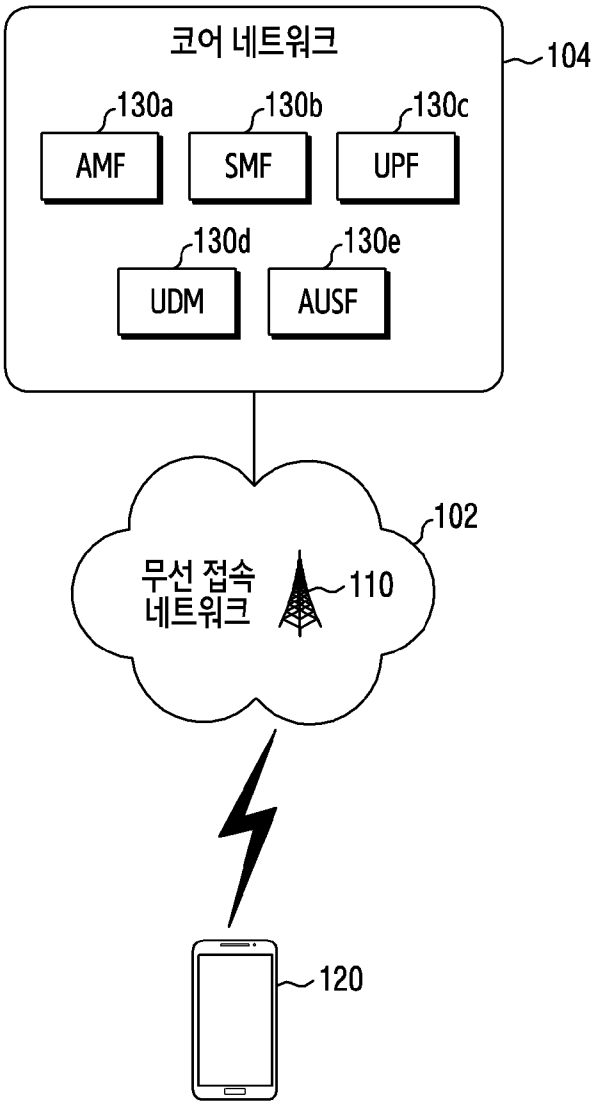
[청구항 13] 청구항 10에 있어서, 상기 적어도 하나의 프로세서는, 상기 등록 요청 메시지에 포함된 상기 UE의 식별자(identifier, ID) 및 상기 사설 네트워크의 식별 정보 중 적어도 하나에 기반하여 상기 공용 네트워크에 대한 상기 UE의 등록이 허용되지 아니함을 결정하고, 상기 UE의 상기 사설 네트워크에 대한 초기 등록을 트리거하기 위해, 상기 UE의 이동성 등록에 대한 등록 거절 메시지를 상기 UE로 전달하도록 구성된 장치.

[청구항 14] 청구항 10에 있어서, 상기 적어도 하나의 프로세서는, 상기 공용 네트워크에 대한 상기 UE의 등록이 허용되지 아니함을 결정하고, 상기 사설 네트워크에 대한 상기 UE의 식별자(identifier, ID)를 상기 UE에 요청하고, 상기 UE로부터 상기 UE의 ID를 획득하도록 구성된 장치.

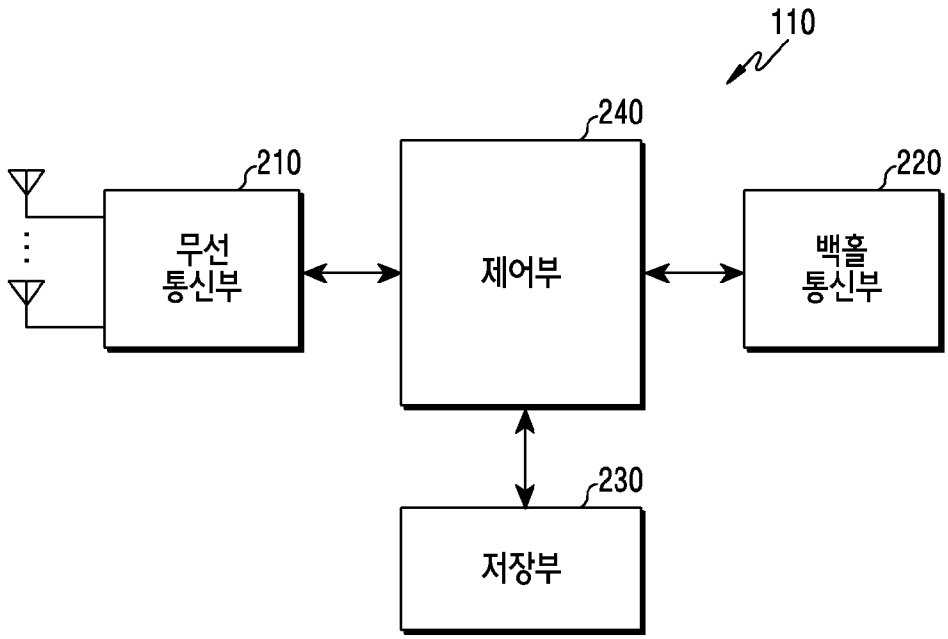
[청구항 15] 청구항 9에 있어서, 상기 사설 네트워크는, 공용 네트워크(public network)와 연동되지 아니한 유형 B 사설 네트워크를 포함하고,
상기 적어도 하나의 프로세서는,
상기 등록 메시지에 포함된 상기 사설 네트워크의 식별 정보에 기반하여,

상기 유형 B 사설 네트워크를 식별하고,
상기 식별에 대응하여, 상기 공용 네트워크에 대한 상기 UE의 등록이 허용되지 아니함을 결정하고,
상기 UE의 상기 사설 네트워크에 대한 초기 등록을 트리거하기 위해, 상기 UE의 이동성 등록에 대한 등록 거절 메시지를 상기 UE로 전달하도록 구성된 장치.

