(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0084100
(43) 공개일자 2014년07월04일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04W 8/02* (2009.01)
(21) 출원번호 10-2014-7011675
(22) 출원일자(국제) 2012년09월28일
심사청구일자 없음
(85) 번역문제출일자 2014년04월29일
(86) 국제출원번호 PCT/US2012/057946
(87) 국제공개번호 WO 2013/049587
국제공개일자 2013년04월04일
(30) 우선권주장
61/540,682 2011년09월29일 미국(US)

(71) 출원인
인터디지탈 패튼 홀딩스, 인크
미국, 델라웨어주 19809, 윌밍턴, 벨뷰 파크웨이 200, 스위트 300
(72) 발명자
드 포이 사비에르
캐나다 퀘벡 에이치9에이치5케이5 커클랜드 뤼 에드몽 3007
타갈리 요시프
미국 뉴저지주 07721 클리프우드 델라웨어 애비뉴 183
(뒷면에 계속)
(74) 대리인
김태홍, 김성기

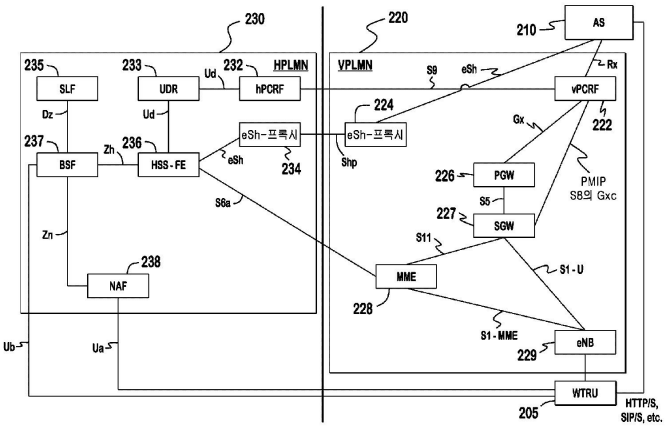
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법 및 장치**

(57) 요 약

모바일 네트워크 운용자와 애플리케이션 공급자 간에 연동시키는 방법 및 장치가 개시된다. 네트워크 애플리케이션 기능(NAF)은 부트스트래핑 서버 기능(BSF)을 통해 홈 가입자 서버(HSS)에 접근하기 위해 애플리케이션 서버가 NAF와 통신할 수 있도록 오픈ID 공급자와 공존될 수 있다. BSF와 HSS 간, 및 BSF와 NAF 간의 인테페이스는 애플리케이션 서버와 HSS 간에 Sh 인터페이스를 통하여 이용가능한 정보를 운반하도록 강화될 수 있다. WTRU가 방문 네트워크에서 로밍할 때, 애플리케이션 서버는 WTRU로부터의 서비스 요청에의 서빙에 대한 과금 및 폴리싱을 위해 방문 네트워크와 통신할 수 있다. 애플리케이션 서버는 NAF와 공존될 수 있고, 일반 부트스트래핑 아키텍처를 이용하여 WTRU를 인증할 수 있으며, HSS에 접근하기 위해 eZn-프록시 기능을 통하여 홈 네트워크의 BSF와 통신할 수 있다.

대 표 도



(72) 발명자

샤헨 카멜 엠

미국 펜실베니아주 19406 킹 오브 프러시아 애쉬톤 드라이브 429

리우 행

미국 매릴랜드주 20878 노스 포토맥 보트 하우스 코트 5

파텔 밀란

영국 에이치에이2 0에이치비 미들섹스 해로우 로워 로드 그레빌 하우스 8

루홀라 오사마

미국 캘리포니아주 92123 샌디에고 #11108 스펙트럼 센터 블러바드 8877

특허청구의 범위

청구항 1

모바일 네트워크 운용자와 애플리케이션 공급자 사이를 연동(interworking)시키는 방법에 있어서,

애플리케이션 서버가 무선 송수신 유닛(wireless transmit/receive unit, WTRU)으로부터 서비스 요청을 수신하는 단계와;

상기 애플리케이션 서버가, 오픈ID를 이용하여 상기 WTRU를 인증하는 단계와;

상기 애플리케이션 서버가, 오픈ID 공급자(OpenID provider, OP)와 공존하는(co-locate) 네트워크 애플리케이션 기능(network application function, NAF)을 통해 홈 가입자 서버(home subscriber server, HSS)에 접근하는 단계를 포함한 연동 방법.

청구항 2

제1항에 있어서, 상기 NAF는 상기 WTRU의 홈 네트워크에 위치된 것인, 모바일 네트워크 운용자와 애플리케이션 공급자 사이의 연동 방법.

청구항 3

제1항에 있어서, 상기 WTRU가 방문 네트워크에서 로밍하고 있고, 상기 애플리케이션 공급자는 상기 방문 네트워크와의 협약을 갖는 것인, 모바일 네트워크 운용자와 애플리케이션 공급자 사이의 연동 방법.

청구항 4

제3항에 있어서, 상기 애플리케이션 서버는 상기 WTRU로부터의 서비스 요청의 서빙에 대한 과금 및 폴리싱(policing)을 위해 상기 방문 네트워크와 통신하는 것인, 모바일 네트워크 운용자와 애플리케이션 공급자 사이의 연동 방법.

청구항 5

모바일 네트워크 운용자와 애플리케이션 공급자 사이를 연동시키는 장치에 있어서,

무선 송수신 유닛(wireless transmit/receive unit, WTRU)으로부터 서비스 요청을 수신하고, 오픈ID를 이용하여 상기 WTRU를 인증하며, 오픈ID 공급자(OpenID provider, OP)와 공존하는 네트워크 애플리케이션 기능(network application function, NAF)을 통해 홈 가입자 서버(home subscriber server, HSS)에 접근하도록 구성된 프로세서를 포함하는, 모바일 네트워크 운용자와 애플리케이션 공급자 사이의 연동 장치.

청구항 6

제5항에 있어서, 상기 NAF는 상기 WTRU의 홈 네트워크에 위치된 것인, 모바일 네트워크 운용자와 애플리케이션 공급자 사이의 연동 장치.

청구항 7

제5항에 있어서, 상기 WTRU가 방문 네트워크에서 로밍하고 있고, 상기 애플리케이션 공급자는 상기 방문 네트워크와의 협약을 갖는 것인, 모바일 네트워크 운용자와 애플리케이션 공급자 사이의 연동 장치.

청구항 8

제7항에 있어서, 상기 프로세서는 상기 WTRU로부터의 서비스 요청의 서빙에 대한 과금 및 폴리싱을 위해 상기 방문 네트워크와 통신하도록 구성된 것인, 모바일 네트워크 운용자와 애플리케이션 공급자 사이의 연동 장치.

청구항 9

모바일 네트워크 운용자와 애플리케이션 공급자 사이를 연동시키는 방법에 있어서,

애플리케이션 서버가, 무선 송수신 유닛(wireless transmit/receive unit, WTRU)- 상기 WTRU는 상기 애플리케

이션 공급자가 협약을 가진 방문 네트워크에서 로밍하고 있고, 상기 애플리케이션 서버는 네트워크 애플리케이션 기능(network application function, NAF)과 공존되는 것임 -으로부터 서비스 요청을 수신하는 단계와;

NAF로서 작용하는 애플리케이션 서버가, 일반 부트스트래핑 아키텍처(Generic Bootstrapping Architecture, GBA)를 이용하여 상기 WTRU를 인증하는 단계와;

애플리케이션 서버가, 홈 가입자 서버(home subscriber server, HSS)에 접근하기 위해 eZn-프록시 기능을 통하여 홈 네트워크의 부트스트래핑 서비 기능(bootstrapping server function, BSF)과 통신하는 단계를 포함하는, 모바일 네트워크 운용자와 애플리케이션 공급자 사이의 연동 방법.

청구항 10

제9항에 있어서, 상기 WTRU가 인증된 조건하에 상기 애플리케이션 서버가, 상기 방문 네트워크의 폴리시 및 과금 규칙 기능(Policy and Charging Rules Function, PCRF)에 대한 Rx 인터페이스를 이용하여 상기 서비스에 대한 서비스 품질 및 과금을 제어하는 단계를 더 포함하는, 모바일 네트워크 운용자와 애플리케이션 공급자 사이의 연동 방법.

청구항 11

방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법에 있어서,

애플리케이션 서버가, 무선 송수신 유닛(wireless transmit/receive unit, WTRU)- 상기 WTRU가 방문 네트워크에서 로밍하고 있고, 애플리케이션 공급자는 상기 방문 네트워크와의 협약을 가짐 -으로부터 서비스 요청을 수신하는 단계와;

상기 애플리케이션 서버가, 상기 WTRU가 상기 방문 네트워크에서 로밍하고 있음을 결정하는 단계와;

상기 애플리케이션 서버가, 상기 WTRU로부터의 서비스 요청의 서빙에 대한 과금, 폴리싱 및 사용자 데이터 접근을 위해 상기 방문 네트워크와 통신하는 단계를 포함하는, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

청구항 12

제11항에 있어서, 상기 애플리케이션 서버가 Rx 인터페이스를 이용하여 상기 방문 네트워크의 폴리시 제어 규칙 기능(policy control rules function, PCRF)(vPCRF)에게 제1 메시지- 상기 제1 메시지는 홈 네트워크의 PCRF(hPCRF)로 포워딩되는 것임 -를 보내는 단계와;

상기 애플리케이션 서버가, 상기 제1 메시지에 응답하여 상기 vPCRF를 통해 제2 메시지를 수신하는 단계를 더 포함하고,

상기 애플리케이션 서버가, 상기 제2 메시지에 포함된 정보에 기초하여 상기 WTRU가 상기 방문 네트워크에서 로밍하고 있음을 결정하는 것인, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

청구항 13

제12항에 있어서, 상기 애플리케이션 서버가, 상기 방문 네트워크의 Sh-프록시로 사용자 데이터 요청을 보내는 단계를 더 포함하고, 상기 사용자 데이터 요청은 Sh-프록시가 어떤 홈 네트워크 Sh-프록시와 통신하는지를 알아낼 수 있게 하는 홈 네트워크 영역 또는 도메인명 정보를 포함한 것인, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

청구항 14

제11항에 있어서, 상기 애플리케이션 서버는 상기 WTRU의 인증 중에 수신된 정보에 기초하여 상기 WTRU가 상기 방문 네트워크에서 로밍하고 있음을 결정하는 것인, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

청구항 15

제14항에 있어서, 상기 애플리케이션 서버는 상기 WTRU의 이동국 국제 가입자 디렉토리 번호(Mobile Station International Subscriber Directory Number, MSISDN)를 수신하고, 상기 MSISDN에 기초하여 상기 WTRU가 상기

방문 네트워크에서 로밍하고 있음을 결정하는 것인, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

청구항 16

제11항에 있어서, 상기 애플리케이션 서버는 홈 네트워크 신원(identification)을 수신하고, 상기 홈 네트워크 신원에 기초하여 상기 WTRU가 상기 방문 네트워크에서 로밍하고 있음을 결정하는 것인, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

청구항 17

제16항에 있어서, 상기 홈 네트워크 신원은 모바일 네트워크 코드(mobile network code, MNC) + 모바일 국가 코드(mobile country code, MCC), 또는 디아미터 영역(Diameter realm)인 것인, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

청구항 18

제11항에 있어서, 상기 애플리케이션 서버가, 사용자 데이터를 획득하기 위해 사용자 데이터 요청을 보내는 단계를 더 포함하고, 상기 WTRU의 홈 네트워크에서 상기 애플리케이션 서버와 홈 가입자 서버(home subscriber server, HSS) 사이의 통신은 상기 방문 네트워크의 Sh-프록시 기능을 통하여 중재되며, 상기 Sh-프록시 기능은 상기 방문 네트워크와 상기 홈 네트워크 사이의 로밍 협약으로부터 도출된 폴리시를 강화하는 것인, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

청구항 19

제11항에 있어서, 상기 애플리케이션 서버가, 상기 애플리케이션 공급자가 상기 WTRU의 홈 네트워크와의 협약을 가짐을 결정하는 단계를 더 포함하고, 상기 애플리케이션 서버는 상기 서비스 요청에 서빙하기 위해 상기 홈 네트워크와 상기 방문 네트워크 중의 어느 하나 또는 양측 모두로의 접속을 이용하는 것인, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

청구항 20

제11항에 있어서, 상기 애플리케이션 서버가, 상기 WTRU의 홈 네트워크에 서빙하는 협력 애플리케이션 공급자가 있음을 결정하는 단계와;

상기 애플리케이션 서버가, 상기 WTRU를 상기 협력 애플리케이션 서버를 향하여 재지향시키는 단계를 더 포함하는, 방문 네트워크와 통합된 애플리케이션에의 접근을 가능하게 하는 방법.

명 세 서

기 술 분 야

[0001] 관련 출원에 대한 교차 참조

[0002] 이 출원은 2011년 9월 29일자 출원한 미국 가특허 출원 제61/540,682호를 우선권 주장하며, 이 가특허 출원의 내용은 여기에서의 인용에 의해 본원에 통합된다.

배 경 기 술

[0003] 데이터 애플리케이션 공급자 제3세대 파트너십 프로젝트(3GPP) 작업 그룹과의 연동(interworking)을 지원하는 진화형 패킷 코어(Evolved Packet Core, EPC)는 애플리케이션 공급자와 3GPP 모바일 네트워크 운용자 코어 네트워크 간의 연동을 위한 솔루션을 제공한다. 도 17은 애플리케이션 플랫폼이 모바일 네트워크 운용자 코어 네트워크에 접속된 비-로밍(non-roaming)의 경우를 보인 것이다. 접근 및 인터넷 프로토콜(IP) 접속성은 모바일 네트워크 운용자에 의해 제공된다. 제3자 애플리케이션 플랫폼은 애플리케이션 서버(예를 들면, 비디오-온-디맨드 서버, 패킷 교환식 스트리밍(packet switched streaming, PSS) 서버, 머신 타입 통신(machine type communication, MTC) 서버 등), 또는 제3자 소프트웨어 개발 플랫폼일 수 있다.

[0004] 도 18은 WTRU가 방문형 공중 육상 모바일 네트워크(visited public land mobile network, VPLMN)를 로밍하고 홈 공중 육상 모바일 네트워크(HPLMN)에 의해 제공된 애플리케이션에 접근하는 로밍 경우를 보인 것이다. 도 17

및 도 18에 도시된 것처럼, 모바일 네트워크 운용자는 애플리케이션 계층 엔티티(예를 들면, 애플리케이션 플랫폼)를 소유하지 않을 수 있다. 대안적으로, 모바일 네트워크 운용자는 애플리케이션 계층 엔티티를 소유할 수 있다. 도 18은 모든 트래픽이 홈 모바일 네트워크 운용자 진화형 패킷 시스템(EPS)에 라우트되고 애플리케이션이 모바일 네트워크 운용자들 간의 로밍 협약(roaming agreement)을 통해 전달되는 홈-라우트 경우를 보인 것이다.

발명의 내용

[0005] 모바일 네트워크 운용자와 애플리케이션 공급자 간에 연동시키는 방법 및 장치가 개시된다. 네트워크 애플리케이션 기능(network application function, NAF)은 애플리케이션 서버가 NAF와 통신하여 부트스트래핑 서버 기능(BSF)을 통해 홈 가입자 서버(HSS)의 사용자 데이터에 접근하거나, HSS에서 정보를 설정하거나, 또는 HSS에 이벤트를 등록할 수 있도록 오픈ID 공급자(OpenID provider, OP)와 공존될 수 있다. BSF와 HSS 간, 및 BSF와 NAF 간의 인테페이스는 애플리케이션 서버와 HSS 간에 Sh 인터페이스를 통하여 이용가능한 정보를 운반하도록 강화될 수 있다. NAF는 홈 네트워크 내에 또는 홈 네트워크 외부에 위치될 수 있다. WTRU는 홈 네트워크에 접속될 수 있고, 또는 방문 네트워크에서 로밍할 수 있다. WTRU가 방문 네트워크에서 로밍할 때, 애플리케이션 서버는 서비스 품질(QoS) 및 서비스에 대한 과금(charging) 제어를 위해 방문 네트워크와 상호작용할 수 있다.

[0006] 대안적으로, 애플리케이션 서버는 NAF와 공존될 수 있고, 일반 부트스트래핑 아키텍처(GBA)를 이용하여 WTRU를 인증할 수 있다. 사용자가 인증되면, 애플리케이션 서버는 HSS의 데이터에 접근하기 위해, HSS에서 정보를 설정하기 위해, 또는 HSS에 이벤트를 등록하기 위해 eZn-프록시 기능을 통하여 홈 네트워크의 BSF와 통신할 수 있다.

[0007] 대안적으로, WTRU가 방문 네트워크에서 로밍하고 애플리케이션 공급자가 방문 네트워크와 협약을 가진 경우에, 애플리케이션 서버는 방문 네트워크와 통신하여 WTRU로부터의 서비스 요청에 서빙하기 위한 과금, 폴리싱(policing), 및 사용자 데이터 접근을 할 수 있다.

도면의 간단한 설명

[0008] 더 구체적인 이해는 첨부 도면과 함께 예로서 주어지는 이하의 설명으로부터 얻을 수 있다.

도 1a는 하나 이상의 본 발명의 실시형태가 구현될 수 있는 예시적인 통신 시스템의 계통도이다.

도 1b는 도 1a에 도시된 통신 시스템에서 사용될 수 있는 예시적인 무선 송수신 유닛(WTRU)의 계통도이다.

도 1c는 도 1a에 도시된 통신 시스템에서 사용될 수 있는 예시적인 무선 접근 네트워크 및 예시적인 코어 네트워크의 계통도이다.