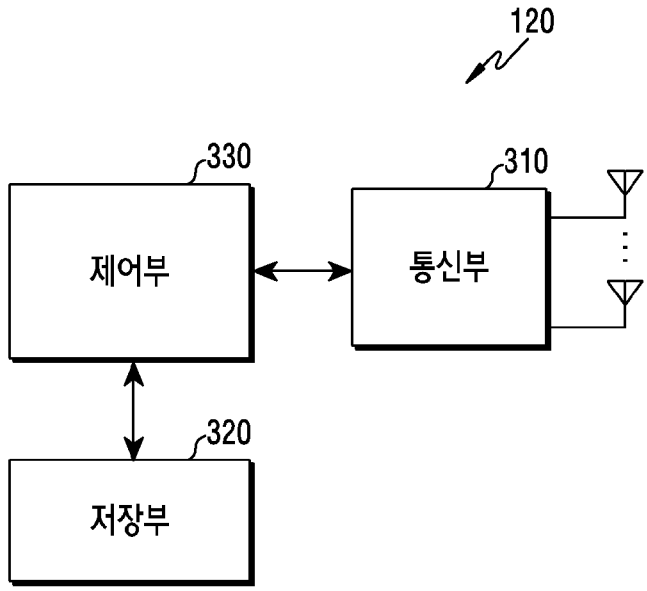
[도1]


코어 네트워크
104
130a
AMF
130b
SMF
130c
UPF
130d
UDM
130e
AUSF
102
무선 접속
네트워크
110
120

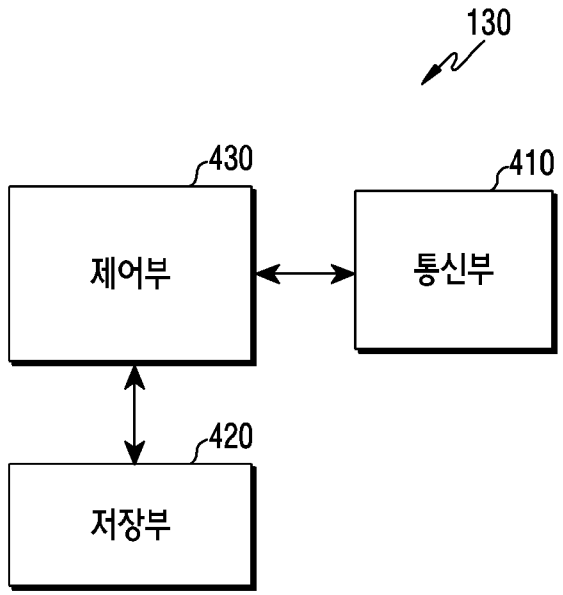
[도2]


110
240
210
220
무선
통신부
제어부
백홀
통신부
230
저장부

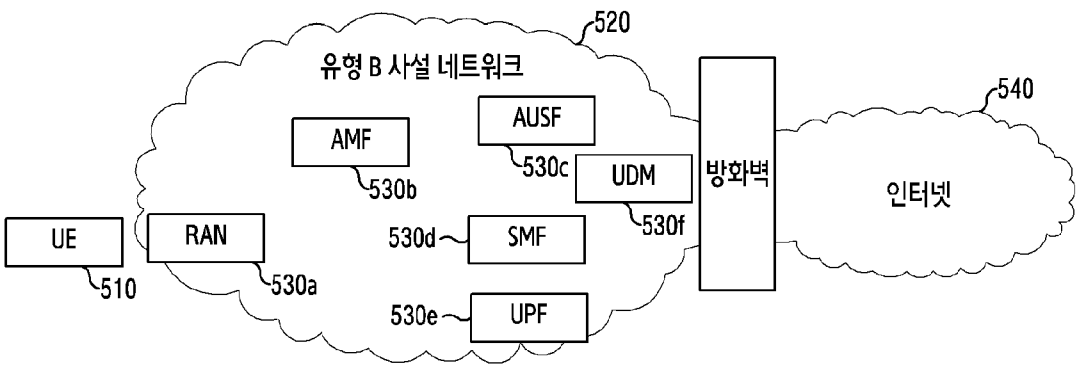
[도3]


120
330
310
제어부
통신부
320
저장부

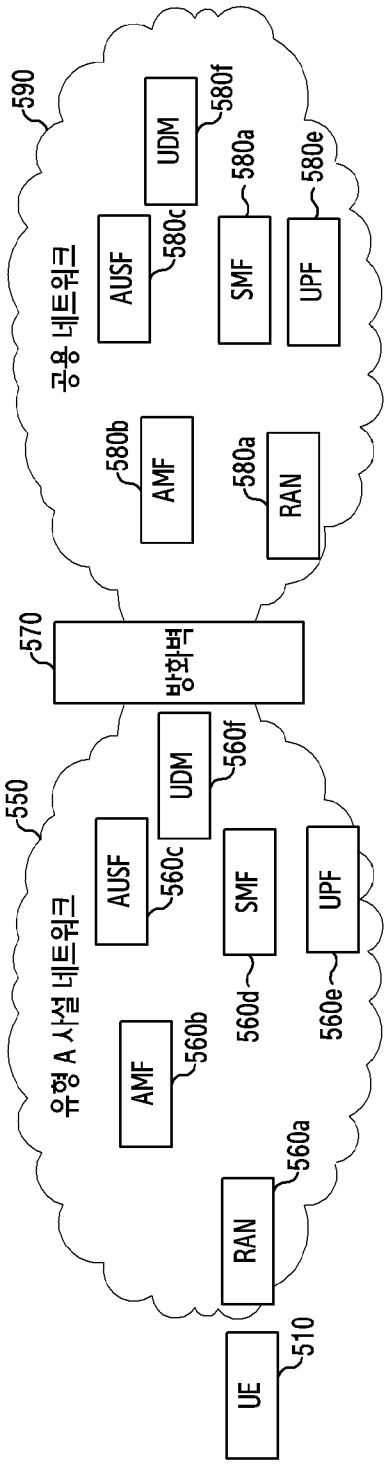
[도4]