도 2는 애플리케이션 서버(AS)가 VPLMN과 상호 접속된 예시적인 네트워크 아키텍처를 보인 도이다.

도 3a 및 도 3b는 일 실시형태에 따라서, 애플리케이션 공급자가 방문 네트워크 운용자와의 협약을 갖지만 홈 네트워크 운용자와의 협약을 갖지 않는 경우에 인증, 세션 폴리시/과금 개시 및 사용자 데이터 요청의 예시적인 처리에 관한 신호도이다.

도 4는 AS가 홈 네트워크 및 방문 네트워크 양자에 상호 접속된 예시적인 네트워크 아키텍처를 보인 도이다.

도 5a 내지 도 5c는 애플리케이션 공급자가 홈 네트워크 운용자 및 방문 네트워크 운용자 양자와의 협약을 갖는 경우에 인증, 세션 폴리시/과금 개시 및 사용자 데이터 요청의 예시적인 처리에 관한 신호도이다.

도 6은 애플리케이션 공급자가 복수의 애플리케이션 서버를 전개하는 예시적인 네트워크 아키텍처를 보인 도이다.

도 7a 및 도 7b는 사용자를 VPLMN에 서빙하는 AS로부터 HPLMN에 서빙하는 AS로 재지향시키기 위한 예시적인 처리에 관한 신호도이다.

도 8은 사용자를 홈 네트워크에 서빙하는 AS로부터 방문 네트워크에 서빙하는 AS로 재지향시키기 위한 예시적인 처리에 관한 신호도이다.

도 9는 NAF 기능이 오픈ID 공급자(OP)와 공존되고 AS-VPLMN 상호접속 및 eZn-프록시가 폴리싱, 과금, 및 사용자 데이터 획득을 위해 사용되는 경우의 예시적인 네트워크 아키텍처를 보인 도이다.

도 10은 일 실시형태에 따라서, 애플리케이션 세션을 확립하고 AS-VPLMN 상호접속 및 eZn-프록시를 이용하여 폴리싱, 과금, 및 사용자 데이터 획득을 행하는 예시적인 처리의 신호도이다.

도 11은 NAF 기능이 OP와 공존되고 AS-VPLMN 상호접속 및 HPLMN의 강화 네트워크 애플리케이션 기능(eNAF)을 이용하여 폴리싱, 과금, 및 사용자 데이터 획득을 행하는 예시적인 네트워크 아키텍처를 보인 도이다.

도 12는 일 실시형태에 따라서 애플리케이션 세션을 확립하는 예시적인 처리의 신호도이다.

도 13은 비-로밍의 경우에 HPLMN에서 eNAF/OP를 가진 예시적인 네트워크 아키텍처를 보인 도이다.

도 14는 일 실시형태에 따라서 비-로밍의 경우에 HPLMN의 eNAF를 이용하여 애플리케이션 세션을 확립하는 예시적인 처리의 신호도이다.

도 15는 공존하는 AS/eNAF를 가진 예시적인 네트워크 아키텍처를 보인 도이다.

도 16은 일 실시형태에 따른, AS 및 eNAF가 공존하는 경우에 애플리케이션 세션을 확립하는 예시적인 처리의 신호도이다.

도 17은 애플리케이션 플랫폼이 모바일 네트워크 운용자 코어 네트워크에 접속된 경우의 비-로밍 경우를 보인 도이다.

도 18은 WTRU가 VPLMN에서 로밍하고 HPLMN에 의해 제공된 애플리케이션에 접근하는 경우의 로밍 경우를 보인 도이다.

발명을 실시하기 위한 구체적인 내용

[0009] 도 1a는 하나 이상의 본 발명의 실시형태를 구현할 수 있는 예시적인 통신 시스템(100)을 보인 도이다. 통신 시스템(100)은 복수의 무선 사용자에게 음성, 데이터, 영상, 메시지, 방송 등의 콘텐츠를 제공하는 다중 접근 시스템일 수 있다. 통신 시스템(100)은 복수의 무선 사용자들이 무선 대역폭을 포함한 시스템 자원을 공유함으로써 상기 콘텐츠에 접근할 수 있게 한다. 예를 들면, 통신 시스템(100)은 코드 분할 다중 접속(CDMA), 시분할 다중 접속(TDMA), 주파수 분할 다중 접속(FDMA), 직교 FDMA(OFDMA), 단일 캐리어 FDMA(SC-FDMA) 등과 같은 하나 이상의 채널 접근 방법을 이용할 수 있다.

[0010] 도 1a에 도시된 것처럼, 통신 시스템(100)은 무선 송수신 유닛(wireless transmit/receive unit, WTRU)(102a, 102b, 102c, 102d), 무선 접근 네트워크(radio access network, RAN)(104), 코어 네트워크(106), 공중 교환식 전화망(public switched telephone network, PSTN)(108), 인터넷(110) 및 기타의 네트워크(112)를 포함하고 있지만, 본 발명의 실시형태는 임의 수의 WTRU, 기지국, 네트워크 및/또는 네트워크 요소를 포함할 수 있다는 것을 이해할 것이다. 각 WTRU(102a, 102b, 102c, 102d)는 무선 환경에서 동작 및/또는 통신하도록 구성된 임의 유형의 장치일 수 있다. 예를 들면, WTRU(102a, 102b, 102c, 102d)는 무선 신호를 송신 및/또는 수신하도록 구성될 수 있고, 사용자 장비(UE), 이동국, 고정식 또는 이동식 가입자 유닛, 페이저, 셀룰러 전화기, 개인 정보 단말기(personal digital assistant, PDA), 스마트폰, 랩톱, 넷북, 퍼스널 컴퓨터, 무선 센서, 소비자 전자제품 등을 포함할 수 있다.

[0011] 통신 시스템(100)은 기지국(114a)과 기지국(114b)을 또한 포함할 수 있다. 각 기지국(114a, 114b)은 적어도 하나의 WTRU(102a, 102b, 102c, 102d)와 무선으로 인터페이스 접속하여 코어 네트워크(106), 인터넷(110) 및/또는 네트워크(112)와 같은 하나 이상의 통신 네트워크에 접근하도록 구성된 임의 유형의 장치일 수 있다. 예를 들면, 기지국(114a, 114b)은 기지국 송수신기(base transceiver station, BTS), 노드-B, e노드 B, 홈 노드 B, 홈 e노드 B, 사이트 제어기, 접근점(access point, AP), 무선 라우터 등일 수 있다. 비록 기지국(114a, 114b)이 각각 단일 요소로서 도시되어 있지만, 기지국(114a, 114b)은 임의 수의 상호접속된 기지국 및/또는 네트워크 요소를 포함할 수 있다는 것을 이해할 것이다.

[0012] 기지국(114a)은 RAN(104)의 일부일 수 있고, RAN(104)은 기지국 제어기(base station controller, BSC), 라디오 네트워크 제어기(radio network controller, RNC), 릴레이 노드 등과 같은 다른 기지국 및/또는 네트워크 요소(도시 생략됨)를 또한 포함할 수 있다. 기지국(114a) 및/또는 기지국(114b)은 셀(도시 생략됨)이라고도 부르는 특정 지리적 영역 내에서 무선 신호를 송신 및/또는 수신하도록 구성될 수 있다. 셀은 복수의 셀 섹터로 세분될 수 있다. 예를 들면, 기지국(114a)과 관련된 셀은 3개의 섹터로 나누어질 수 있다. 따라서, 일 실시형태에 있어서, 기지국(114a)은 셀의 각 섹터마다 하나씩 3개의 송수신기를 포함할 수 있다. 다른 실시형태에 있어서, 기지국(114a)은 다중입력 다중출력(MIMO) 기술을 사용할 수 있고, 따라서 셀의 각 섹터마다 복수의 송수신기를

사용할 수 있다.

[0013] 기지국(114a, 114b)은 임의의 적당한 무선 통신 링크(예를 들면, 라디오 주파수(RF), 마이크로파, 적외선(IR), 자외선(UV), 가시광선 등)일 수 있는 무선 인터페이스(116)를 통하여 하나 이상의 WTRU(102a, 102b, 102c, 102d)와 통신할 수 있다. 무선 인터페이스(116)는 임의의 적당한 무선 접근 기술(radio access technology, RAT)을 이용하여 확립될 수 있다.

[0014] 더 구체적으로, 위에서 언급한 것처럼, 통신 시스템(100)은 다중 접근 시스템일 수 있고, CDMA, TDMA, FDMA, OFDMA, SC-FDMA 등과 같은 하나 이상의 채널 접근 방식을 이용할 수 있다. 예를 들면, RAN(104) 내의 기지국(114a)과 WTRU(102a, 102b, 102c)는 광대역 CDMA(WCDMA)를 이용하여 무선 인터페이스(116)를 확립하는 범용 이동통신 시스템(UMTS) 지상 라디오 액세스(UTRA)와 같은 무선 기술을 구현할 수 있다. WCDMA는 고속 패킷 액세스(HSPA) 및/또는 진화형 HSPA(HSPA+)와 같은 통신 프로토콜을 포함할 수 있다. HSPA는 고속 다운링크 패킷 액세스(HSDPA) 및/또는 고속 업링크 패킷 액세스(HSUPA)를 포함할 수 있다.

[0015] 다른 실시형태에 있어서, 기지국(114a)과 WTRU(102a, 102b, 102c)는 롱텀 에볼루션(LTE) 및/또는 LTE-어드반스드(LTE-A)를 이용하여 무선 인터페이스(116)를 확립하는 진화형 UMTS 지상 라디오 액세스(E-UTRA)와 같은 무선 기술을 구현할 수 있다.

[0016] 다른 실시형태에 있어서, 기지국(114a)과 WTRU(102a, 102b, 102c)는 IEEE 802.16(즉, WiMAX(Worldwide Interoperability for Microwave Access)), CDMA2000, CDMA2000 1X, CDMA2000 EV-DO, 잠정 표준 2000(IS-2000), 잠정 표준 95(IS-95), 잠정 표준 856(IS-856), 글로벌 이동통신 시스템(GSM), EDGE(Enhanced Data rates for GSM Evolution), GSM EDGE(GERAN) 등과 같은 무선 기술을 구현할 수 있다.

[0017] 도 1a의 기지국(114b)은 예를 들면 무선 라우터, 홈 노드 B, 홈 e노드 B, 또는 접근점일 수 있고, 사업장, 홈, 자동차, 캠퍼스 등과 같은 국소 지역에서 무선 접속을 가능하게 하는 임의의 적당한 RAT를 이용할 수 있다. 일 실시형태에 있어서, 기지국(114b)과 WTRU(102c, 102d)는 IEEE 802.11과 같은 무선 기술을 구현하여 무선 근거리 통신망(WLAN)을 확립할 수 있다. 다른 실시형태에 있어서, 기지국(114b)과 WTRU(102c, 102d)는 IEEE 802.15와 같은 무선 기술을 구현하여 무선 개인 통신망(WPAN)을 확립할 수 있다. 또 다른 실시형태에 있어서, 기지국(114b)과 WTRU(102c, 102d)는 셀룰러 기반 RAT(예를 들면, WCDMA, CDMA2000, GSM, LTE, LTE-A 등)를 이용하여 피코셀 또는 펨토셀을 확립할 수 있다. 도 1a에 도시된 바와 같이, 기지국(114b)은 인터넷(110)에 직접 접속될 수 있다. 그러므로, 기지국(114b)은 코어 네트워크(106)를 통해 인터넷(110)에 접속할 필요가 없다.

[0018] RAN(104)은 코어 네트워크(106)와 통신하고, 코어 네트워크(106)는 하나 이상의 WTRU(102a, 102b, 102c, 102d)에게 음성, 데이터, 애플리케이션 및/또는 인터넷을 통한 음성 프로토콜(voice over internet protocol, VoIP) 서비스를 제공하도록 구성된 임의 유형의 네트워크일 수 있다. 예를 들면, 코어 네트워크(106)는 호출 제어, 빌링(billing) 서비스, 모바일 위치 기반 서비스, 선불 통화, 인터넷 접속, 영상 분배 등을 제공할 수 있고, 및/또는 사용자 인증과 같은 고급 보안 기능을 수행할 수 있다. 비록 도 1a에 도시되어 있지 않지만, RAN(104) 및/또는 코어 네트워크(106)는 RAN(104)과 동일한 RAT 또는 다른 RAT를 이용하는 다른 RAN과 직접 또는 간접 통신을 할 수 있다는 것을 이해할 것이다. 예를 들면, E-UTRA 무선 기술을 이용하는 RAN(104)에 접속되는 것 외에, 코어 네트워크(106)는 GSM 무선 기술을 이용하는 다른 RAN(도시 생략됨)과도 또한 통신할 수 있다.

[0019] 코어 네트워크(106)는 WTRU(102a, 102b, 102c, 102d)가 PSTN(108), 인터넷(110) 및/또는 기타 네트워크(112)에 접속하게 하는 게이트웨이로서 또한 기능할 수 있다. PSTN(108)은 재래식 전화 서비스(plain old telephone service, POTS)를 제공하는 회선 교환식 전화망을 포함할 수 있다. 인터넷(110)은 TCP/IP 인터넷 프로토콜 스위트(suite)에서 전송 제어 프로토콜(TCP), 사용자 데이터그램 프로토콜(UDP) 및 인터넷 프로토콜(IP)과 같은 공통의 통신 프로토콜을 이용하는 상호접속된 컴퓨터 네트워크 및 장치의 글로벌 시스템을 포함할 수 있다. 네트워크(112)는 다른 서비스 공급자에 의해 소유 및/또는 운용되는 유선 또는 무선 통신 네트워크를 포함할 수 있다. 예를 들면, 네트워크(112)는 RAN(104)과 동일한 RAT 또는 다른 RAT를 이용하는 하나 이상의 RAN에 접속된 다른 코어 네트워크를 포함할 수 있다.

[0020] 통신 시스템(100)의 WTRU(102a, 102b, 102c, 102d)의 일부 또는 전부는 다중 모드 능력을 구비할 수 있다. 즉, WTRU(102a, 102b, 102c, 102d)는 다른 무선 링크를 통하여 다른 무선 네트워크와 통신하기 위한 복수의 송수신기를 포함할 수 있다. 예를 들면, 도 1a에 도시된 WTRU(102c)는 셀룰러 기반 무선 기술을 이용할 수 있는 기지국(114a), 및 IEEE 802 무선 기술을 이용할 수 있는 기지국(114b)과 통신하도록 구성될 수 있다.

[0021] 도 1b는 예시적인 WTRU(102)의 계통도이다. 도 1b에 도시된 바와 같이, WTRU(102)는 프로세서(118), 송수신기

(120), 송수신 엘리멘트(122), 스피커/마이크로폰(124), 키패드(126), 디스플레이/터치패드(128), 비분리형 메모리(130), 분리형 메모리(132), 전원(134), 글로벌 위치확인 시스템(GPS) 칩세트(136) 및 기타 주변장치(138)를 포함할 수 있다. WTRU(102)는 실시형태의 일관성을 유지하면서 전술한 요소들의 임의의 부조합(sub-combination)을 포함할 수 있다는 것을 이해할 것이다.

[0022] 프로세서(118)는 범용 프로세서, 특수 용도 프로세서, 전통적 프로세서, 디지털 신호 프로세서(DSP), 복수의 마이크로프로세서, DSP 코어와 연합하는 하나 이상의 마이크로프로세서, 컨트롤러, 마이크로컨트롤러, 용도 지정 집적회로(ASIC), 현장 프로그램가능 게이트 어레이(FPGA) 회로, 임의의 다른 유형의 집적회로(IC), 상태 기계 등일 수 있다. 프로세서(118)는 신호 부호화, 데이터 처리, 전력 제어, 입력/출력 처리, 및/또는 WTRU(102)가 무선 환경에서 동작하게 하는 임의의 다른 기능을 수행할 수 있다. 프로세서(118)는 송수신기(120)에 결합되고, 송수신기(120)는 송수신 엘리멘트(122)에 결합될 수 있다. 비록 도 1b에서는 프로세서(118)와 송수신기(120)가 별도의 구성요소로서 도시되어 있지만, 프로세서(118)와 송수신기(120)는 전자 패키지 또는 칩으로 함께 통합될 수 있음을 이해할 것이다.

[0023] 송수신 엘리멘트(122)는 무선 인터페이스(116)를 통하여 기지국(예를 들면 기지국(114a))에 신호를 송신하거나 기지국으로부터 신호를 수신하도록 구성될 수 있다. 예를 들면, 일 실시형태에 있어서, 송수신 엘리멘트(122)는 RF 신호를 송신 및/또는 수신하도록 구성된 안테나일 수 있다. 다른 실시형태에 있어서, 송수신 엘리멘트(122)는 예를 들면, IR, UV 또는 가시광 신호를 송신 및/또는 수신하도록 구성된 에미터/검지기일 수 있다. 또 다른 실시형태에 있어서, 송수신 엘리멘트(122)는 RF 신호와 광신호 둘 다를 송신 및 수신하도록 구성될 수 있다. 송수신 엘리멘트(122)는 임의의 무선 신호 조합을 송신 및/또는 수신하도록 구성될 수 있다는 것을 이해할 것이다.

[0024] 또한, 비록 송수신 엘리멘트(122)가 도 1b에서 단일 엘리멘트로서 도시되어 있지만, WTRU(102)는 임의 수의 송수신 엘리멘트(122)를 포함할 수 있다. 더 구체적으로, WTRU(102)는 MIMO 기술을 이용할 수 있다. 따라서, 일 실시형태에 있어서, WTRU(102)는 무선 인터페이스(116)를 통해 무선 신호를 송신 및 수신하기 위해 2개 이상의 송수신 엘리멘트(122)(예를 들면, 다중 안테나)를 포함할 수 있다.

[0025] 송수신기(120)는 송수신 엘리멘트(122)에 의해 송신할 신호들을 변조하고 송수신 엘리멘트(122)에 의해 수신된 신호를 복조하도록 구성될 수 있다. 전술한 바와 같이, WTRU(102)는 다중 모드 능력을 구비할 수 있다. 따라서, 송수신기(120)는 WTRU(102)가 예를 들면 UTRA 및 IEEE 802.11과 같은 복수의 RAT를 통하여 통신하게 하는 복수의 송수신기를 포함할 수 있다.

[0026] WTRU(102)의 프로세서(118)는 스피커/마이크로폰(124), 키패드(126), 및/또는 디스플레이/터치패드(128)(예를 들면, 액정 디스플레이(LCD) 표시 장치 또는 유기 발광 다이오드(OLED) 표시 장치)에 결합되어 이들로부터 사용자 입력 데이터를 수신할 수 있다. 프로세서(118)는 또한 스피커/마이크로폰(124), 키패드(126), 및/또는 디스플레이/터치패드(128)에 사용자 데이터를 출력할 수 있다. 또한, 프로세서(118)는 비분리형 메모리(130) 및/또는 분리형 메모리(132)와 같은 임의 유형의 적당한 메모리로부터의 정보에 액세스하고 상기 적당한 메모리에 데이터를 저장할 수 있다. 비분리형 메모리(130)는 랜덤 액세스 메모리(RAM), 읽기 전용 메모리(ROM), 하드 디스크 또는 임의의 다른 유형의 메모리 기억장치를 포함할 수 있다. 분리형 메모리(132)는 가입자 식별 모듈(SIM) 카드, 메모리 스틱, 보안 디지털(SD) 메모리 카드 등을 포함할 수 있다. 다른 실시형태에 있어서, 프로세서(118)는 서버 또는 홈 컴퓨터(도시 생략됨)와 같이 물리적으로 WTRU(102)에 위치되어 있지 않은 메모리로부터의 정보에 액세스하고 그러한 메모리에 데이터를 저장할 수 있다.

[0027] 프로세서(118)는 전원(134)으로부터 전력을 수신하고, WTRU(102)의 각종 구성요소에 대하여 전력을 분배 및/또는 제어하도록 구성될 수 있다. 전원(134)은 WTRU(102)에 전력을 공급하는 임의의 적당한 장치일 수 있다. 예를 들면, 전원(134)은 하나 이상의 건전지 배터리(예를 들면, 니켈-카드뮴(NiCd), 니켈-아연(NiZn), 니켈 금속 하이드라이드(NiMH), 리튬-이온(Li-ion) 등), 태양 전지, 연료 전지 등을 포함할 수 있다.

[0028] 프로세서(118)는 WTRU(102)의 현재 위치에 관한 위치 정보(예를 들면, 경도 및 위도)를 제공하도록 구성된 GPS 칩세트(136)에 또한 결합될 수 있다. GPS 칩세트(136)로부터의 정보에 추가해서 또는 그 대신으로, WTRU(102)는 기지국(예를 들면 기지국(114a, 114b))으로부터 무선 인터페이스(116)를 통해 위치 정보를 수신하고, 및/또는 2개 이상의 인근 기지국으로부터 신호가 수신되는 타이밍에 기초하여 그 위치를 결정할 수 있다. WTRU(102)는 실시형태의 일관성을 유지하면서 임의의 적당한 위치 결정 방법에 의해 위치 정보를 획득할 수 있다는 것을 이해할 것이다.

[0029] 프로세서(118)는 추가의 특징, 기능, 및/또는 유선 또는 무선 접속을 제공하는 하나 이상의 소프트웨어 및/또는 하드웨어 모듈을 포함한 기타 주변 장치(138)에 또한 결합될 수 있다. 예를 들면, 주변 장치(138)는 가속도계, e-콤파스, 위성 송수신기, 디지털 카메라(사진용 또는 영상용), 범용 직렬 버스(USB) 포트, 진동 장치, 텔레비전 송수신기, 핸즈프리 헤드셋, 블루투스® 모듈, 주파수 변조(FM) 라디오 장치, 디지털 뮤직 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저 등을 포함할 수 있다.

[0030] 도 1c는 일 실시형태에 따른 RAN(104) 및 코어 네트워크(106)의 계통도이다. 전술한 바와 같이, RAN(104)은 E-UTRA 라디오 기술을 이용하여 무선 인터페이스(116)를 통해 WTRU(102a, 102b, 102c)와 통신할 수 있다. RAN(104)은 코어 네트워크(106)와 또한 통신할 수 있다.

[0031] RAN(104)이 e노드-B(140a, 140b, 140c)를 포함하고 있지만, RAN(104)은 실시형태의 일관성을 유지하면서 임의 수의 e노드-B를 포함할 수 있다는 것을 이해할 것이다. e노드-B(140a, 140b, 140c)는 무선 인터페이스(116)를 통하여 WTRU(102a, 102b, 102c)와 통신하는 하나 이상의 송수신기를 각각 포함할 수 있다. 일 실시형태에 있어서, e노드-B(140a, 140b, 140c)는 MIMO 기술을 구현할 수 있다. 따라서, 예를 들면 e노드-B(140a)는 복수의 안테나를 사용하여 WTRU(102a)에게 무선 신호를 송신하고 WTRU(102a)로부터 무선 신호를 수신할 수 있다.

[0032] 각각의 e노드-B(140a, 140b, 140c)는 특정 셀(도시 생략됨)과 연합될 수 있고, 무선 자원 관리 결정, 핸드오버 결정, 업링크 및/또는 다운링크에서 사용자의 스케줄링 등을 취급하도록 구성될 수 있다. 도 1c에 도시된 바와 같이, e노드-B(140a, 140b, 140c)는 X2 인터페이스를 통해 서로 통신할 수 있다.

[0033] 도 1c에 도시된 코어 네트워크(106)는 이동도 관리 게이트웨이(MME)(142), 서빙 게이트웨이(144) 및 패킷 데이터 네트워크(PDN) 게이트웨이(146)를 포함할 수 있다. 전술한 요소들이 각각 코어 네트워크(106)의 일부로서 도시되어 있지만, 이 요소들 중 임의의 요소는 코어 네트워크 운용자가 아닌 다른 엔티티에 의해 소유 및/또는 운용될 수 있다는 것을 이해할 것이다.

[0034] MME(142)는 S1 인터페이스를 통해 RAN(104) 내의 각각의 e노드-B(140a, 140b, 140c)에 접속될 수 있고, 제어 노드로서 기능할 수 있다. 예를 들면, MME(142)는 WTRU(102a, 102b, 102c)의 사용자를 인증하고, 베어러를 활성화/비활성화하고, WTRU(102a, 102b, 102c)의 초기 부착 중에 특정 서빙 게이트웨이를 선택하는 등의 임무를 수행할 수 있다. MME(142)는 또한 GSM 또는 WCDMA와 같은 다른 무선 기술을 이용하는 다른 RAN(도시 생략됨)과 RAN(104) 간의 스위칭을 위한 제어 평면 기능(control plane function)을 또한 제공할 수 있다.

[0035] 서빙 게이트웨이(144)는 RAN(104) 내의 각각의 e노드-B(140a, 140b, 140c)에 S1 인터페이스를 통해 접속될 수 있다. 서빙 게이트웨이(144)는 일반적으로 WTRU(102a, 102b, 102c)로/로부터 사용자 데이터 패킷을 라우트 및 포워딩할 수 있다. 서빙 게이트웨이(144)는 또한 e노드-B 간의 핸드오버 중에 사용자 평면(user plane)을 고정(anchoring)하는 것, 다운링크 데이터가 WTRU(102a, 102b, 102c)에 이용할 수 있을 때 페이징을 트리거하는 것, WTRU(102a, 102b, 102c)의 콘텍스트를 관리 및 저장하는 것 등의 다른 기능을 수행할 수 있다.

[0036] 서빙 게이트웨이(144)는 PDN 게이트웨이(146)에 또한 접속될 수 있고, PDN 게이트웨이(146)는 WTRU(102a, 102b, 102c)와 IP-인에이블 장치 간의 통신이 가능하도록 인터넷(110)과 같은 패킷 교환식 네트워크에 대한 액세스를 WTRU(102a, 102b, 102c)에게 제공할 수 있다.

[0037] 코어 네트워크(106)는 다른 네트워크와의 통신을 가능하게 한다. 예를 들면, 코어 네트워크(106)는 WTRU(102a, 102b, 102c)와 전통적인 지상선(land-line) 통신 장치 간의 통신이 가능하도록, PSTN(108)과 같은 회선 교환식 네트워크에 대한 액세스를 WTRU(102a, 102b, 102c)에게 제공할 수 있다. 예를 들면, 코어 네트워크(106)는 코어 네트워크(106)와 PSTN(108) 간의 인터페이스로서 기능하는 IP 게이트웨이(예를 들면, IP 멀티미디어 서브시스템(IMS) 서버)를 포함하거나 그러한 IP 게이트웨이와 통신할 수 있다. 또한, 코어 네트워크(106)는 다른 서비스 공급자에 의해 소유 및/또는 운용되는 다른 유선 또는 무선 네트워크를 포함하는 네트워크(112)에 대한 액세스를 WTRU(102a, 102b, 102c)에게 제공할 수 있다.

[0038] 이하에서, 용어 "애플리케이션"은 모바일 네트워크 운용자 또는 제3자가 모바일 가입자에게 제공하는 서비스를 의미한다. 용어 "애플리케이션 서버"(AS) 및 "애플리케이션 플랫폼"은 상호 교환적으로 사용된다. 애플리케이션 플랫폼은 비디오-온-디맨드 서버, PSS 서버, MTC 서버 등과 같은 AS이다. 대안적으로 애플리케이션 플랫폼은 소프트웨어 개발 플랫폼일 수 있다.

[0039] 홈 공중 육상 모바일 네트워크(HPLMN)는 특정 사용자가 그 가입자로 되는 셀룰러 네트워크이다. 방문형 공중 육상 모바일 네트워크(VPLMN)는 가입자가 그 가입자가 아니지만 현재 등록되어 있는 셀룰러 네트워크이다. 용어

"HPLMN"과 "홈 네트워크"는 상호 교환적으로 사용되고, 용어 "VPLMN"과 "방문 네트워크"는 상호 교환적으로 사용될 것이다.

[0040] 도면에서, AS는 방문 네트워크에 또는 홈 네트워크에 위치되는 것으로 도시되지만, AS는 방문 네트워크 또는 홈 네트워크의 내측 또는 외측의 어디에도 위치될 수 있다는 점에 주목하여야 한다.

[0041] 이하에서는 AS가 폴리싱, 과금 및 사용자 데이터 획득을 위해 방문 네트워크와 상호접속하는 방식으로 애플리케이션 공급자가 방문 네트워크(즉, VPLMN) 운용자와 협약(agreement)을 갖는 경우의 실시형태에 대하여 설명한다. 애플리케이션 공급자는 홈 네트워크(즉, HPLMN) 운용자와 협약을 가질 수도 있고 갖지 않을 수도 있다.

[0042] 일 실시형태에 있어서, AS 대 VPLMN 상호접속 및 eSh-프록시가 폴리싱, 과금 및 사용자 데이터 획득을 위해 사용될 수 있다. 도 2는 AS가 VPLMN과 상호접속된 경우의 예시적인 네트워크 아키텍처를 보인 것이다. AS(210)(예를 들면, 비-IMS AS)는 애플리케이션 공급자의 제어하에 있다. 대안적으로, AS(210)는 VPLMN 운용자의 제어하에 있을 수 있다. WTRU(205)는 VPLMN(220)에서 로밍한다. VPLMN(220)은 다른 무엇보다도 특히 vPCRF(222), eSh-프록시(224), PGW(226), SGW(227), MME(228), 및 eNB(229)를 포함한다. HPLMN(230)은 다른 무엇보다도 특히 hPCRF(232), 사용자 데이터 저장소(UDR)(233), eSh-프록시(234), 가입자 로케이터 기능(subscriber locator function, SLF)(235), HSS-FE(236), 부트스트래핑 서버 기능(BSF)(237) 및 네트워크 애플리케이션 기능(NAF)(238)을 포함한다. BSF(237)와 NAF(238)는 일반 부트스트래핑 아키텍처(Generic Bootstrapping Architecture, GBA)의 일부이다. BSF(237)와 WTRU(205)는 인증 및 키 협약(Authentication and Key Agreement, AKA) 프로토콜을 이용하여 상호 인증하고, 나중에 WTRU(205)와 NAF(238) 사이에 적용되는 세션 키에 대하여 협의한다. SLF(235)는 가입자 특정 데이터를 포함한 HSS의 명칭을 취득하기 위해 Dz 인터페이스를 통해 BSF(237)에 의해 질의된다. SLF(235)는 하나의 HSS만 있거나 BSF(237)가 미리 규정된 HSS에 의해 구성 또는 관리되는 경우에는 필요 없을 수 있다. UDR(233)은 사용자 데이터가 일반적인 방법으로 접근, 저장 및 관리될 수 있는 설비이다. 프론트 엔드(front end, FE)는 저장소에 저장된 사용자 데이터에 접근할 수 있는 코어 네트워크 기능 엔티티 또는 서비스 계층 엔티티 또는 공급 엔티티(provisioning entity)이다.

[0043] WTRU(205)의 사용자는 예를 들면 서비스 가격 및/또는 조건에 대하여 사용자에게 통보할 수 있는 웹 포털을 통하여 애플리케이션 공급자가 제공하는 서비스에 대한 정보를 획득한다. 그 다음에, 사용자는 서비스 자원 위치 지정자(uniform resource locator, URL)에 대한 링크에서 클릭할 수 있다. 그 다음에 요청이 하이퍼 텍스트 운송 프로토콜(HTTP), 보안 HTTP(HTTPS), 세션 개시 프로토콜(SIP), 보안 SIP(SIPS) 등을 이용하여 WTRU(205)로부터 AS로 전송될 수 있다. AS(210)는 사용자의 인증을 위해 오픈ID 공급자(OP)와 같은 인증 서버(도시 생략됨)를 향해 WTRU(205)를 재지향시킬 수 있다.

[0044] 인증 서버는 NAF(238)와 공존되거나 NAF(238)와 통신할 수 있다. GBA는 인증 목적으로, 및 WTRU(205)와 NAF(238) 간에 통신 경로를 확보하기 위해 NAF(238)와 WTRU(205) 사이에서 사용될 수 있다. 부트스트래핑이 완료된 후에, WTRU(205)와 NAF(238)는 메시지를 획득할 때 WTRU(205)와 BSF(237) 사이에서 인증 중에 생성된 세션 키를 이용할 수 있다. NAF(238)는 만일 NAF238)가 홈 네트워크에 위치하고 있으면 직접, 또는 NAF가 방문 네트워크에 위치하고 있으면 Zn-프록시를 통하여 홈 BSF(237)와 통신할 수 있다. 도 2는 NAF(238)가 HPLMN(230)에 위치하고 있는 경우를 도시하고 있지만, NAF는 VPLMN(220)에 또는 외부 네트워크에 위치될 수 있다. NAF(238)가 HPLMN(230)에 위치하고 있지 않을 때는 Zn-프록시가 사용될 수 있다. Zn-프록시는 방문 NAF와 가입자의 홈 BSF 간의 프록시 기능이다. Zn-프록시는 WTRU가 홈 네트워크가 아닌 다른 네트워크에서 로밍하는 경우에 방문 NAF에 의해 사용될 수 있다.

[0045] WTRU(205)가 AS(210)에 의해 인증되면, AS(210)는 방문 폴리시 제어 규칙 기능(visited Policy Control rules Function, vPCRF)(222)에 대한 그 Rx 인터페이스를 이용하여 서비스에 대한 폴리시 및 과금을 제어할 수 있다. Rx 기준점은 애플리케이션 기능(AF)과 PCRF 사이에 존재한다. Rx 기준점은 AF로부터 PCRF로 애플리케이션 레벨 세션 정보의 운송을 가능하게 한다. 그러한 정보는 비제한적인 예를 들자면 폴리시 제어 및/또는 차별화된 과금을 위한 서비스 데이터 흐름, 서비스 품질(QoS) 제어를 위한 미디어/애플리케이션 대역폭 필요조건 등을 식별하는 IP 필터 정보를 포함한다. vPCRF(222)는 AS(210)로부터의 Rx 메시지를 S9를 통해 홈 폴리시 제어 규칙 기능(hPCRF)(232)으로 포워딩할 수 있다. hPCRF(232)는 사용자 가입 정보를 획득하고, 그 다음에 AS(210)에게 응답하는 vPCRF(222)에게 응답을 보낼 수 있다. hPCRF(232)는 S9를 이용해서 및 vPCRF(222)를 통하여 폴리시 및 과금 강화 기능(Policy and Charging Enforcement Function, PCEF)/베어러 결합 및 이벤트 보고 기능(Bearer Binding and Event Reporting Function, BBERF)과 상호작용할 수 있다.

[0046] AS(210)가 사용자 데이터(예를 들면, 사용자 프로필)에 접근할 필요가 있을 때, AS(210)는 강화된 Sh(enhanced Sh, eSh) 인터페이스를 이용할 수 있다. Sh 인터페이스는 AS(210)와 HSS-FE(236) 간에 사용자 프로필 정보(예를 들면, 사용자 관련 데이터, 그룹 리스트, 사용자 서비스 관련 정보, 사용자 위치 정보, 또는 과금 기능 어드레스 등)를 교환하기 위해 사용된다. 일 실시형태에 있어서, 종래의 Sh 인터페이스는 운용자 네트워크의 경계 밖에서 사용되도록 강화된다(예를 들면, 보안화 된다).