130
430
410
제어부
통신부
420
저장부

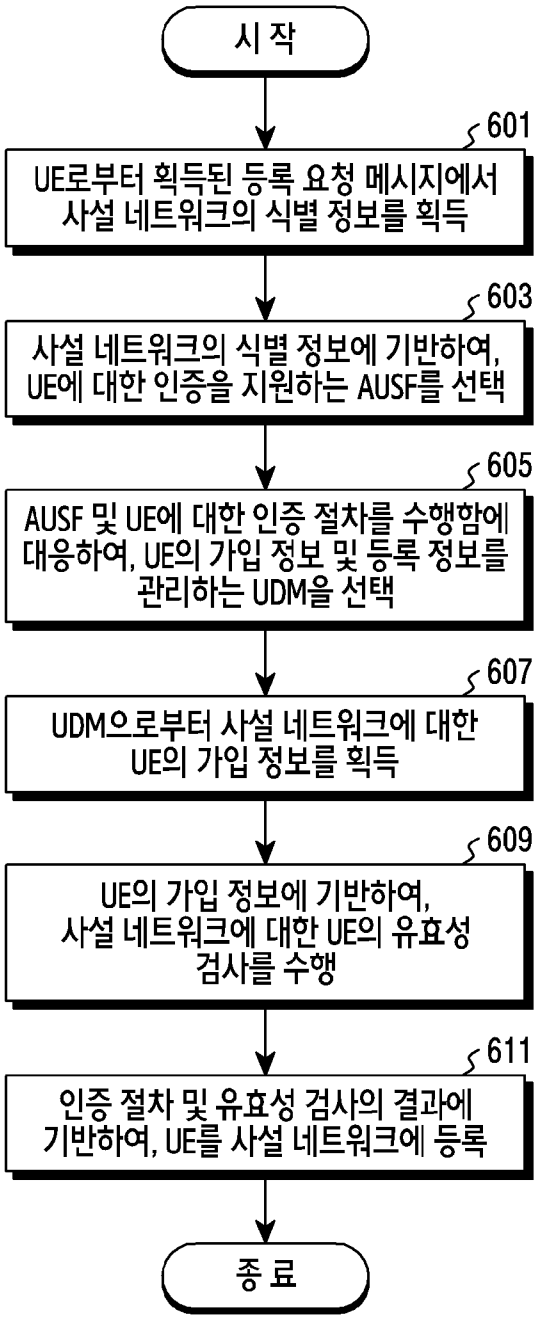
[도5a]


520
유형 B 사설 네트워크
AMF
530b
AUSF
530c
UDM
530f
530d
SMF
530e
UPF
UE
510
RAN
530a
방화벽
540
인터넷

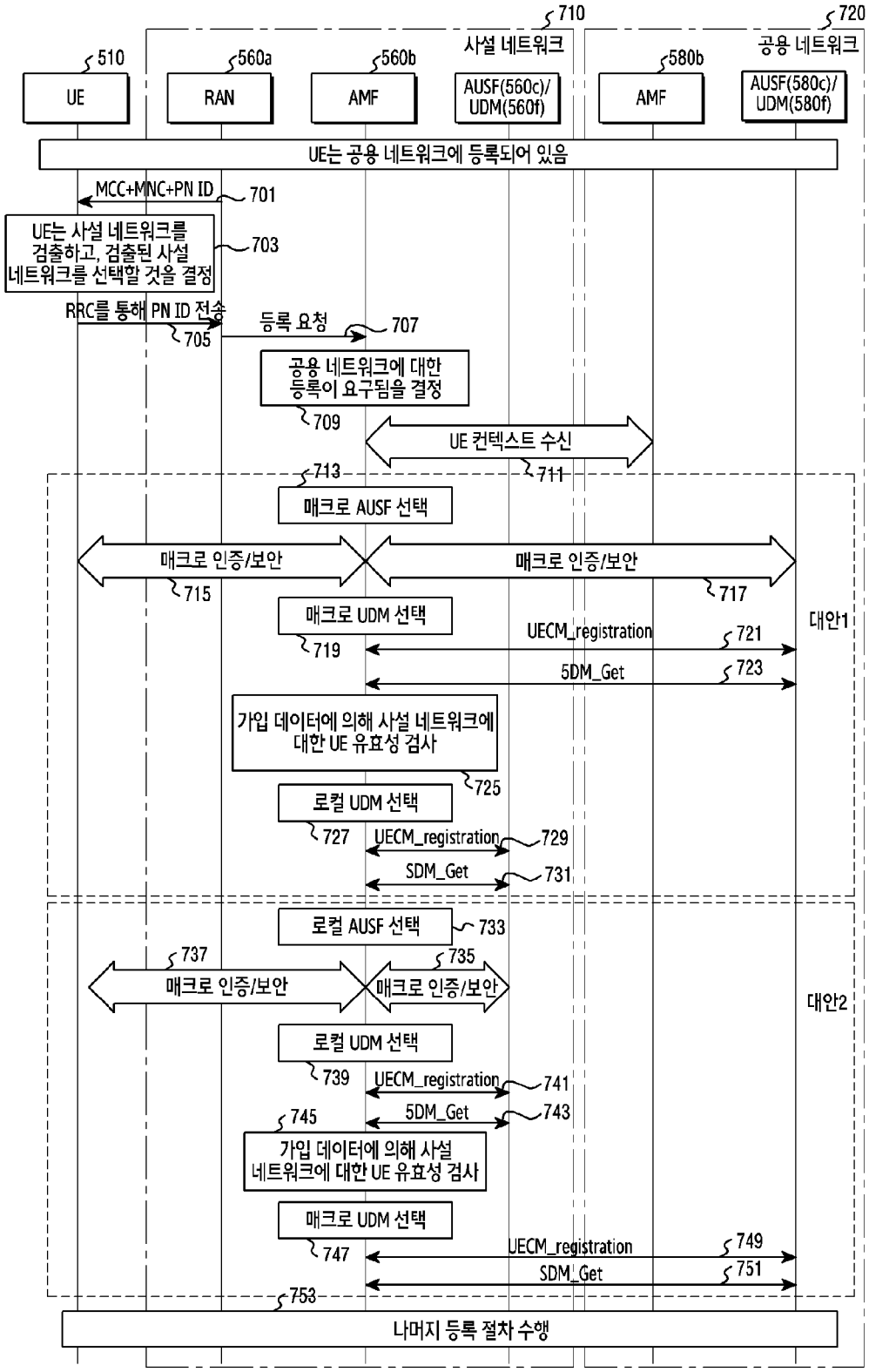
[도5b]