[0047] 사용자 데이터는 홈 네트워크로부터 획득될 수 있다. AS(210)는 인증 절차(예를 들면, GBA/오픈ID 절차) 중에 획득된 이동국 국제 가입자 디렉토리 번호(Mobile Station International Subscriber Directory Number, MSISDN)를 이용하여 eSh를 통해 사용자를 식별할 수 있다.

[0048] eSh 인터페이스에 대한 운용자 간 통신을 가능하게 하기 위해 새로운 Sh-프록시 네트워크 기능(eSh-프록시)(224, 234)이 도입된다. eSh-프록시(224, 234)는 사용자 정보의 기밀성을 보장하기 위해 보안 방식으로 VPLMN(220)과 HPLMN(230) 간에 eSh 메시지를 중계할 수 있다. 새로운 Shp 기준점(eSh)은 eSh-프록시(224, 234)들 간에 eSh 프로토콜 메시지를 중계하기 위해 도입된다. eShp 기준점은 eSh-프록시(224, 234)들 간에 안전한 상호접속을 구성하기 위해 사용될 수 있다. eShp 기준점은 폴리시와 같은 다른 정보를 교환하기 위해 사용될 수 있다.

[0049] eSh-프록시(224, 234)는 VPLMN(220)과 HPLMN(230) 간의 애플리케이션 로밍 협약으로부터 도출된 폴리시를 강화할 수 있다. 예를 들면, 소정 부류의 애플리케이션은 사용자 데이터에 대한 접근을 획득할 수 있고, 이것은 eSh-프록시(224, 234)에 의해 강화될 수 있다. eSh-프록시(224, 234)는 HPLMN(230)으로부터의 권한부여(authorization)에 기초하여 사용자 데이터 접근의 범위를 제한할 수 있다(예를 들면, 사용자 프로필 또는 홈 네트워크 폴리시는 방문 네트워크 애플리케이션에 의해 접근가능한 사용자 데이터의 유형을 제한할 수 있다). eSh-프록시(224, 234)는 운용자 간 협약의 검증을 가능하게 하는 동작(예를 들면, 부피로) 또는 애플리케이션 공급자의 빌링(billing)(운용자 간 Shp 인터페이스의 사용량에 대해)을 가능하게 하는 동작들을 기록할 수 있다.

[0050] AS(210)는 AS(210)가 필요할 때 eSh-프록시(224)를 이용하여 사용자 데이터에 접근하는 결정을 할 수 있도록 소정의 사용자가 네트워크에 방문하고 있는지를 결정할 수 있다. 만일 사용자가 VPLMN(220)의 가입자이면(즉, 사용자가 VPLMN(220)에 방문하지 않는다), AS(210)는 VPLMN HSS(도시 생략됨)와 대신 통신하여 사용자 데이터를 획득할 수 있다.

[0051] 일 실시형태에 있어서, WTRU(205)가 VPLMN(220)에 방문중인지 여부를 결정하기 위해, AS(210)는 임의의 사용자 데이터에 접근하기 전에 PCRF에 대한 Rx 인터페이스를 이용할 수 있고, Rx 초기 세션 개시 응답 메시지로부터, AS(210)는 hPCRF(232)의 디아미터 영역(Diameter realm) 및 호스트명을 획득할 수 있다. AS(210)는 이 정보를 그 구성과 비교하고, PCRF 엔드포인트가 VPLMN(220) 내에 없다고 결정할 수 있다. 이것에 대해서는 아래에서 도 3a 및 도 3b를 참조하여 또한 설명된다. AS(210)는 그 다음에 eSh-프록시(224)와 통신할 필요가 있다고 결정할 수 있다. AS(210)는 eSh-프록시(224)와 통신할 때 영역 정보를 이용할 수 있다(또는 대안적으로, 호스트명으로부터 획득된 도메인명을 이용할 수 있다). 예를 들면, AS(210)는 디아미터 목적지 영역(Diameter Destination-Realm)을 hPCRF(232)로부터 획득된 값으로 설정할 수 있다. 디아미터 목적지 영역은 디아미터 아이덴티티 유형의 것이고, 메시지가 라우트되어야 하는 영역을 포함한다. eSh-프록시(224)는 HPLMN(230)에 위치하고 있는 피어 eSh-프록시(234)와 상기 정보 간에 맵핑을 유지한다.

[0052] 다른 실시형태에 있어서, WTRU(205)의 홈 네트워크를 결정하기 위한 충분한 정보를 AS(210)에게 제공하기 위해 GBA/오픈ID 통합을 사용할 수 있다. 예를 들면, 오픈ID 공급자/NAF는 오픈ID 절차 중에 AS(210)에게 WTRU(205)의 MSISDN을 제공할 수 있다. AS(210)는 그 다음에 룩업 서비스를 이용하여 MSISDN에 대한 홈 네트워크 아이덴티티를 획득할 수 있다.

[0053] 오픈ID 공급자/NAF에 의해 AS(210)에게 제공될 수 있는 운용자 특정 신원(identification)은 MSISDN 또는 부트스트랩 거래 ID(Bootstrap Transaction ID, B-TID)이다. B-TID는 기준점(Ua, Ub, Zn)의 키 재료에 가입자 아이덴티티를 결합하기 위해 사용된다. 대안적으로, 오픈ID 공급자/NAF는 홈 네트워크 신원을 MSISDN 또는 B-TID 외에 AS(210)에게 제공할 수 있다. 홈 네트워크 신원은 예를 들면 모바일 네트워크 코드(MNC) + 모바일 국가 코드(MCC), 또는 eSh-프록시가 특정 PLMN과 연합할 수 있는 디아미터 영역일 수 있다.

[0054] 전술한 실시형태 및 설명은 이하에서 설명하는 임의의 실시형태에도 적용할 수 있다는 점에 주목하여야 한다.

[0055] 도 3a 및 도 3b는 일 실시형태에 따라서, 애플리케이션 공급자가 방문 네트워크 운용자와의 협약을 갖지만 홈

네트워크 운용자와의 협약을 갖지 않는 경우에 인증, 세션 폴리시/과금 개시 및 사용자 데이터 요청을 위한 예시적인 처리의 신호도이다. VPLMN(220)과 HPLMN(230)의 eSh-프록시(224, 234)들 간에 통신이 확립된다(302). VPLMN(220)의 eSh-프록시(224)와 AS(210) 간에도 또한 통신이 확립된다(304). eSh-프록시 대 eSh-프록시 및 eSh-프록시 대 AS의 통신은 미리 확립될 수도 있고, 또는 대안적으로 온디맨드(on-demand)로 확립될 수도 있다.

[0056] WTRU(205)는 서비스 요청을 AS(210)에게 보낸다(306). WTRU(205)와 AS(210) 간에 인증 절차가 수행되고, 이것은 다른 노드를 또한 수반한다(308). WTRU가 인증되면, AS(210)는 서비스를 WTRU(205)에게 제공하도록 결정한다(310).

[0057] AS(210)는 새로운 Rx 디아미터 세션에 대한 디아미터 AA-요청(AAR)을 보냄으로써 vPCRF(222)에게 세션 정보를 제공한다(312). vPCRF(222)는 세션 정보를 저장하고 디아미터 AAR을 hPCRF(232)에게 포워딩한다(314). vPCRF(222)는 운용자 폴리시를 이용하고, 만일 제공된 세션 정보가 수용불능이면 AS(210)로부터의 AAR을 거절할 수 있다. hPCRF(232)는 수신된 세션 정보를 저장하고, 디아미터 AA-응답(AAA)으로 vPCRF(222)에게 응답한다(316). 만일 hPCRF(232)가 가입 관련 정보를 요구하고 그 정보를 갖지 않으면, hPCRF(232)는 허용된 서비스, 서비스 품질(QoS) 정보, 폴리시 및 과금 제어(PCC) 규칙 정보 등을 포함한 정보를 수신하기 위해 가입자 폴리시 레지스터(SPR)에게 요청을 보낸다. vPCRF(222)는 디아미터 AAA를 AS(210)에게 포워딩한다(318). hPCRF(232)는 PCRF 개시형 IP-CAN 세션 수정을 위해 vPCRF(222)를 통하여 폴리시 및 과금 강화 기능(PCEF)/베어러 결합 및 이벤트 보고 기능(BBERF)과 상호작용할 수 있다(320, 322, 324).

[0058] Rx 응답(즉, 디아미터 AAA)에 기초해서, AS(210)는 WTRU(205)가 VPLMN(220)에 방문중임을 검출할 수 있다(326). WTRU(205)가 VPLMN(220)에 방문중인지를 결정하기 위해 상기와는 다른 방법을 사용할 수 있다는 점에 주목하여야 한다.

[0059] AS(210)는 사용자 데이터에 접근하도록 결정하고 사용자 데이터 요청을 eSh-프록시(224)에게 보낸다(328, 330). 사용자 데이터 요청은 HPLMN 영역 또는 도메인을 포함할 수 있고, AS(210)에 의해 eSh-프록시(224)에게 제공된 정보는 eSh-프록시와 통신하는 HPLMN을 알아낼 수 있게 한다.

[0060] eSh-프록시(224)는 WTRU(205)와 연합하는 eSh-프록시를 검출하고, AS(210)가 HPLMN으로부터 이 유형의 데이터를 검색하도록 허용되는지를 체크할 수 있다(332). 그 다음에, eSh-프록시(224)는 사용자 데이터 요청을 HPLMN(230)의 eSh-프록시(234)에게 보낸다(334). eSh-프록시(234)는 AS(210)가 HPLMN 및/또는 사용자로부터 데이터를 검색하도록 허용되는지를 또한 체크할 수 있다(336). 만일 허용된다고 결정되면, eSh-프록시(234)는 사용자 데이터 요청을 홈 가입자 서버(HSS)(236)에게 보낸다(338). 그 다음에, eSh-프록시(234, 224)를 통해 HSS(236)로부터 AS(210)에게로 사용자 데이터 응답이 전송된다(340).

[0061] 이하에서는 AS가 폴리싱, 과금 및 사용자 데이터 획득을 위해 홈 네트워크 및/또는 방문 네트워크와 상호접속하는 방식으로 애플리케이션 공급자가 홈 네트워크 운용자 및 방문 네트워크 운용자 양자와의 협약을 갖는 경우의 실시형태에 대하여 설명한다.

[0062] 도 4는 AS가 홈 네트워크 및 방문 네트워크 양자에 상호 접속된 예시적인 네트워크 아키텍처를 보인 것이다. AS(410)는 전술한 임의의 방법을 이용하여 WTRU(405)가 VPLMN(420)에 방문중인지를 검출할 수 있다. AS(410)는 예를 들면 WTRU(405)가 VPLMN(420)에 방문중인지를 결정하기 위한 정보를 AS(410)가 갖지만 그 HPLMN이 어떤 것인지를 알기 위한 충분한 정보를 갖지 않은 경우에, WTRU(405)의 HPLMN을 획득하기 위해 eSh-프록시(424)와 추가로 통신할 수 있다. AS(410)는 VPLMN(420) 및 HPLMN(430) 양자와 상호접속된다. AS(410)는 애플리케이션 공급자의 제어하에 있을 수 있다. 대안적으로, AS(410)는 VPLMN 네트워크 운용자의 제어하에 있을 수 있다.

[0063] 만일 AS(410)가 그 내부 상태 또는 구성에 기초하여, AS(410)가 HPLMN(430)과의 협약을 또한 갖는다는 것을 인식하면, AS(410)는 HPLMN(430)에 대한 그 직접 상호접속을 이용하여 서비스를 제공하도록 선택할 수 있다. 대안적으로, AS(410)는 그 VPLMN 상호접속을 이용하도록 대신 선택할 수 있다. 이 경우에, AS(410)는 VPLMN의 PGW(426)를 통하여 라우트되는 트래픽을 위하여 VPLMN 상호접속을 이용하는 폴리시를 따를 수 있다.

[0064] 도 4는 NAF(438)가 HPLMN(430)에 위치된 것을 도시하고 있지만, NAF는 VPLMN(420)에 또는 외부 네트워크에 또한 위치될 수 있다. NAF(438)가 HPLMN(430)에 위치되어 있지 않을 때, Zn-프록시가 사용될 수 있다. 오픈ID 인증 서버는 NAF 및 Zn-프록시 기능을 통합할 수 있다.

[0065] 도 5a 내지 도 5c는 애플리케이션 공급자가 홈 네트워크 운용자 및 방문 네트워크 운용자 양자와의 협약을 갖는 경우에 인증, 세션 폴리시/과금 개시 및 사용자 데이터 요청을 위한 예시적인 처리의 신호도이다. VPLMN(420)과 HPLMN(430)의 eSh-프록시(424, 434)들 간에 통신이 확립된다(502). VPLMN(420)의 eSh-프록시(424)와 AS(410)

간에도 또한 통신이 확립된다(504). eSh-프록시 대 eSh-프록시 및 eSh-프록시 대 AS의 통신은 미리 확립될 수도 있고, 또는 대안적으로 온디맨드로 확립될 수도 있다.

[0066] WTRU(405)는 서비스 요청을 AS(410)에게 보낸다(506). WTRU(405)와 AS(410) 간에 인증 절차가 수행되고, 이것은 다른 노드를 또한 수반한다(508). WTRU가 인증되면, AS(410)는 서비스를 WTRU(405)에게 제공하도록 결정한다(510).

[0067] AS(410)는 새로운 Rx 디아미터 세션에 대한 디아미터 AAR을 보냄으로써 vPCRF(422)에게 세션 정보를 제공한다(512). vPCRF(422)는 세션 정보를 저장하고 디아미터 AAR을 hPCRF(432)에게 포워딩한다(514). vPCRF(422)는 운용자 폴리시를 이용하고, 만일 제공된 세션 정보가 수용불능이면 AS(410)로부터의 AAR을 거절할 수 있다. hPCRF(432)는 수신된 세션 정보를 저장하고, 디아미터 AAA로 vPCRF(422)에게 응답한다(516). 만일 hPCRF(432)가 가입 관련 정보를 요구하고 그 정보를 갖지 않으면, hPCRF(432)는 허용된 서비스, QoS 정보, PCC 규칙 정보 등을 포함한 정보를 수신하기 위해 SPR에게 요청을 보낸다. vPCRF(422)는 디아미터 AAA를 AS(410)에게 포워딩한다(518). hPCRF(432)는 PCRF 개시형 IP-CAN 세션 수정을 위해 vPCRF(422)를 통하여 PCEF/BBERF와 상호작용할 수 있다(520, 522, 524).

[0068] Rx 응답(즉, 디아미터 AAA)에 기초해서, AS(410)는 WTRU(405)가 VPLMN(420)에 방문중인지를 검출할 수 있다(526). WTRU(405)가 VPLMN(420)에 방문중인지를 결정하기 위해 상기와는 다른 방법을 사용할 수 있다는 점에 주목하여야 한다.

[0069] AS(410)는 WTRU(405)의 HPLMN을 결정하기 위한 충분한 정보를 가질 수도 있고 갖지 않을 수도 있다. AS(410)가 WTRU(405)의 HPLMN을 결정하기 위한 충분한 정보를 갖지 않으면, AS(410)는 사용자 데이터 요청을 eSh-프록시(424)에게 보낼 수 있다(528). 사용자 데이터 요청은 HPLMN 영역 또는 도메인을 포함할 수 있고, AS(410)에 의해 eSh-프록시(424)에게 제공된 정보는 eSh-프록시와 통신하는 HPLMN을 알아낼 수 있게 한다. eSh-프록시(424)는 WTRU(405)와 연합하는 eSh-프록시를 검출하고, AS(410)가 HPLMN으로부터 이 유형의 데이터를 검색하도록 허용되는지를 체크할 수 있다(530). 그 다음에, eSh-프록시(424)는 사용자 데이터 요청을 HPLMN(430)의 eSh-프록시(434)에게 보낸다(532). eSh-프록시(434)는 AS(410)가 HPLMN 및/또는 사용자로부터 데이터를 검색하도록 허용되는지를 또한 체크할 수 있다(534). 만일 허용된다고 결정되면, eSh-프록시(434)는 사용자 데이터 요청을 HSS(436)에게 보낸다(536). 그 다음에, eSh-프록시(434, 424)를 통해 HSS(436)로부터 AS(410)에게로 사용자 데이터 응답이 포워딩된다(538). 만일 AS(410)가 WTRU(405)의 HPLMN을 결정하기 위한 충분한 정보를 갖고 있으면, 단계 528-538은 생략될 수 있다.

[0070] WTRU(405)의 HPLMN이 결정된 때, AS(410)는 AS(410)가 HPLMN(430)과의 협약을 갖고 있음을 검출한다(540). 일실시형태에 있어서, AS(410)는 HPLMN(430)과 그 직접 Rx/eSh 인터페이스를 사용하도록 선택할 수 있다(542a). AS(410)는 vPCRF(422)를 통한 IP-CAN 세션을 먼저 종결할 수 있다. 대안적으로, AS(410)는 VPLMN(420)과 그 Rx/eSh 인터페이스를 사용하도록 선택할 수 있다(542b). 대안적으로, AS(410)는 VPLMN(420)에 대하여 Rx의 사용을 계속하고, HPLMN(430)에 대하여 eSh의 사용을 시작하도록 선택할 수 있다(542c). 대안적으로, AS(410)는 VPLMN(420)에 대하여 eSh의 사용을 계속하고(eSh-프록시를 통하여), HPLMN(430)에 대하여 Rx의 사용을 시작하도록 선택할 수 있다(542d). 만일 Rx가 이전에 사용되었으면, AS(410)는 vPCRF(422)를 통한 IP-CAN 세션을 종결할 수 있다.

[0071] 만일 HPLMN(430)에 대한 관계를 가진 협력 AS에 의해 동일한 서비스가 제공될 수 있음을 AS(410)가 인식하면, AS(410)는 예를 들면 HTTP 재지향과 같은 애플리케이션 레벨 재지향을 이용하여 사용자를 협력 AS에게 재지향시키도록 선택할 수 있다.

[0072] 도 6은 애플리케이션 공급자가 복수의 애플리케이션 서버를 전개하는 예시적인 네트워크 아키텍처를 보인 도이다. AS(610)는 VPLMN(620)과 상호접속되고 다른 AS(640)는 HPLMN(630)과 상호접속된다. 애플리케이션 서버(610, 640)는 애플리케이션 공급자의 제어하에 있을 수 있고, 또는 대안적으로 네트워크 운용자의 제어하에 있을 수도 있다. 도 6은 NAF가 HPLMN(630)에 위치된 것을 도시하고 있지만, NAF는 VPLMN(620)에 또는 외부 네트워크에 위치될 수 있다. NAF가 HPLMN(630)에 위치되어 있지 않을 때, Zn-프록시가 사용될 수 있다. 오픈ID 인증 서버는 NAF 및 Zn-프록시 기능을 통합할 수 있다. 애플리케이션 공급자는 방문 네트워크의 AS(610)에 접근하려고 시도하는 로밍 사용자가 그 홈 네트워크에 대하여 서빙하는 AS(610)에게 재지향되는 것을 보장하기 위해 재지향을 사용할 수 있다.

[0073] 도 7a 및 도 7b는 사용자를 VPLMN(620)에 서빙하는 AS(610)로부터 HPLMN(630)에 서빙하는 AS(640)로 재지향시

키기 위한 예시적인 처리에 관한 신호도이다. VPLMN(620)과 HPLMN(630)의 eSh-프록시(624, 634)들 간에 통신이 확립된다(702). VPLMN(620)의 eSh-프록시(624)와 AS(610) 간에도 또한 통신이 확립된다(704). eSh-프록시 대 eSh-프록시 및 eSh-프록시 대 AS의 통신은 미리 확립될 수도 있고, 또는 대안적으로 온디맨드로 확립될 수도 있다.

[0074] WTRU(605)는 서비스 요청을 AS(610)에게 보낸다(706). WTRU(605)와 AS(610) 간에 인증 절차가 수행되고, 이것은 다른 노드를 또한 수반한다(708). WTRU가 인증되면, AS(610)는 서비스를 WTRU(605)에게 제공하도록 결정한다(710).

[0075] AS(610)는 새로운 Rx 디아미터 세션에 대한 디아미터 AAR을 보냄으로써 vPCRF(622)에게 세션 정보를 제공한다(712). vPCRF(622)는 세션 정보를 저장하고 디아미터 AAR을 hPCRF(632)에게 포워딩한다(714). vPCRF(622)는 운용자 폴리시를 이용하고, 만일 제공된 세션 정보가 수용불능이면 AS(610)로부터의 AAR을 거절할 수 있다. hPCRF(632)는 수신된 세션 정보를 저장하고, 디아미터 AAA로 vPCRF(622)에게 응답한다(716). 만일 hPCRF(632)가 가입 관련 정보를 요구하고 그 정보를 갖지 않으면, hPCRF(632)는 허용된 서비스, QoS 정보 및 PCC 규칙 정보를 포함한 정보를 수신하기 위해 가입자 폴리시 레지스터(SPR)에게 요청을 보낸다. vPCRF(622)는 디아미터 AAA를 AS(610)에게 포워딩한다(718). hPCRF(632)는 PCRF 개시형 IP-CAN 세션 수정을 위해 vPCRF(622)를 통하여 PCEF/BBERF와 상호작용할 수 있다(720, 722, 724).

[0076] Rx 응답에 기초해서, AS(610)는 WTRU(605)가 VPLMN(620)에 방문중인지를 검출할 수 있다(726). WTRU(605)가 VPLMN(620)에 방문중인지를 결정하기 위해 상기와는 다른 방법을 사용할 수 있다는 점에 주목하여야 한다.

[0077] AS(610)는 WTRU(605)의 HPLMN을 결정하기 위한 충분한 정보를 가질 수도 있고 갖지 않을 수도 있다. AS(610)가 WTRU(605)의 HPLMN을 결정하기 위한 충분한 정보를 갖지 않으면, AS(610)는 사용자 데이터 요청을 eSh-프록시(624)에게 보낼 수 있다(728). 사용자 데이터 요청은 HPLMN 영역 또는 도메인을 포함할 수 있고, AS(610)에 의해 eSh-프록시(624)에게 제공된 정보는 eSh-프록시와 통신하는 HPLMN을 알아낼 수 있게 한다. eSh-프록시(624)는 WTRU(605)와 연합하는 eSh-프록시를 검출하고, AS(610)가 홈 네트워크로부터 이 유형의 데이터를 검색하도록 허용되는지를 체크할 수 있다(730). 그 다음에, eSh-프록시(624)는 사용자 데이터 요청을 HPLMN(630)의 eSh-프록시(634)에게 보낸다(732). eSh-프록시(634)는 AS(610)가 HPLMN(630) 및/또는 사용자로부터 데이터를 검색하도록 허용되는지를 체크할 수 있다(734). 만일 허용된다고 결정되면, eSh-프록시(634)는 사용자 데이터 요청을 HSS(636)에게 보낸다(736). 그 다음에, eSh-프록시(634, 624)를 통해 HSS(636)로부터 AS(610)에게로 사용자 데이터 응답이 포워딩된다(738). 만일 AS(610)가 WTRU(605)의 HPLMN을 결정하기 위한 충분한 정보를 갖고 있으면, 단계 728-738은 생략될 수 있다.

[0078] WTRU(605)의 HPLMN이 결정된 때, AS(610)는 협력하는 AS(640)가 HPLMN(630)과의 협약을 갖고 있음을 검출한다(740). 일 실시형태에 있어서, AS(610)는 WTRU(605)를 협력 AS(640)에게 재지향시키지 않고 서비스의 전달을 계속할 수 있다. 대안적으로, AS(610)는 WTRU(605)를 협력 AS(640)에게 재지향시키도록 선택할 수 있다(742). 만일 Rx가 이전에 사용되었으면, AS(610)는 vPCRF(622)와의 IP-CAN 세션을 종결할 수 있다. AS(610)는 재지향 요청(예를 들면, HTTP 재지향)을 WTRU(605)에게 보낸다(744). 그 다음에, WTRU(605)는 서비스 요청을 HPLMN(630)에 대하여 서빙하는 AS(640)에게 보낸다.

[0079] 다른 실시형태에 있어서, WTRU(605)는 홈 네트워크의 AS(640)로부터 방문 네트워크의 AS(610)로 재지향될 수 있다. 예를 들어서, 만일 서비스가 많은 트래픽을 발생하면, 애플리케이션 공급자는 방문 네트워크와 상호접속된 AS(610)를 향해 사용자를 재지향시킬 수 있다.

[0080] 도 8은 사용자를 홈 네트워크에 서빙하는 AS로부터 방문 네트워크에 서빙하는 AS로 재지향시키기 위한 예시적인 처리의 신호도이다. VPLMN(620)과 HPLMN(630)의 eSh-프록시(624, 634)들 간에 통신이 확립된다(802). VPLMN(620)의 eSh-프록시(624)와 AS(610) 간에도 또한 통신이 확립된다(804). eSh-프록시 대 eSh-프록시 및 eSh-프록시 대 AS의 통신은 미리 확립될 수도 있고, 또는 대안적으로 온디맨드로 확립될 수도 있다.

[0081] WTRU(605)는 서비스 요청을 HPLMN(630)의 AS(640)에게 보낸다(806). WTRU(605)와 AS(640) 간에 인증 절차가 수행되고, 이것은 다른 노드를 또한 수반한다(808). AS(640)는 Rx(전술한 실시형태 중의 하나에 따름) 또는 eSh(위치 요청에 따름)를 이용하여 WTRU 위치를 획득하고, WTRU(605)가 VPLMN(620)에 방문중임을 인식한다(810). AS(640)는 협력 AS(610)가 VPLMN 사용자(812)에게 동일한 서비스를 제공한다는 것을 그 내부 상태 또는 구성을 이용하여 검출한다. 일 실시형태에 있어서, AS(640)는 WTRU(605)를 AS(610)에게 재지향시키지 않고 서비스의 전달을 계속할 수 있다. 대안적으로, AS(640)는 WTRU(605)를 협력 AS(610)를 향해 재지향시키도록 선택할 수 있다

(814). AS(640)는 재지향 요청(예를 들면, HTTP 재지향)을 WTRU(605)에게 보낸다(816). 그 다음에, WTRU(605)는 서비스 요청을 VPLMN(620)에게 서빙하는 AS(610)에게 보낸다(818).

[0082] 도 9는 NAF 기능이 OP와 공존되고 AS-VPLMN 상호접속 및 eZn-프록시가 폴리싱, 과금, 및 사용자 데이터 획득을 위해 사용되는 경우의 예시적인 네트워크 아키텍처를 보인 것이다. AS(910)는 애플리케이션 공급자의 제어하에 있을 수 있다. 대안적으로 AS(910)는 VPLMN 네트워크 운용자의 제어하에 있을 수 있다.

[0083] NAF 기능은 일반 부트스트래핑 아키텍처(GBA)와 오픈ID 아키텍처를 결합하기 위해 OP와 공존된다. NAF 기능은 오픈ID 서버에 추가되어도 좋다. 오픈ID는 사용자가 분산화 방식으로 인증되는 방법을 설명하는 표준이다. 사용자는 OP에 의해 계정을 생성할 수 있고, 그 다음에 오픈ID 인증을 수용하는 임의의 웹사이트에 대한 서명의 기초로서 상기 계정을 사용할 수 있다. 오픈ID 표준은 OP와 오픈ID 수용자("신뢰 당사자"(relying party, RP)) 사이에서 발생하는 통신에 대한 하부구조(framework)를 제공한다. 최종 사용자는 특수 아이덴티티를 단정(assert)하기 원하는 엔티티이다. RP는 최종 사용자의 식별자를 검증하기 원하는 웹사이트 또는 애플리케이션이다. OP는 오픈ID 인증을 제공한다. 오픈ID는 최종 사용자가 RP와 통신할 수 있게 한다. 이 통신은 식별자(즉, 오픈ID)의 교환을 통해 행하여진다.

[0084] 도 9를 참조하면, 강화 NAF/OP(eNAF/OP)(926)가 VPLMN(920)에 위치되고 eNAF(926)는 eZn-프록시 기능(928)을 통해 HPLMN(930)의 eBSF(937)와 통신한다. 대안적으로, eNAF/OP(926)와 eZn-프록시(928)는 VPLMN(920)이 아닌 다른 네트워크에 위치될 수 있다. 애플리케이션 공급자는 VPLMN 운용자와 협약을 갖는다. RP로서 작용하는 AS(910)는 싱글 사인온(Single Sign-On, SSO) 프로토콜(예를 들면, 오픈ID, 자유 동맹 등)을 이용하여 VPLMN(920)의 OP 서버로서 작용하는 eNAF(926)와 상호접속할 수 있다.

[0085] GBA는 범용 집적회로 카드(UICC) 기반 증명서(credential)로 제한된다. 일 실시형태에 있어서, GBA 엔티티(예를 들면, BSF, Zn-프록시 및 NAF) 및 기준점(예를 들면, Ua, Ub, Zn, Zn' 및 Zh)은 비-UICC 기반 증명서(예를 들면, SIP 다이제스트, 패스워드 등) 및 자동화 인증 방법 협상 및 선택이 가능하도록 강화될 수 있다. Zn 기준점은 애플리케이션 특정의 사용자 보안 설정(USS)에 추가하여 eSh를 통하여 통상적으로 이용가능한 사용자 특정 데이터를 검색할 수 있도록 강화(즉, eZn)될 수 있다. eZn' 기준점은 이것이 운용자들 간에 사용된다는 점에서 Zn 기준점과 구별된다. Zh 기준점은 인증 벡터(AV), GBA 사용자 보안 설정(GUSS), 및 USS에 추가하여 HSS로부터 eSh를 통하여 통상적으로 이용가능한 사용자 특정 데이터를 검색할 수 있도록 강화(즉, eZh)될 수 있다. GUSS는 BSF 특정 정보 요소 및 모든 애플리케이션 특정 USS의 집합을 포함한다. 자유 동맹/오픈ID 기준점을 통한 속성 교환은 eSh 인터페이스를 통해 이용가능한 정보를 운반하도록 강화될 수 있다.

[0086] 도 10은 일 실시형태에 따라서, 애플리케이션 세션을 확립하고 AS-VPLMN 상호접속 및 eZn-프록시를 이용하여 폴리싱, 과금, 및 사용자 데이터 획득을 행하는 예시적인 처리의 신호도이다. WTRU(905)는 사용자 공급 식별자를 RP로서 작용하는 AS(910)에게 보낸다(1002). AS(910)는 OP의 어드레스를 검색하고, 최종 사용자가 인증을 위해 사용하기 원하는 OP 엔드포인트 URL의 발견(discovery)을 수행한다(사용자 공급 식별자에 기초해서)(1004).

[0087] AS(910)와 eNAF/OP(926)는 예를 들면 디피 헬만 키 교환 프로토콜을 이용하여 공유 비밀을 확립할 수 있다(1006). 이 공유 비밀의 목적은 eNAF/OP(926)가 후속하는 메시지에 서명하고 AS(910)가 그 메시지를 검증하는 것이다.

[0088] AS(910)는 WTRU(905)를 오픈ID 인증 요청을 가진 eNAF/OP(926)에게 재지향시킨다(1008). WTRU(905)는 HTTP 취득 요청을 eNAF/OP(926)에게 보낸다(1010). eNAF/OP(926)는 WTRU 인증을 개시하고 HTTPS 응답 코드 401 "권한없음"(Unauthorized)으로 응답하고, 상기 응답 코드는 WTRU에게 서버 측 인증서(certificate)를 가진 GBA에 의한 다이제스트 인증을 사용하도록 요청하는 챌린지를 운반하는 WWW 인증 헤더를 포함한다(1012).

[0089] 만일 이용가능한 유효 K가 없으면, WTRU(905)는 유효 K를 획득하기 위해 eBSF(937)에 의해 부트스트랩할 수 있다(1014). 이것에 의해, WTRU(905)는 애플리케이션 특정 NAF 키를 도출할 수 있다. WTRU(905)는 HTTPS 취득 요청을 eNAF/OP(926)에게 보낸다(1016). HTTPS 취득 요청은 eBSF(937)로부터 수신된 B-TID를 포함한 권한부여 헤더를 소지한다.

[0090] B-TID 및 NAF_ID를 이용해서, eNAF/OP(926)는 공유 애플리케이션 특정 NAF 키 및 USS를 eBSF(937)로부터 검색할 수 있다(1018). eNAF/OP(926)는 오픈ID 사용자 세션과 GBA 세션의 매칭이 가능하도록 B-TID, 암호화 키 및 사용자 공급 식별자를 저장할 수 있다.

[0091] eNAF/OP(926)는 오픈ID의 사용자를 인증한다(1020). eNAF/OP(926)는 인증이 승인된 단정(assertion) 또는 인증이 실패한 메시지와 함께 WTRU(905)를 AS(910)에게 다시 재지향시킨다(1022). WTRU(905)는 단정과 함께 HTTPS

요청을 보낸다(1024). AS(910)는 단정을 비준한다(즉, 인증이 승인되었는지 체크한다)(1026). 만일 단정의 비준이 성공이면, 사용자는 AS(910)의 서비스에 로그인된다.

[0092] WTRU(905)가 GBA/오픈ID를 이용하여 인증되면, AS(910)는 Rx를 이용하여 세션에 대한 QoS 또는 다른 폴리시 및 과금을 제어할 수 있다(1028). AS(910)는 eNAF(926), eZn-프록시(928), 및 eBSF(937)를 통하여 HSS(936)의 사용자 데이터(예를 들면, 애플리케이션 특정 사용자 프로필)에 접근할 수 있다(1030). AS(910)는 또한 eNAF(926), eZn-프록시(928), 및 eBSF(937)를 통하여 HSS(936)에서 정보(예를 들면, 애플리케이션 특정 사용자 프로필)를 설정할 수 있다(1032). AS(910)는 eNAF(926), eZn-프록시(928), 및 eBSF(937)를 통하여 HSS(936)에서 이벤트(예를 들면, 위치 변경)를 등록할 수 있다(1034).

[0093] 도 11은 eNAF 기능이 OP와 공존되고 AS-VPLMN 상호접속 및 HPLMN의 eNAF가 폴리싱, 과금, 및 사용자 데이터 획득을 위해 사용되는 경우의 예시적인 네트워크 아키텍처를 보인 것이다. 애플리케이션 공급자는 VPLMN 운용자와의 협약을 갖는다. 이것은 도 9와 유사하고, 차이점은 eNAF/OP(1137)가 HPLMN(1130)에 위치되어 있다는 점이다. RP로서 작용하는 AS(1110)는 SSO 프로토콜(예를 들면, 오픈ID, 자유 동맹 등)을 이용하여 HPLMN(1130)의 eNAF/OP(1135)와 상호접속할 수 있다. eNAF/OP(1135)는 eZn 기준점을 통하여 HPLMN(1130)의 eBSF(1137)와 통신한다. AS(1110)는 애플리케이션 공급자의 제어하에 있을 수 있다. 대안적으로 AS(1110)는 VPLMN 네트워크 운용자의 제어하에 있을 수 있다.