590
공용 네트워크
UDM
580f
AUSF
580c
SMF
580a
UPF
580e
AMF
580b
RAN
580a
570
방화벽
550
유형 A 사설 네트워크
UDM
560f
AUSF
560c
SMF
560d
UPF
560e
AMF
560b
RAN
560a
UE
510

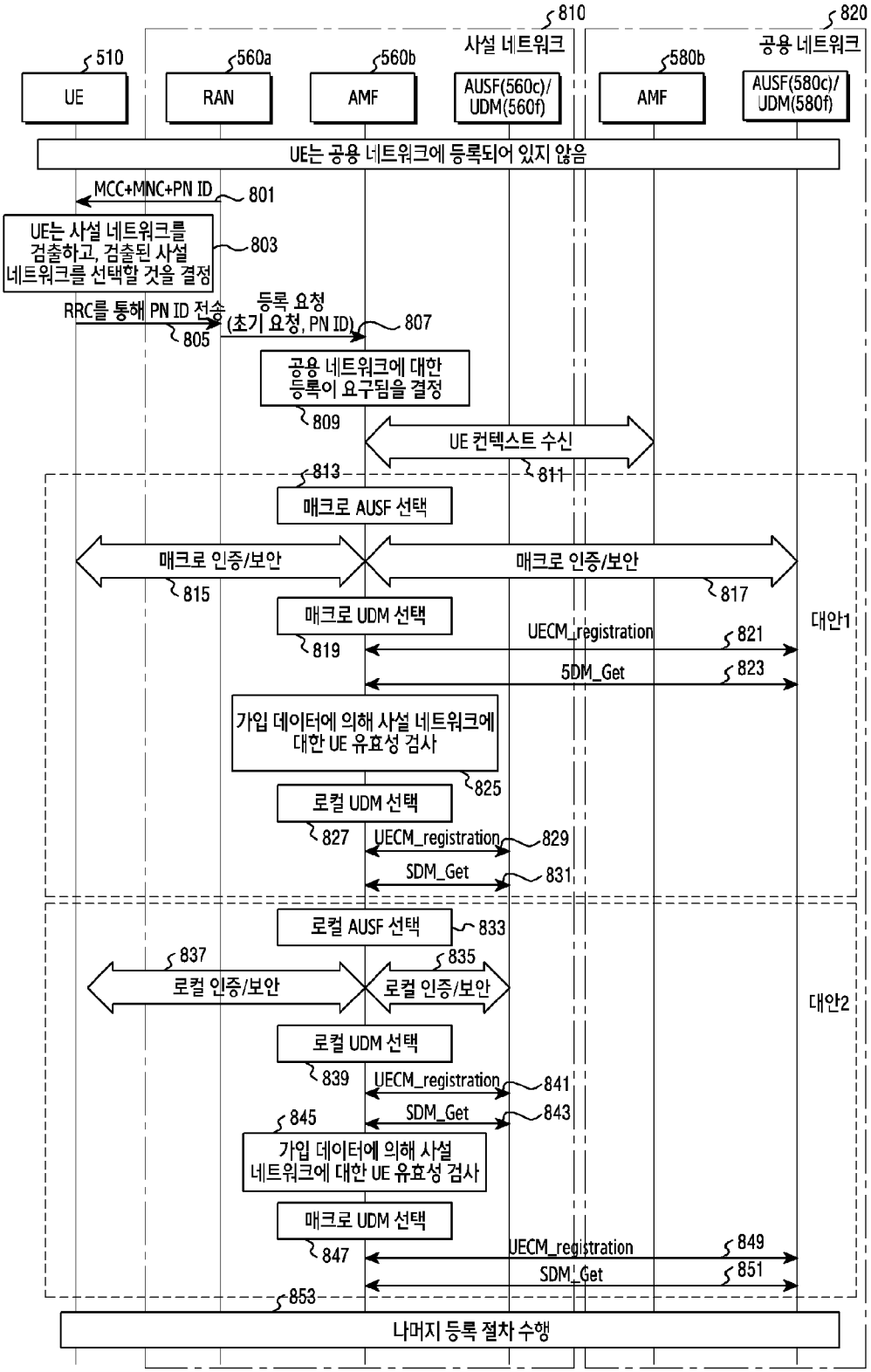
[도6]


시 작
601
UE로부터 획득된 등록 요청 메시지에서 사설 네트워크의 식별 정보를 획득
603
사설 네트워크의 식별 정보에 기반하여, UE에 대한 인증을 지원하는 AUSF를 선택
605
AUSF 및 UE에 대한 인증 절차를 수행함에 대응하여, UE의 가입 정보 및 등록 정보를 관리하는 UDM을 선택
607
UDM으로부터 사설 네트워크에 대한 UE의 가입 정보를 획득
609
UE의 가입 정보에 기반하여, 사설 네트워크에 대한 UE의 유효성 검사를 수행
611
인증 절차 및 유효성 검사의 결과에 기반하여, UE를 사설 네트워크에 등록
종 료