[0094] GBA는 UICC 기반 증명서로 제한된다. 일 실시형태에 있어서, GBA 엔티티(예를 들면, BSF 및 NAF) 및 기준점(예를 들면, Ua, Ub, Zn, 및 Zh)은 비-UICC 기반 증명서(예를 들면, SIP 다이제스트, 패스워드 등) 및 자동화 인증 방법 협상 및 선택이 가능하도록 강화될 수 있다. Zn 기준점은 애플리케이션 특정의 USS에 추가하여 eSh를 통하여 통상적으로 이용가능한 사용자 특정 데이터를 검색할 수 있도록 강화(즉, eZn)될 수 있다. Zh 기준점은 AV, GUSS, 및 USS에 추가하여 HSS로부터 eSh를 통하여 통상적으로 이용가능한 사용자 특정 데이터를 검색할 수 있도록 강화(즉, eZh)될 수 있다. 자유 동맹/오픈ID 기준점을 통한 속성 교환은 eSh 인터페이스를 통해 이용가능한 정보를 운반하도록 강화될 수 있다.

[0095] 도 12는 일 실시형태에 따라서 애플리케이션 세션을 확립하는 예시적인 처리의 신호도이다. WTRU(1105)는 사용자 공급 식별자를 신뢰 당사자로서 작용하는 AS(1110)에게 보낸다(1202). AS는 오픈ID를 이용하여 WTRU를 인증할 수 있다. AS(1110)는 eNAF/OP(1135)의 어드레스를 검색하고, 최종 사용자가 인증을 위해 사용하기 원하는 OP 엔드포인트 URL의 발견을 수행한다(사용자 공급 식별자에 기초해서)(1204).

[0096] AS(1110)와 HPLMN(1130)의 eNAF/OP(1135)는 예를 들면 디피 헬만 키 교환 프로토콜을 이용하여 공유 비밀을 확립할 수 있다(1206). 이 공유 비밀의 목적은 eNAF/OP(1135)가 후속하는 메시지에 서명하고 AS(1110)가 그 메시지를 검증하는 것이다.

[0097] AS(1110)는 WTRU(1105)를 오픈ID 인증 요청을 가진 eNAF/OP(1135)에게 재지향시킨다(1208). WTRU(1105)는 HTTP 취득 요청을 HPLMN(1130)의 eNAF/OP(1135)에게 보낸다(1210). eNAF/OP(1135)는 WTRU 인증을 개시하고 HTTPS 응답 코드 401 "권한없음"으로 응답하고, 상기 응답 코드는 WTRU에게 서버 측 인증서를 가진 GBA에 의한 다이제스트 인증을 사용하도록 요청하는 챌린지를 운반하는 WWW 인증 헤더를 포함한다(1212).

[0098] 만일 이용가능한 유효 K가 없으면, WTRU(1105)는 유효 K를 획득하기 위해 eBSF(1137)에 의해 부트스트랩할 수 있다(1214). 이것에 의해, WTRU(1105)는 애플리케이션 특정 NAF 키를 도출할 수 있다. WTRU(1105)는 HTTPS 취득 요청을 eNAF/OP(1135)에게 보낸다(1216). HTTPS 취득 요청은 eBSF(1137)로부터 수신된 B-TID를 포함한 권한부여 헤더를 소지한다.

[0099] B-TID 및 NAF_ID를 이용해서, eNAF/OP(1135)는 공유 애플리케이션 특정 NAF 키 및 USS를 eBSF(1137)로부터 검색한다(1218). eNAF/OP(1135)는 오픈ID 사용자 세션과 GBA 세션의 매칭이 가능하도록 B-TID, 암호화 키 및 사용자 공급 식별자를 저장할 수 있다.

[0100] eNAF/OP(1135)는 오픈ID의 사용자를 인증한다(1220). eNAF/OP(1135)는 인증이 승인된 단정 또는 인증이 실패한 메시지와 함께 WTRU(1105)를 AS(1110)에게 다시 재지향시킨다(1222). WTRU(1105)는 단정과 함께 HTTPS 요청을 보낸다(1224). AS(1110)는 단정을 비준한다(즉, 인증이 승인되었는지 체크한다)(1226). 만일 단정의 비준이 성공이면, 사용자는 AS(1110)의 서비스에 로그인된다.

[0101] WTRU(1105)가 GBA/오픈ID를 이용하여 인증되면, AS(1110)는 Rx를 이용하여 그 세션에 대한 QoS 및 과금을 제어할 수 있다(1228). AS(1110)는 eNAF(1135) 및 eBSF(1137)를 통하여 HSS(1136)의 사용자 데이터(예를 들면, 애플리케이션 특정 사용자 프로필)에 접근할 수 있다(1230). AS(1110)는 또한 eNAF(1135) 및 eBSF(1137)를 통하

여 HSS(1136)에서 정보(예를 들면, 애플리케이션 특정 사용자 프로필)를 설정할 수 있다(1232). AS(1110)는 eNAF(1135) 및 eBSF(1137)를 통하여 HSS(1136)에서 이벤트(예를 들면, 위치 변경)를 등록할 수 있다(1234).

[0102] 도 13은 비-로밍의 경우에 HPLMN에서 eNAF/OP를 가진 예시적인 네트워크 아키텍처를 보인 것이다. eNAF/OP에 의해 인에이블되는 메카니즘은 비-로밍 상황에서 사용될 수 있다. 이 실시형태에 있어서, 애플리케이션 공급자는 HPLMN 운용자와의 협약을 갖는다. eNAF/OP(1335)는 HPLMN(1330)에 위치되어 있다. RP로서 작용하는 AS(1310)는 SSO 프로토콜(예를 들면, 오픈ID, 자유 동맹 등)을 이용하여 HPLMN(1330)의 eNAF/OP(1335)와 상호접속할 수 있다. eNAF/OP(1335)는 eZn 기준점을 통하여 HPLMN(1330)의 eBSF(1337)와 통신한다. 대안적으로, eNAF/OP(1335)는 HPLMN(1330)의 다른 네트워크에 위치될 수 있다. 이 경우에, eNAF/OP(1335)는 Zn-프록시(eNAF/OP(1335)와 공존될 수 있음)을 이용하여 HPLMN(1330)의 eBSF(1337)와 통신할 수 있다. 여기에서 설명한 실시형태들은 양자의 경우에 적용할 수 있다. AS(1310)는 애플리케이션 공급자의 제어하에 있을 수 있다. 대안적으로 AS(1310)는 VPLMN 네트워크 운용자의 제어하에 있을 수 있다.

[0103] GBA는 UICC 기반 증명서로 제한된다. GBA 엔티티(예를 들면, BSF 및 NAF) 및 기준점(예를 들면, Ua, Ub, Zn 및 Zh)은 비-UICC 기반 증명서(예를 들면, SIP 다이제스트, 패스워드 등) 및 자동화 인증 방법 협상 및 선택이 가능하도록 강화될 수 있다. Zn 기준점은 애플리케이션 특정의 USS에 추가하여 eSh를 통하여 통상적으로 이용가능한 사용자 특정 데이터를 검색할 수 있도록 강화(즉, eZn)될 수 있다. Zh 기준점은 AV, GUSS 및 USS에 추가하여 HSS로부터 eSh를 통하여 통상적으로 이용가능한 사용자 특정 데이터를 검색할 수 있도록 강화(즉, eZh)될 수 있다. 자유 동맹/오픈ID 기준점을 통한 속성 교환은 eSh 인터페이스를 통해 이용가능한 정보를 운반하도록 강화될 수 있다.

[0104] 도 14는 일 실시형태에 따라서 비-로밍의 경우에 HPLMN의 eNAF를 이용하여 애플리케이션 세션을 확립하는 예시적인 처리의 신호도이다. WTRU(1305)는 사용자 공급 식별자를 RP로서 작용하는 AS(1310)에게 보낸다(1402). AS는 오픈ID를 이용하여 WTRU를 인증할 수 있다. AS(1310)는 OP의 어드레스를 검색하고, 최종 사용자가 인증을 위해 사용하기 원하는 OP 엔드포인트 URL의 발견을 수행한다(사용자 공급 식별자에 기초해서)(1404).

[0105] AS(1310)와 HPLMN(1330)의 eNAF/OP(1335)는 예를 들면 디피 헬만 키 교환 프로토콜을 이용하여 공유 비밀을 확립할 수 있다(1406). 이 공유 비밀의 목적은 eNAF/OP(1335)가 후속하는 메시지에 서명하고 AS(1310)가 그 메시지를 검증하는 것일 수 있다.

[0106] AS(1310)는 WTRU(1305)를 오픈ID 인증 요청을 가진 eNAF/OP(1335)에게 재지향시킨다(1408). WTRU(1305)는 HTTP 취득 요청을 eNAF/OP(1335)에게 보낸다(1410). eNAF/OP(1335)는 WTRU 인증을 개시하고 HTTPS 응답 코드 401 "권한없음"으로 응답하며, 상기 응답 코드는 WTRU에게 서버 측 인증서를 가진 GBA에 의한 다이제스트 인증을 사용하도록 요청하는 챌린지를 운반하는 WWW 인증 헤더를 포함한다(1412).

[0107] 만일 이용가능한 유효 K가 없으면, WTRU(1305)는 유효 K를 획득하기 위해 eBSF(1337)에 의해 부트스트랩할 수 있다(1414). 이것에 의해, WTRU(1305)는 애플리케이션 특정 NAF 키를 도출할 수 있다. WTRU(1305)는 HTTPS 취득 요청을 eNAF/OP(1335)에게 보낸다(1416). HTTPS 취득 요청은 eBSF(1337)로부터 수신된 B-TID를 포함한 권한부여 헤더를 소지한다.

[0108] B-TID 및 NAF_ID를 이용해서, eNAF/OP(1335)는 공유 애플리케이션 특정 NAF 키 및 USS를 eBSF(1337)로부터 검색한다(1418). eNAF/OP(1335)는 오픈ID 사용자 세션과 GBA 세션의 매칭이 가능하도록 B-TID, 암호화 키 및 사용자 공급 식별자를 저장할 수 있다.

[0109] eNAF/OP(1335)는 오픈ID의 사용자를 인증한다(1420). eNAF/OP(1335)는 인증이 승인된 단정 또는 인증이 실패한 메시지와 함께 WTRU(1305)를 AS(1310)에게 다시 재지향시킨다(1422). WTRU(1305)는 단정과 함께 HTTPS 요청을 보낸다(1424). AS(1310)는 단정을 비준한다(즉, 인증이 승인되었는지 체크한다)(1426). 만일 단정의 비준이 성공이면, 사용자는 AS(1310)의 서비스에 로그인된다.

[0110] WTRU(1305)가 GBA/오픈ID를 이용하여 인증되면, AS(1310)는 Rx를 이용하여 세션에 대한 QoS 및 과금을 제어할 수 있다(1428). AS(1310)는 eNAF(1335) 및 eBSF(1337)를 통하여 HSS의 사용자 데이터(예를 들면, 애플리케이션 특정 사용자 프로필)에 접근할 수 있다(1430). AS(1310)는 또한 eNAF(1335) 및 eBSF(1337)를 통하여 HSS에서 정보(예를 들면, 애플리케이션 특정 사용자 프로필)를 설정할 수 있다(1432). AS(1310)는 eNAF(1335) 및 eBSF(1337)를 통하여 HSS에서 이벤트(예를 들면, 위치 변경)를 등록할 수 있다(1434).

[0111] 다른 실시형태에서는 AS와 eNAF가 공존될 수 있다. 도 15는 공존하는 AS/eNAF를 가진 예시적인 네트워크 아키텍처를 보인 것이다.애플리케이션 공급자는 VPLMN 운용자와의 협약을 갖는다. VPLMN(1520)에 의해 호스트되는

AS(1510)는 eNAF로서 작용하고 eZn-프록시 기능(1528)을 통하여 HPLMN(1530)의 eBSF(1537)와 통신한다.

[0112] GBA는 UICC 기반 증명서로 제한된다. GBA 엔티티(예를 들면, BSF 및 NAF) 및 기준점(예를 들면, Ua, Ub, Zn 및 Zh)은 비-UICC 기반 증명서(예를 들면, SIP 다이제스트, 패스워드 등) 및 자동화 인증 방법 협상 및 선택이 가능하도록 강화될 수 있다. Zn 기준점은 애플리케이션 특정의 USS에 추가하여 eSh를 통하여 통상적으로 이용가능한 사용자 특정 데이터를 검색할 수 있도록 강화(즉, eZn)될 수 있다. Zh 기준점은 AV, GUSS 및 USS에 추가하여 HSS로부터 eSh를 통하여 통상적으로 이용가능한 사용자 특정 데이터를 검색할 수 있도록 강화(즉, eZh)될 수 있다. 자유 동맹/오픈ID 기준점을 통한 속성 교환은 eSh 인터페이스를 통해 이용가능한 정보를 운반하도록 강화될 수 있다.

[0113] 도 16은 일 실시형태에 따라서 AS 및 eNAF가 공존하는 경우에 애플리케이션 세션을 확립하는 예시적인 처리의 신호도이다. WTRU(1505)는 HTTP 취득 요청을 AS/eNAF(1510)에게 보낸다(1602). AS/eNAF(1510)는 WTRU 인증을 개시하고 인증 요청으로 응답한다(1604). WTRU(1505)는 유효 K를 획득하기 위해 eBSF(1537)에 의해 부트스트래핑 절차를 수행할 수 있다(1606).

[0114] WTRU(1505)는 HTTPS 취득 요청을 AS/eNAF(1510)에게 보낸다(1608). HTTPS 취득 요청은 eBSF(1537)로부터 수신된 B-TID를 포함한 권한부여 헤더를 소지한다. B-TID 및 NAF_ID를 이용해서, AS/eNAF(1510)는 공유 애플리케이션 특정 NAF 키 및 USS를 eBSF(1537)로부터 검색한다(1610). eNAF/AS(1510)는 사용자를 인증하고, AS-WTRU 통신이 진행될 수 있다(1612).

[0115] WTRU(1505)가 GBA/오픈ID를 이용하여 인증되면, AS/eNAF(1510)는 Rx를 이용하여 세션에 대한 QoS 및 과금을 제어할 수 있다(1614). AS/eNAF(1510)는 eZn-프록시(1528) 및 eBSF(1537)를 통하여 HSS의 사용자 데이터(예를 들면, 애플리케이션 특정 사용자 프로필)에 접근할 수 있다(1616). AS/eNAF(1510)는 또한 eZn-프록시(1528) 및 eBSF(1537)를 통하여 HSS에서 정보(예를 들면, 애플리케이션 특정 사용자 프로필)를 설정할 수 있다(1618). AS/eNAF(1510)는 eZn-프록시(1528) 및 eBSF(1537)를 통하여 HSS에서 이벤트(예를 들면, 위치 변경)를 등록할 수 있다(1620).

[0116] 실시형태

[0117] 1. 모바일 네트워크 운용자와 애플리케이션 공급자 간의 연동 방법.

[0118] 2. 실시형태 1에 있어서, 애플리케이션 서버가 WTRU로부터 서비스 요청을 수신하는 단계를 포함한 연동 방법.

[0119] 3. 실시형태 2에 있어서, 애플리케이션 서버가 오픈ID를 이용하여 WTRU를 인증하는 단계를 더 포함한 연동 방법.

[0120] 4. 실시형태 3에 있어서, 애플리케이션 서버가 OP와 공존하는 NAF를 통해 HSS에 접근하는 단계를 더 포함한 연동 방법.

[0121] 5. 실시형태 4에 있어서, 상기 NAF는 상기 WTRU의 홈 네트워크에 위치된 것인 연동 방법.

[0122] 6. 실시형태 2-5 중 어느 하나에 있어서, 상기 WTRU는 방문 네트워크에서 로밍하고 있고, 상기 애플리케이션 공급자는 상기 방문 네트워크와의 협약을 갖는 것인 연동 방법.

[0123] 7. 실시형태 6에 있어서, 상기 애플리케이션 서버는 상기 WTRU로부터의 서비스 요청의 서빙에 대한 과금 및 폴리싱을 위해 상기 방문 네트워크와 통신하는 것인 연동 방법.

[0124] 8. 모바일 네트워크 운용자와 애플리케이션 공급자 간의 연동 장치.

[0125] 9. 실시형태 8에 있어서, WTRU로부터 서비스 요청을 수신하도록 구성된 프로세서를 포함한 연동 장치.

[0126] 10. 실시형태 9에 있어서, 상기 프로세서는 오픈ID를 이용하여 WTRU를 인증하도록 구성된 것인 연동 장치.

[0127] 11. 실시형태 10에 있어서, 상기 프로세서는 OP와 공존하는 NAF를 통해 HSS에 접근하도록 구성된 것인 연동 장치.

[0128] 12. 실시형태 11에 있어서, 상기 NAF는 상기 WTRU의 홈 네트워크에 위치된 것인 연동 장치.

[0129] 13. 실시형태 9-12 중 어느 하나에 있어서, 상기 WTRU가 방문 네트워크에서 로밍하고 있고, 상기 애플리케이션 공급자는 상기 방문 네트워크와의 협약을 갖는 것인 연동 장치.

[0130] 14. 실시형태 13에 있어서, 상기 프로세서는 상기 WTRU로부터의 서비스 요청의 서빙에 대한 과금 및 폴리싱을

위해 상기 방문 네트워크와 통신하도록 구성된 것인 연동 장치.