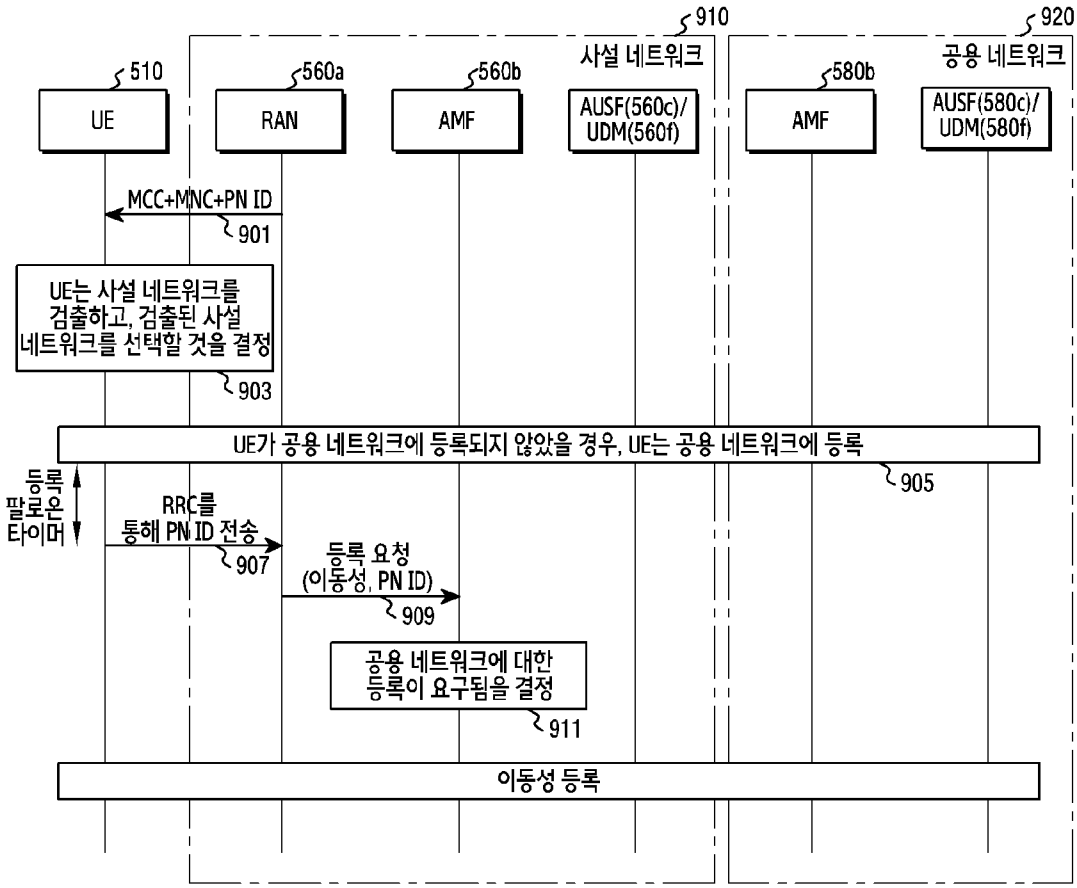
[도7]


710
720
사설 네트워크
공용 네트워크
510
560a
560b
580b
UE
RAN
AMF
AUSF(560c)/ UDM(560f)
AMF
AUSF(580c)/ UDM(580f)
UE는 공용 네트워크에 등록되어 있음
MCC+MNC+PN ID
701
UE는 사설 네트워크를 검출하고, 검출된 사설 네트워크를 선택할 것을 결정
703
RRC를 통해 PN ID 전송
705
등록 요청
707
공용 네트워크에 대한 등록이 요구됨을 결정
709
UE 컨텍스트 수신
711
713
매크로 AUSF 선택
매크로 인증/보안
715
매크로 인증/보안
717
매크로 UDM 선택
719
UECM_registration
721
5DM_Get
723
대안1
가입 데이터에 의해 사설 네트워크에 대한 UE 유효성 검사
725
로컬 UDM 선택
727
UECM_registration
729
SDM_Get
731
로컬 AUSF 선택
733
737
매크로 인증/보안
735
매크로 인증/보안
대안2
로컬 UDM 선택
739
UECM_registration
741
745
5DM_Get
743
가입 데이터에 의해 사설 네트워크에 대한 UE 유효성 검사
매크로 UDM 선택
747
UECM_registration
749
SDM_Get
751
753
나머지 등록 절차 수행

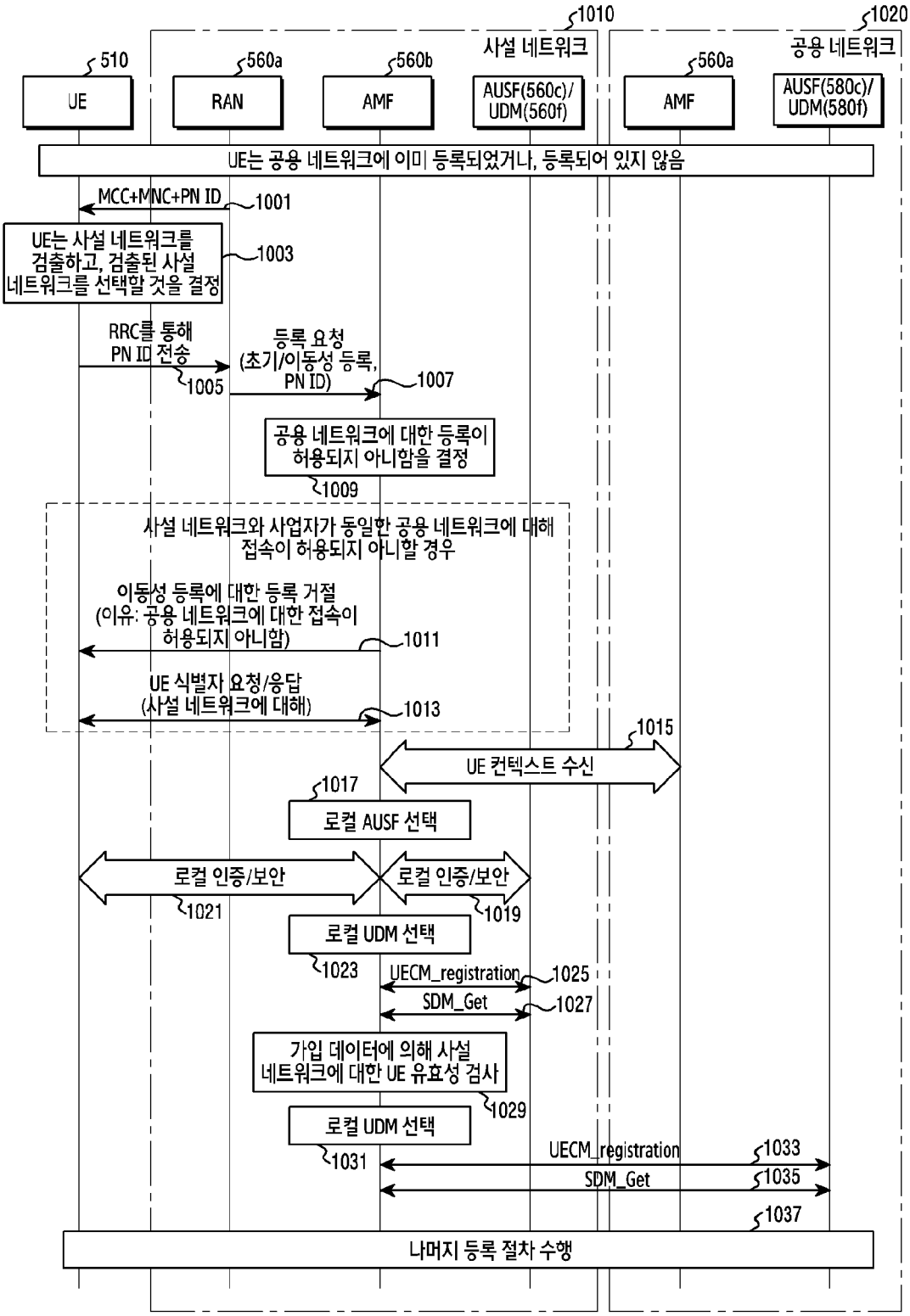
[도8]