[0131] 15. 모바일 네트워크 운용자와 애플리케이션 공급자 간의 연동 방법.

[0132] 16. 실시형태 15에 있어서, 애플리케이션 서버가 WTRU로부터 서비스 요청을 수신하는 단계를 포함한 연동 방법.

[0133] 17. 실시형태 16에 있어서, 상기 WTRU가, 애플리케이션 공급자가 협약을 가진 방문 네트워크에서 로밍하고 있고, 상기 애플리케이션 서버는 NAF와 공존되는 것인 연동 방법.

[0134] 18. 실시형태 16-17 중 어느 하나에 있어서, NAF로서 작용하는 애플리케이션 서버가 GBA를 이용하여 WTRU를 인증하는 단계를 포함한 연동 방법.

[0135] 19. 실시형태 18에 있어서, 애플리케이션 서버가 HSS에 접근하기 위해 eZn-프록시 기능을 통하여 홈 네트워크의 BSF와 통신하는 단계를 포함한 연동 방법.

[0136] 20. 실시형태 18-19 중 어느 하나에 있어서, 상기 WTRU가 인증된 조건하에, 애플리케이션 서버가 상기 방문 네트워크의 PCRF에 대한 Rx 인터페이스를 이용하여 서비스에 대한 서비스 품질 및 과금을 제어하는 단계를 더 포함한 연동 방법.

[0137] 21. 방문 네트워크와 통합된 애플리케이션에 대한 접근을 가능하게 하는 방법.

[0138] 22. 실시형태 21에 있어서, 애플리케이션 서버가 WTRU로부터 서비스 요청을 수신하는 단계를 포함한 방법.

[0139] 23. 실시형태 22에 있어서, 상기 WTRU가 상기 방문 네트워크에서 로밍하고 있고, 애플리케이션 공급자는 상기 방문 네트워크와의 협약을 갖는 것인 방법.

[0140] 24. 실시형태 22-23 중 어느 하나에 있어서, 상기 WTRU가 상기 방문 네트워크에서 로밍중인지를 애플리케이션 서버가 결정하는 단계를 포함한 방법.

[0141] 25. 실시형태 22-24 중 어느 하나에 있어서, 애플리케이션 서버가 상기 WTRU로부터의 서비스 요청의 서빙에 대한 과금, 폴리싱 및 사용자 데이터 접근을 위해 상기 방문 네트워크와 통신하는 단계를 포함한 방법.

[0142] 26. 실시형태 22-25 중 어느 하나에 있어서, 애플리케이션 서버가 제1 메시지를 Rx 인터페이스를 이용하여 vPCRF에게 보내는 단계를 더 포함한 방법.

[0143] 27. 실시형태 26에 있어서, 상기 제1 메시지는 hPCRF로 포워딩되는 것인 방법.

[0144] 28. 실시형태 26-27 중 어느 하나에 있어서, 애플리케이션 서버가 상기 제1 메시지에 응답하여 상기 vPCRF를 통해 제2 메시지를 수신하는 단계를 더 포함한 방법.

[0145] 29. 실시형태 28에 있어서, 상기 애플리케이션 서버는 상기 제2 메시지에 포함된 정보에 기초하여 상기 WTRU가 상기 방문 네트워크에서 로밍하고 있고 결정하는 것인 방법.

[0146] 30. 실시형태 22-29 중 어느 하나에 있어서, 애플리케이션 서버가 상기 방문 네트워크의 Sh-프록시로 사용자 데이터 요청을 보내는 단계를 더 포함한 방법.

[0147] 31. 실시형태 30에 있어서, 상기 사용자 데이터 요청은 Sh-프록시가 어떤 홈 네트워크 Sh-프록시와 통신하는지를 알아낼 수 있게 하는 홈 네트워크 영역 또는 도메인명 정보를 포함한 것인 방법.

[0148] 32. 실시형태 22-31 중 어느 하나에 있어서, 상기 애플리케이션 서버는 상기 WTRU의 인증 중에 수신된 정보에 기초하여 상기 WTRU가 상기 방문 네트워크에서 로밍하고 있음을 결정하는 것인 방법.

[0149] 33. 실시형태 32에 있어서, 상기 애플리케이션 서버는 상기 WTRU의 MSISDN을 수신하고, 상기 MSISDN에 기초하여 상기 WTRU가 상기 방문 네트워크에서 로밍하고 있음을 결정하는 것인 방법.

[0150] 34. 실시형태 22-33 중 어느 하나에 있어서, 상기 애플리케이션 서버는 홈 네트워크 신원을 수신하고, 상기 홈 네트워크 신원에 기초하여 상기 WTRU가 상기 방문 네트워크에서 로밍하고 있음을 결정하는 것인 방법.

[0151] 35. 실시형태 34에 있어서, 상기 홈 네트워크 신원은 MNC 및 MCC, 또는 디아미터 영역인 방법.

[0152] 36. 실시형태 22-35 중 어느 하나에 있어서, 애플리케이션 서버가 사용자 데이터를 획득하기 위해 사용자 데이터 요청을 보내는 단계를 더 포함한 방법.

[0153] 37. 실시형태 36에 있어서, 상기 WTRU의 홈 네트워크에서 상기 애플리케이션 서버와 HSS 간의 통신은 상기 방문

네트워크의 Sh-프록시 기능을 통하여 중재되고, 상기 Sh-프록시 기능은 상기 방문 네트워크와 상기 홈 네트워크 간의 로밍 협약으로부터 도출된 폴리시를 강화하는 것인 방법.

[0154] 38. 실시형태 22-37 중 어느 하나에 있어서, 상기 애플리케이션 공급자가 상기 WTRU의 홈 네트워크와의 협약을 갖는 것을 애플리케이션 서버가 결정하는 단계를 더 포함하고, 상기 애플리케이션 서버는 상기 서비스 요청에 서빙하기 위해 상기 홈 네트워크와 상기 방문 네트워크 중의 어느 하나 또는 양자와의 접속을 이용하는 것인 방법.

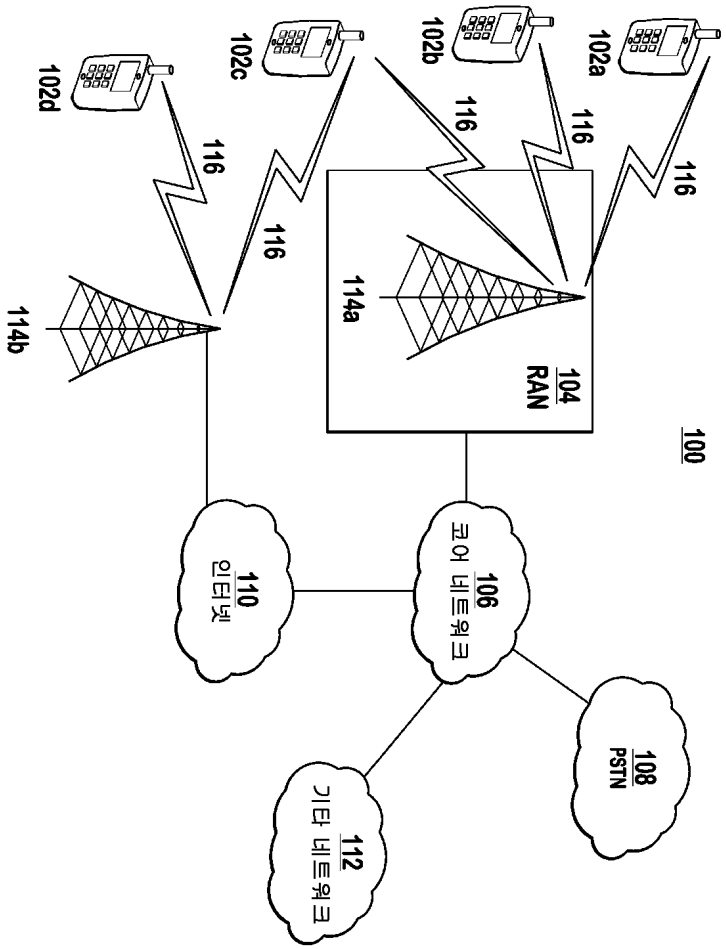
[0155] 39. 실시형태 22-38 중 어느 하나에 있어서, 상기 WTRU의 홈 네트워크에 서빙하는 협력 애플리케이션 공급자가 있는지를 애플리케이션 서버가 결정하는 단계를 더 포함한 방법.

[0156] 40. 실시형태 39에 있어서, 애플리케이션 서버가 상기 WTRU를 상기 협력 애플리케이션 서버를 향하여 재지향시키는 단계를 포함한 방법.

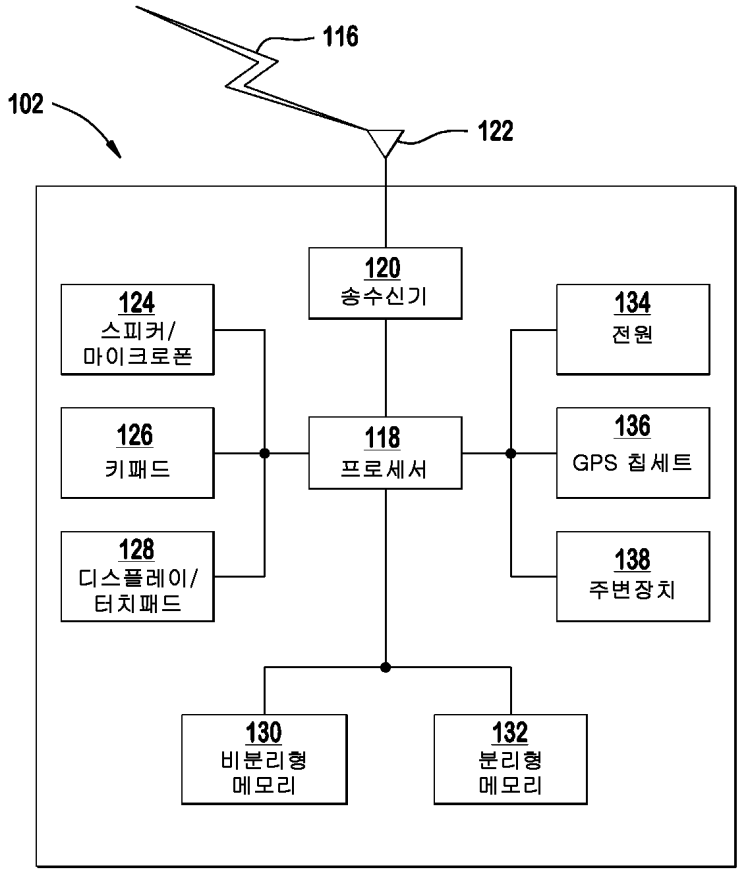
[0157] 지금까지 특징 및 요소들을 특수한 조합으로 설명하였지만, 이 기술에 통상의 지식을 가진 사람이라면 각 특징 또는 요소는 단독으로 또는 다른 특징 및 요소와 함께 임의의 조합으로 사용될 수 있다는 것을 이해할 것이다. 또한, 여기에서 설명한 방법들은 컴퓨터 또는 프로세서에 의해 실행되는 컴퓨터 판독가능 매체에 통합된 컴퓨터 프로그램, 소프트웨어 또는 펌웨어로 구현될 수 있다. 컴퓨터 판독가능 매체의 예로는 전자 신호(유선 또는 무선 접속을 통해 송신된 것) 및 컴퓨터 판독가능 기억 매체가 있다. 컴퓨터 판독가능 기억 매체의 예로는, 비제한적인 예를 들자면, 읽기 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 레지스터, 캐시 메모리, 반도체 메모리 소자, 내부 하드 디스크 및 착탈식 디스크와 같은 자기 매체, 자기 광학 매체, 및 CD-ROM 디스크 및 디지털 다기능 디스크(DVD)와 같은 광학 매체가 있다. 프로세서는 소프트웨어와 연합해서 WTRU, UE, 단말기, 기지국, RNC, 또는 임의의 호스트 컴퓨터에서 사용되는 라디오 주파수 송수신기를 구현하기 위해 사용될 수 있다.

도면

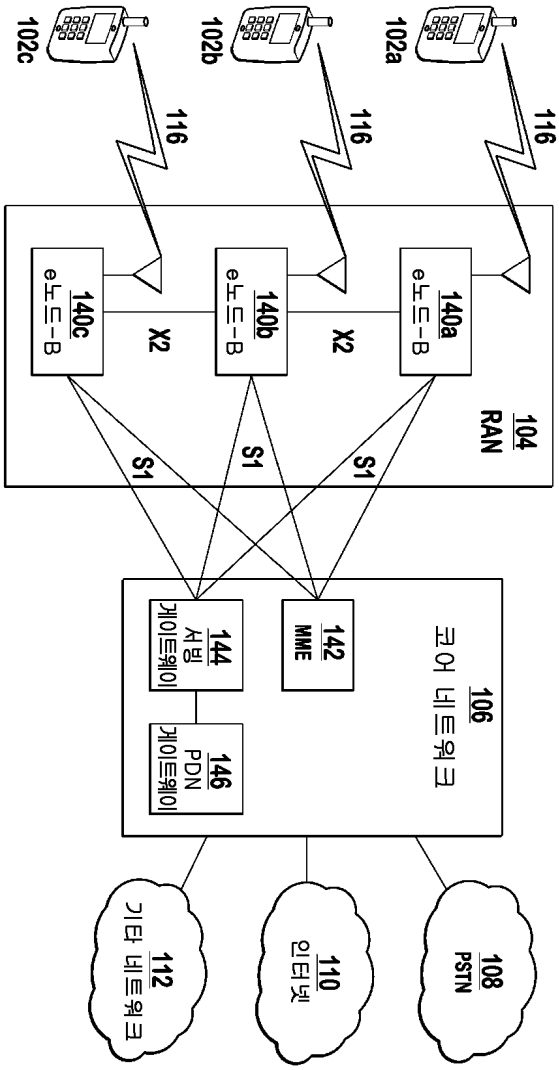
도면1a



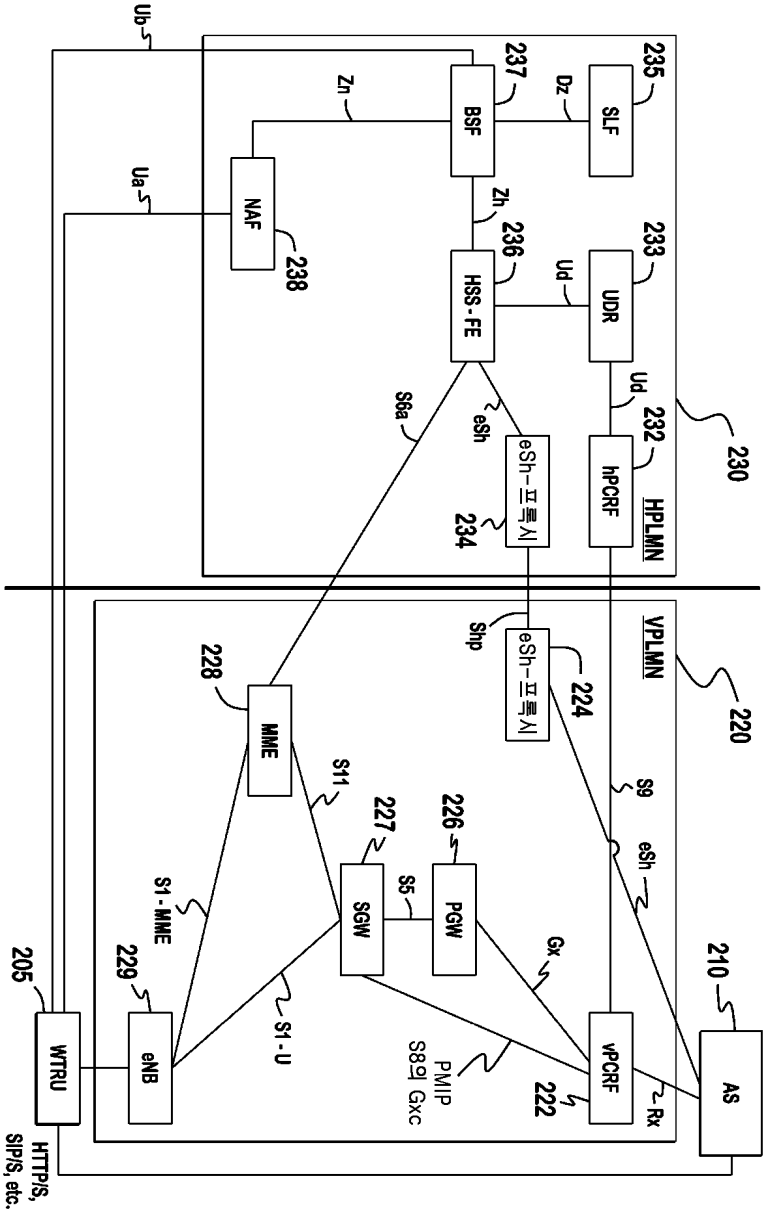
도면1b


116
102
122
120
송수신기
124
스피커/
마이크로폰
134
전원
126
키패드
118
프로세서
136
GPS 칩세트
128
디스플레이/
터치패드
138
주변장치
130
비분리형
메모리
132
분리형
메모리