810
820
사설 네트워크
공용 네트워크
510
560a
560b
580b
UE
RAN
AMF
AUSF(560c)/ UDM(560f)
AMF
AUSF(580c)/ UDM(580f)
UE는 공용 네트워크에 등록되어 있지 않음
MCC+MNC+PN ID
801
UE는 사설 네트워크를 검출하고, 검출된 사설 네트워크를 선택할 것을 결정
803
RRC를 통해 PN ID 전송
805
등록 요청 (초기 요청, PN ID)
807
공용 네트워크에 대한 등록이 요구됨을 결정
809
UE 컨텍스트 수신
811
813
매크로 AUSF 선택
매크로 인증/보안
815
매크로 인증/보안
817
매크로 UDM 선택
819
UECM_registration
821
SDM_Get
823
대안1
가입 데이터에 의해 사설 네트워크에 대한 UE 유효성 검사
825
로컬 UDM 선택
827
UECM_registration
829
SDM_Get
831
로컬 AUSF 선택
833
837
로컬 인증/보안
835
로컬 인증/보안
대안2
로컬 UDM 선택
839
UECM_registration
841
SDM_Get
843
845
가입 데이터에 의해 사설 네트워크에 대한 UE 유효성 검사
매크로 UDM 선택
847
UECM_registration
849
SDM_Get
851
853
나머지 등록 절차 수행

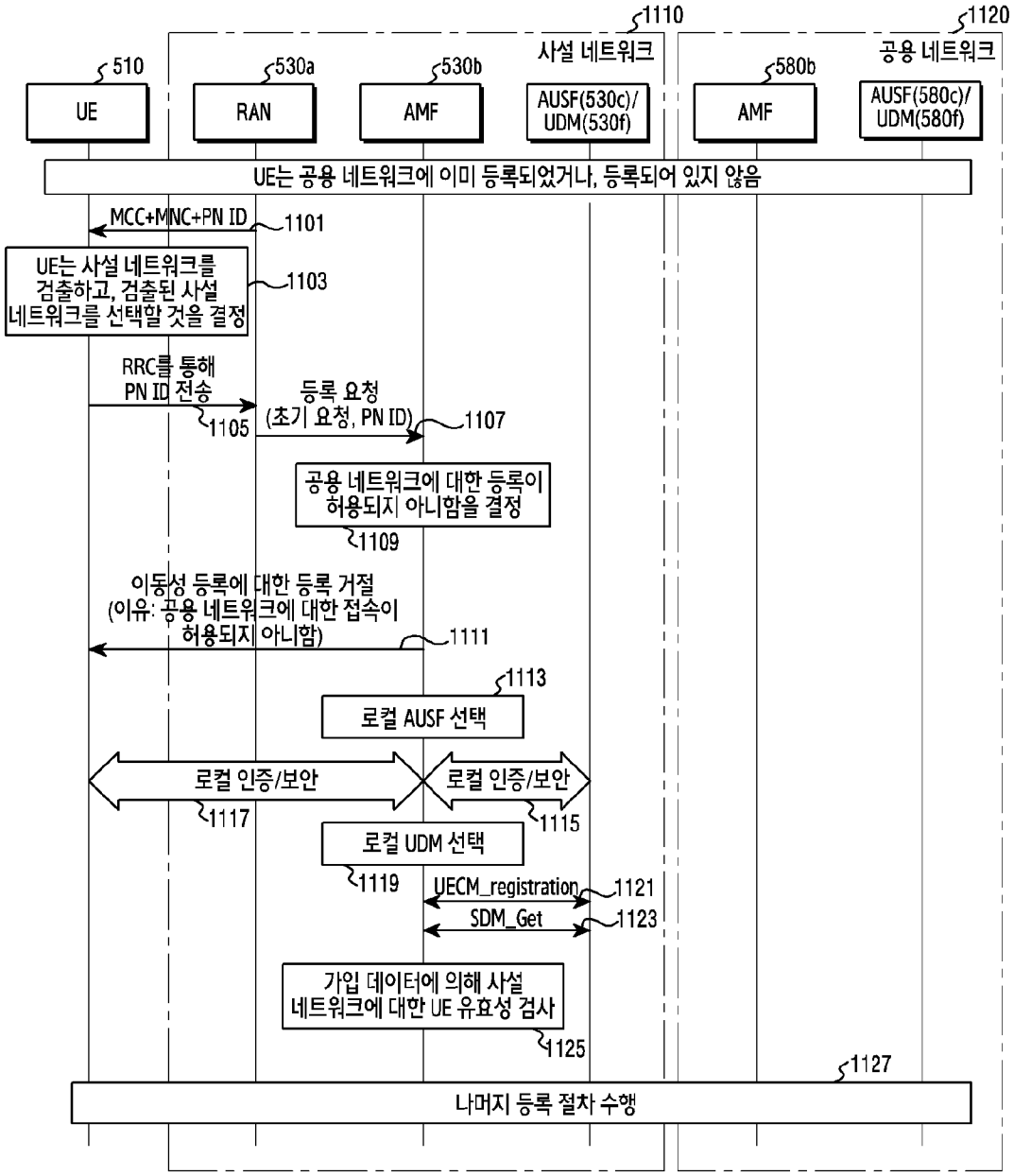
[도9]


910
920
사설 네트워크
공용 네트워크
510
560a
560b
580b
UE
RAN
AMF
AUSF(560c)/ UDM(560f)
AMF
AUSF(580c)/ UDM(580f)
MCC+MNC+PN ID
901
UE는 사설 네트워크를 검출하고, 검출된 사설 네트워크를 선택할 것을 결정
903
UE가 공용 네트워크에 등록되지 않았을 경우, UE는 공용 네트워크에 등록
905
등록 팔로온 타이머
RRC를 통해 PN ID 전송
907
등록 요청 (이동성, PN ID)
909
공용 네트워크에 대한 등록이 요구됨을 결정
911
이동성 등록

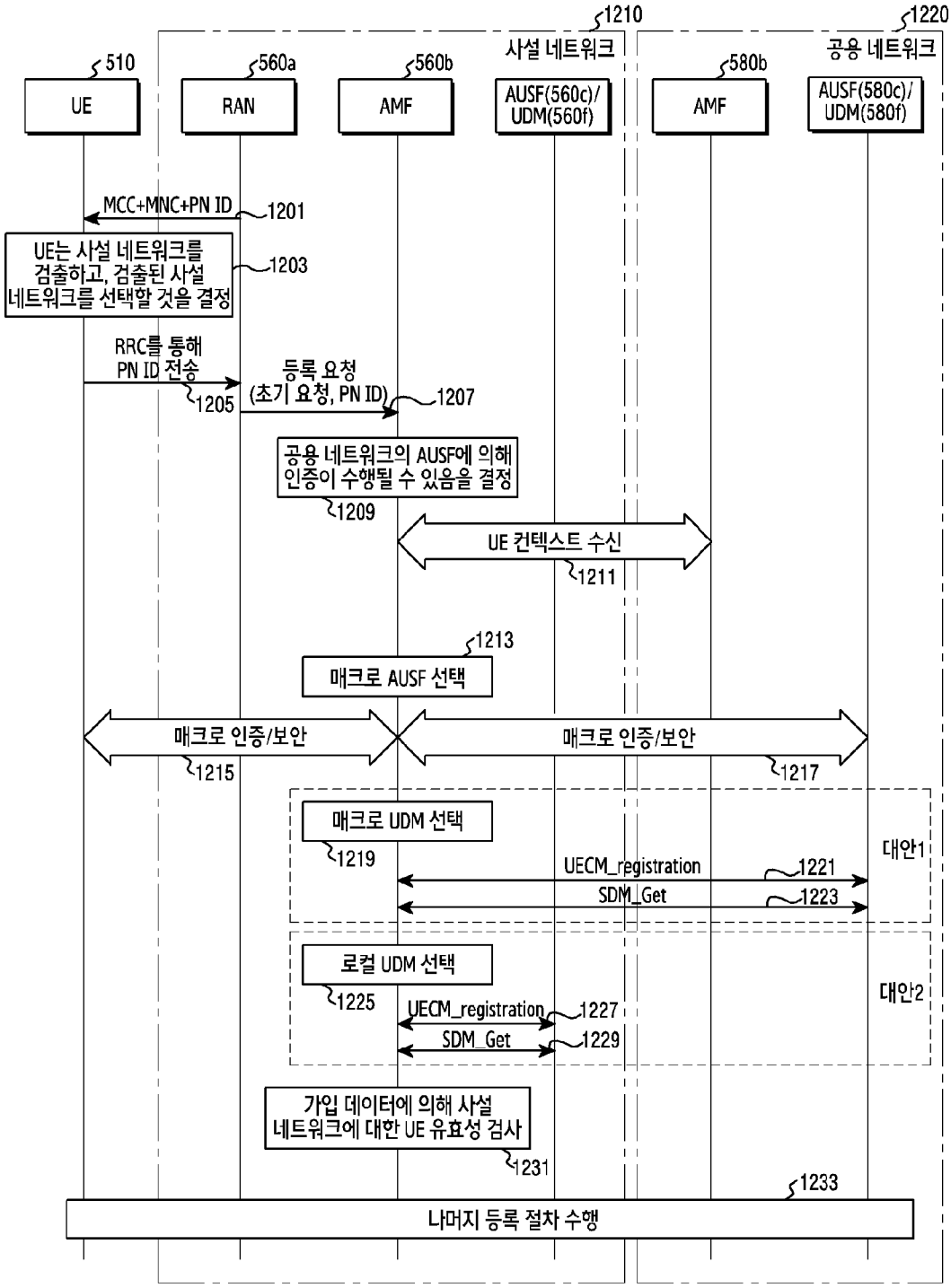
[도10]


1010
사설 네트워크
1020
공용 네트워크
510
UE
560a
RAN
560b
AMF
AUSF(560c)/
UDM(560f)
560a
AMF
AUSF(580c)/
UDM(580f)
UE는 공용 네트워크에 이미 등록되었거나, 등록되어 있지 않음
MCC+MNC+PN ID
1001
UE는 사설 네트워크를 검출하고, 검출된 사설 네트워크를 선택할 것을 결정
1003
RRC를 통해 PN ID 전송
1005
등록 요청 (초기/이동성 등록, PN ID)
1007
공용 네트워크에 대한 등록이 허용되지 아니함을 결정
1009
사설 네트워크와 사업자가 동일한 공용 네트워크에 대해 접속이 허용되지 아니할 경우
이동성 등록에 대한 등록 거절 (이유: 공용 네트워크에 대한 접속이 허용되지 아니함)
1011
UE 식별자 요청/응답 (사설 네트워크에 대해)
1013
1015
UE 컨텍스트 수신
1017
로컬 AUSF 선택
로컬 인증/보안
1021
로컬 인증/보안
1019
로컬 UDM 선택
1023
UECM_registration
1025
SDM_Get
1027
가입 데이터에 의해 사설 네트워크에 대한 UE 유효성 검사
1029
로컬 UDM 선택
1031
UECM_registration
1033
SDM_Get
1035
1037
나머지 등록 절차 수행

[도11]


1110
사설 네트워크
1120
공용 네트워크
510
UE
530a
RAN
530b
AMF
AUSF(530c)/
UDM(530f)
580b
AMF
AUSF(580c)/
UDM(580f)
UE는 공용 네트워크에 이미 등록되었거나, 등록되어 있지 않음
MCC+MNC+PN ID
1101
UE는 사설 네트워크를
검출하고, 검출된 사설
네트워크를 선택할 것을 결정
1103
RRC를 통해
PN ID 전송
1105
등록 요청
(초기 요청, PN ID)
1107
공용 네트워크에 대한 등록이
허용되지 아니함을 결정
1109
이동성 등록에 대한 등록 거절
(이유: 공용 네트워크에 대한 접속이
허용되지 아니함)
1111
1113
로컬 AUSF 선택
로컬 인증/보안
1117
로컬 인증/보안
1115
로컬 UDM 선택
1119
UECM_registration
1121
SDM_Get
1123
가입 데이터에 의해 사설
네트워크에 대한 UE 유효성 검사
1125
1127
나머지 등록 절차 수행

[도12]


1210
사설 네트워크
1220
공용 네트워크
510
UE
560a
RAN
560b
AMF
AUSF(560c)/
UDM(560f)
580b
AMF
AUSF(580c)/
UDM(580f)
MCC+MNC+PN ID
1201
UE는 사설 네트워크를
검출하고, 검출된 사설
네트워크를 선택할 것을 결정
1203
RRC를 통해
PN ID 전송
1205
등록 요청
(초기 요청, PN ID)
1207
공용 네트워크의 AUSF에 의해
인증이 수행될 수 있음을 결정
1209
UE 컨텍스트 수신
1211
1213
매크로 AUSF 선택
매크로 인증/보안
1215
매크로 인증/보안
1217
매크로 UDM 선택
1219
UECM_registration
1221
SDM_Get
1223
대안1
로컬 UDM 선택
1225
UECM_registration
1227
SDM_Get
1229
대안2
가입 데이터에 의해 사설
네트워크에 대한 UE 유효성 검사
1231
1233
나머지 등록 절차 수행

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2019/010265

A. CLASSIFICATION OF SUBJECT MATTER

H04W 48/02(2009.01)i, H04W 48/18(2009.01)i, H04W 8/20(2009.01)i, H04W 60/00(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 48/02; H04W 12/06; H04W 16/24; H04W 24/02; H04W 48/04; H04W 48/18; H04W 8/20; H04W 60/00

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: private network, public network, AUSF(authentication server function), UDM(unified data management), authentication, validity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2013-0318572 A1 (SINGH, Sukhjinder et al.) 28 November 2013 See paragraphs [0032], [0037], [0039]-[0040], [0059], [0078]-[0080], [0085]-[0086], [0092].	1-15
Y	5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.2.0 Release 15). ETSI TS 123 501 V15.2.0. 28 June 2018 See pages 17, 48, 122-123, 179, 185-186, 190.	1-15
A	KR 10-2017-0119296 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 26 October 2017 See paragraphs [0106]-[0140].	1-15
A	5G; Procedures for the 5G System (3GPP TS 23.502 version 15.2.0 Release 15). ETSI TS 123 502 V15.2.0. 28 June 2018 See page 19; and figure 4.2.2.2.2-1.	1-15
A	KR 10-2017-0004835 A (KT CORPORATION) 11 January 2017 See paragraphs [0061]-[0083]; and figure 1.	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
13 DECEMBER 2019 (13.12.2019)	**13 DECEMBER 2019 (13.12.2019)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2019/010265

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2013-0318572 A1	28/11/2013	CA 2816131 A1	25/11/2013
		EP 2667664 A1	27/11/2013
		EP 2667664 B1	23/01/2019
		US 10129751 B2	13/11/2018
		US 2019-0274047 A1	05/09/2019
KR 10-2017-0119296 A	26/10/2017	US 10142994 B2	27/11/2018
		US 10412741 B2	10/09/2019
		US 2017-0303259 A1	19/10/2017
		US 2019-0098618 A1	28/03/2019
KR 10-2017-0004835 A	11/01/2017	KR 10-1629006 B1	13/06/2016
		WO 2017-007122 A1	12/01/2017

국제조사보고서

국제출원번호
PCT/KR2019/010265

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 48/02(2009.01)i, H04W 48/18(2009.01)i, H04W 8/20(2009.01)i, H04W 60/00(2009.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04W 48/02; H04W 12/06; H04W 16/24; H04W 24/02; H04W 48/04; H04W 48/18; H04W 8/20; H04W 60/00

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: 사설 네트워크(private network), 공용 네트워크(public network), AUSF(authentication server function), UDM(unified data management), 인증(authentication), 유효성(validity)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	US 2013-0318572 A1 (SUKHJINDER SINGH 등) 2013.11.28 단락 [0032], [0037], [0039]-[0040], [0059], [0078]-[0080], [0085]-[0086], [0092] 참조.	1-15
Y	`5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.2.0 Release 15)', ETSI TS 123 501 V15.2.0, 2018.06.28 페이지 17, 48, 122-123, 179, 185-186, 190 참조.	1-15
A	KR 10-2017-0119296 A (한국전자통신연구원) 2017.10.26 단락 [0106]-[0140] 참조.	1-15
A	`5G; Procedures for the 5G System (3GPP TS 23.502 version 15.2.0 Release 15)', ETSI TS 123 502 V15.2.0, 2018.06.28 페이지 19; 및 도면 4.2.2.2.2-1 참조.	1-15
A	KR 10-2017-0004835 A (주식회사 케이티) 2017.01.11 단락 [0061]-[0083]; 및 도면 1 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

"D" 본 국제출원에서 출원인이 인용한 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
2019년 12월 13일 (13.12.2019)	2019년 12월 13일 (13.12.2019)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
권성호
전화번호 +82-42-481-3547

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2019/010265

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2013-0318572 A1	2013/11/28	CA 2816131 A1	2013/11/25
		EP 2667664 A1	2013/11/27
		EP 2667664 B1	2019/01/23
		US 10129751 B2	2018/11/13
		US 2019-0274047 A1	2019/09/05
KR 10-2017-0119296 A	2017/10/26	US 10142994 B2	2018/11/27
		US 10412741 B2	2019/09/10
		US 2017-0303259 A1	2017/10/19
		US 2019-0098618 A1	2019/03/28
KR 10-2017-0004835 A	2017/01/11	KR 10-1629006 B1	2016/06/13
		WO 2017-007122 A1	2017/01/12