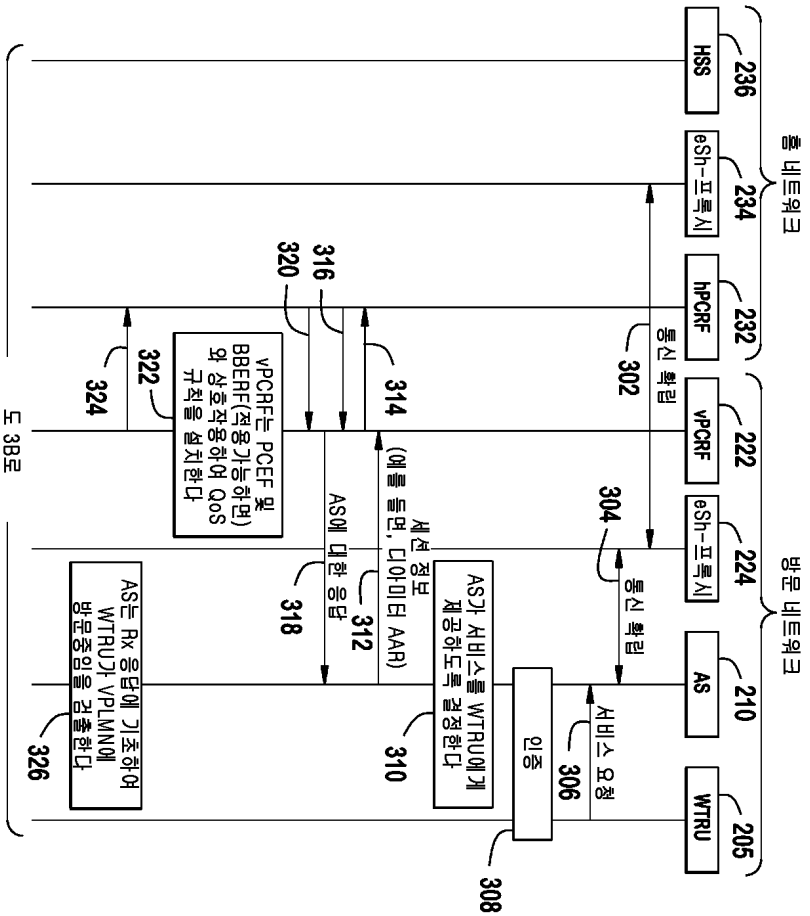
도면1c


102c
102b
102a
116
116
116
140c
e노드-B
140b
e노드-B
140a
e노드-B
X2
X2
104
RAN
S1
S1
S1
106
코어 네트워크
144
서빙
게이트웨이
142
MME
146
PDN
게이트웨이
112
기타 네트워크
110
인터넷
108
PSTN

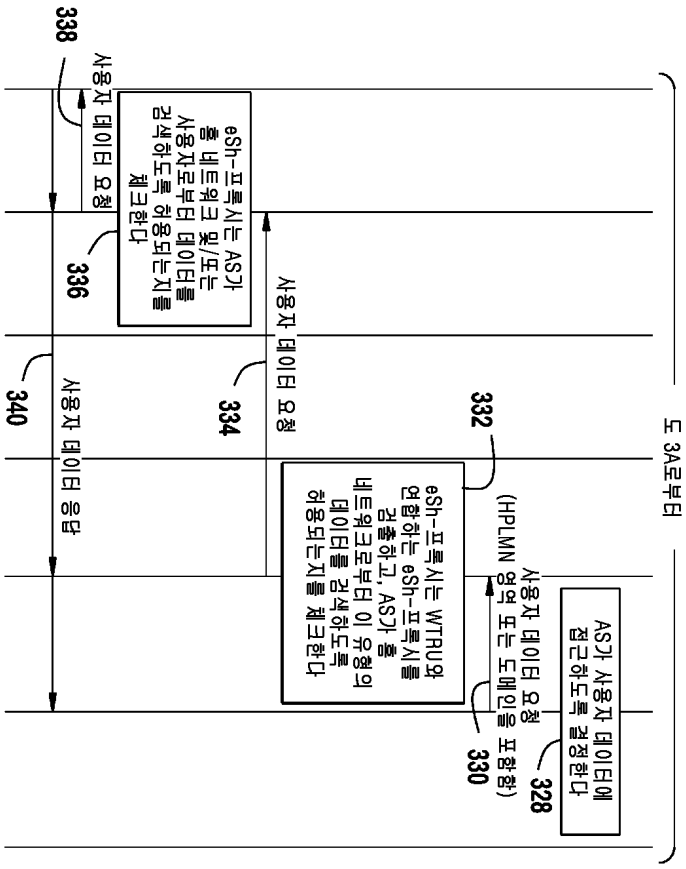
도면2


Ub
Zn
Dz
BSF
SLF
235
237
Ua
NAF
238
Zh
236
HSS-FE
Ud
UDR
233
S6a
eSh
eSh-프록시
234
Ud
232
hPCRF
HPLMN
230
Shp
eSh-프록시
224
VPLMN
220
228
MME
S11
227
SGW
S5
226
PGW
S9
eSh
S1-MME
229
eNB
S1-U
205
WTRU
Gx
vPCRF
222
PMIP
S8의 Gxc
Rx
210
AS
HTTP/S,
SIP/S, etc.

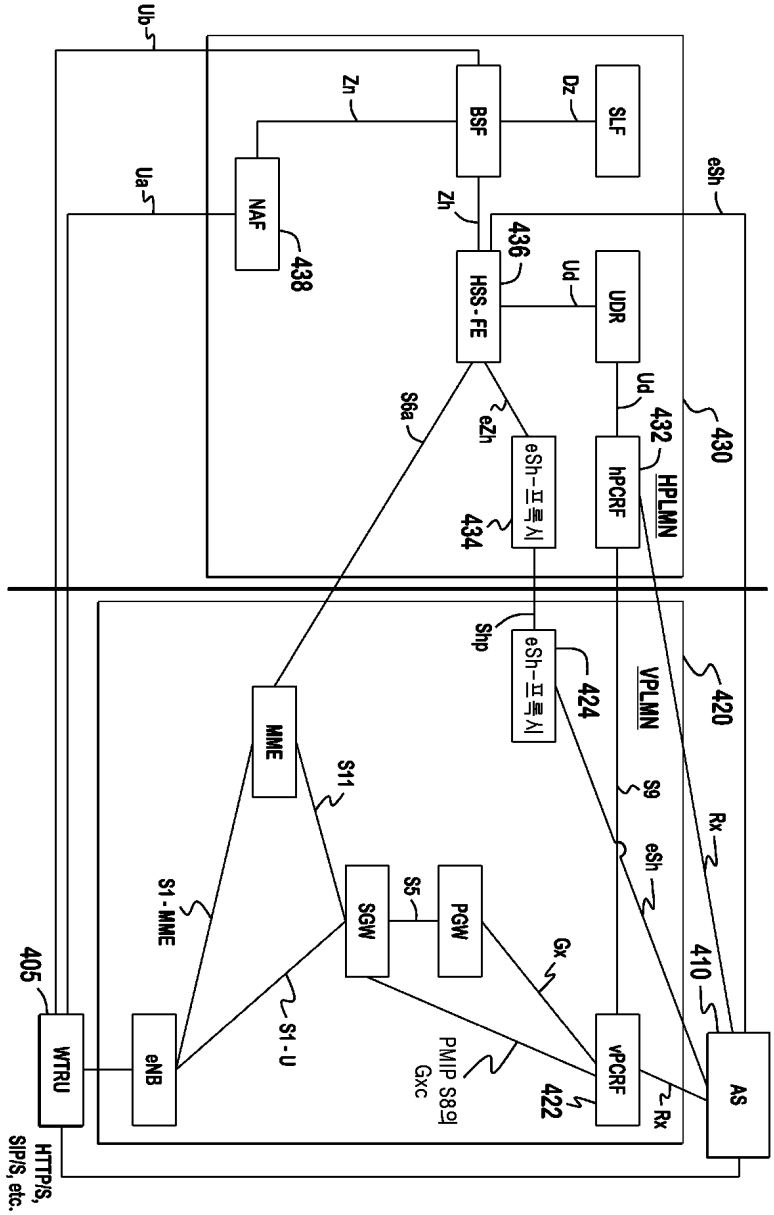
도면3a


홈 네트워크
방문 네트워크
HSS
236
eSh-프록시
234
hPCRF
232
vPCRF
222
eSh-프록시
224
AS
210
WTRU
205
도 3B로
통신 확립
302
304
316
320
314
322
324
vPCRF는 PCEF 및 BBERF(적용가능하면)와 상호작용하여 QoS 규칙을 설치한다
세션 정보 (예를 들면, 디아미터 AAR)
AS에 대한 응답
312
318
AS가 서비스를 WTRU에게 제공하도록 결정한다
310
인증
308
서비스 요청
306
AS는 Rx 응답에 기초하여 WTRU가 VPLMN에 방문중임을 검출한다
326

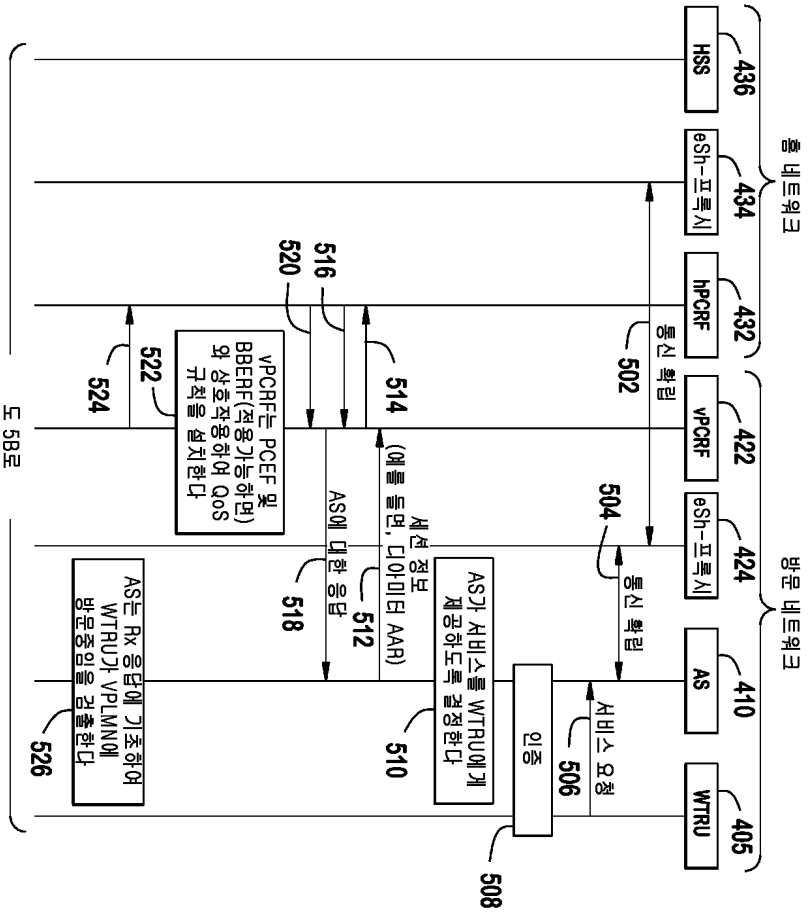
도면3b


도 3A로부터
328
AS가 사용자 데이터에 접근하도록 결정한다
330
사용자 데이터 요청 (HPLMN 영역 또는 도메인을 포함함)
332
eSh-프록시는 WTRU와 연합하는 eSh-프록시를 검출하고, AS가 홈 네트워크로부터 이 유형의 데이터를 검색하도록 허용되는지를 체크한다
334
사용자 데이터 요청
336
eSh-프록시는 AS가 홈 네트워크 및/또는 사용자로부터 데이터를 검색하도록 허용되는지를 체크한다
338
사용자 데이터 요청
340
사용자 데이터 응답

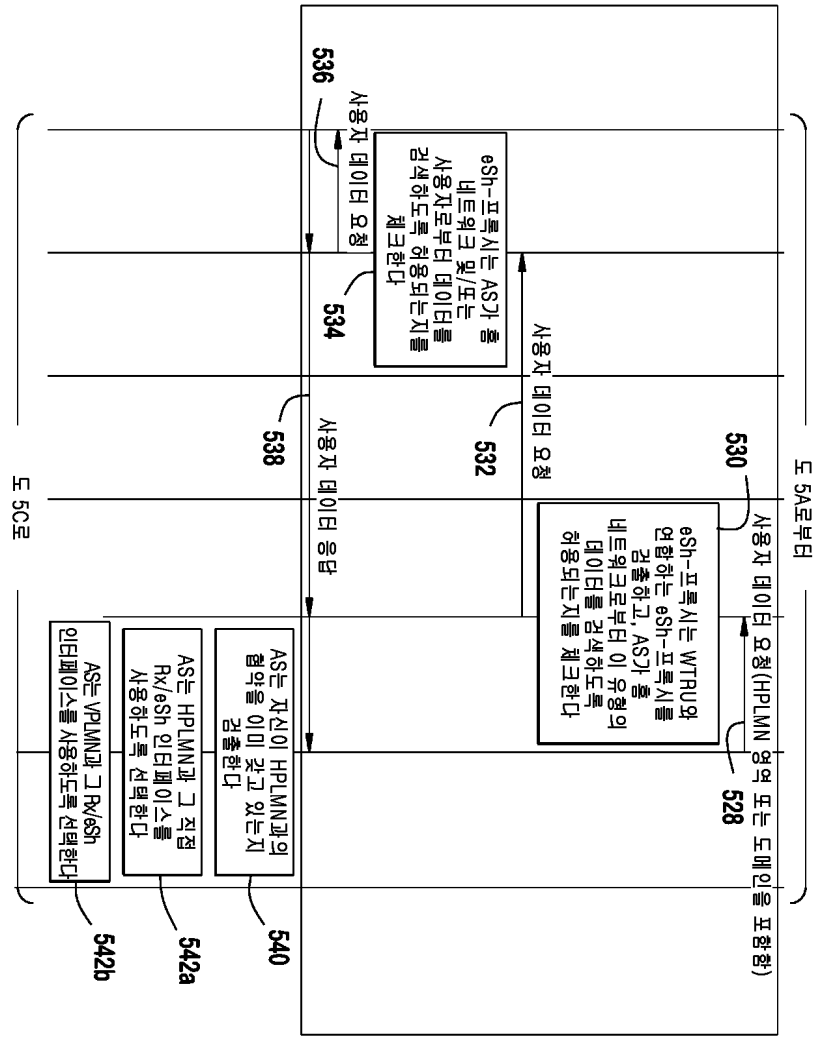
도면4


Ub
Zn
BSF
Dz
SLF
eSh
Ua
NAF
438
Zh
436
HSS-FE
Ud
UDR
S6a
eZh
eSh-프록시
434
Ud
432
HPLMN
hPCRF
430
Shp
eSh-프록시
424
VPLMN
420
MME
S11
S9
Rx
eSh
S1-MME
SGW
S5
PGW
Gx
410
405
WTRU
eNB
S1-U
PMIP S8의 Gxc
422
vPCRF
Rx
AS
HTTP/S, SIP/S, etc.

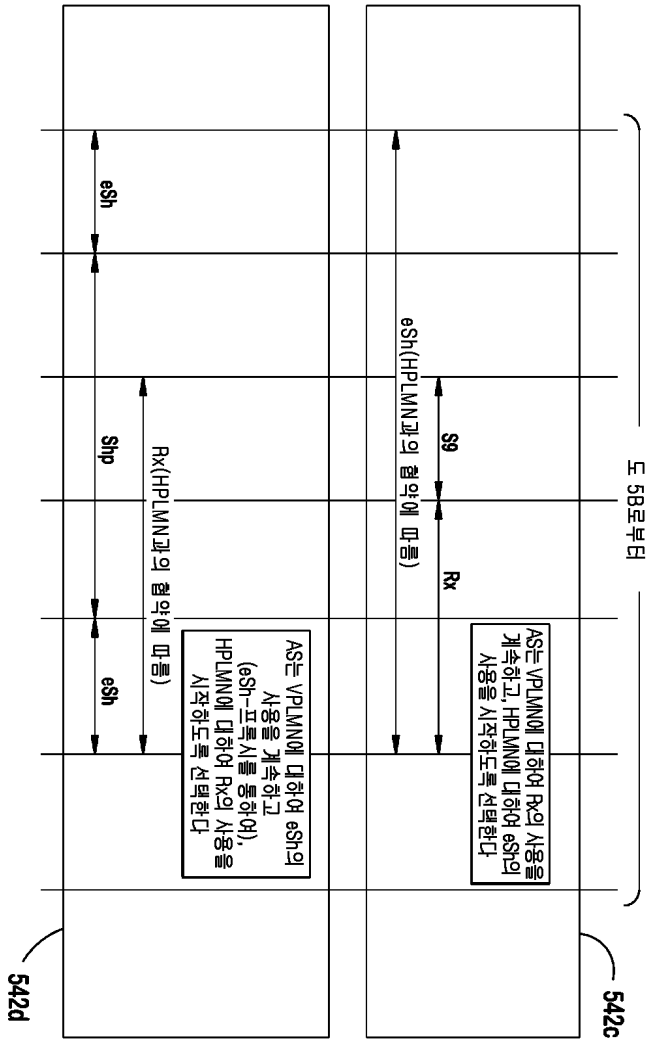
도면5a


홈 네트워크
방문 네트워크
HSS
436
eSh-프록시
434
hPCRF
432
vPCRF
422
eSh-프록시
424
AS
410
WTRU
405
502
통신 확립
504
통신 확립
506
서비스 요청
508
인증
510
AS가 서비스를 WTRU에게 제공하도록 결정한다
512
세션 정보 (예를 들면, 디아미터 AAR)
514
516
AS에 대한 응답
518
520
vPCRF는 PCEF 및 BBERF(적용가능하면)와 상호작용하여 QoS 규칙을 설치한다
522
524
AS는 Rx 응답에 기초하여 WTRU가 VPLMN에 방문중임을 검출한다
526
도 5B로

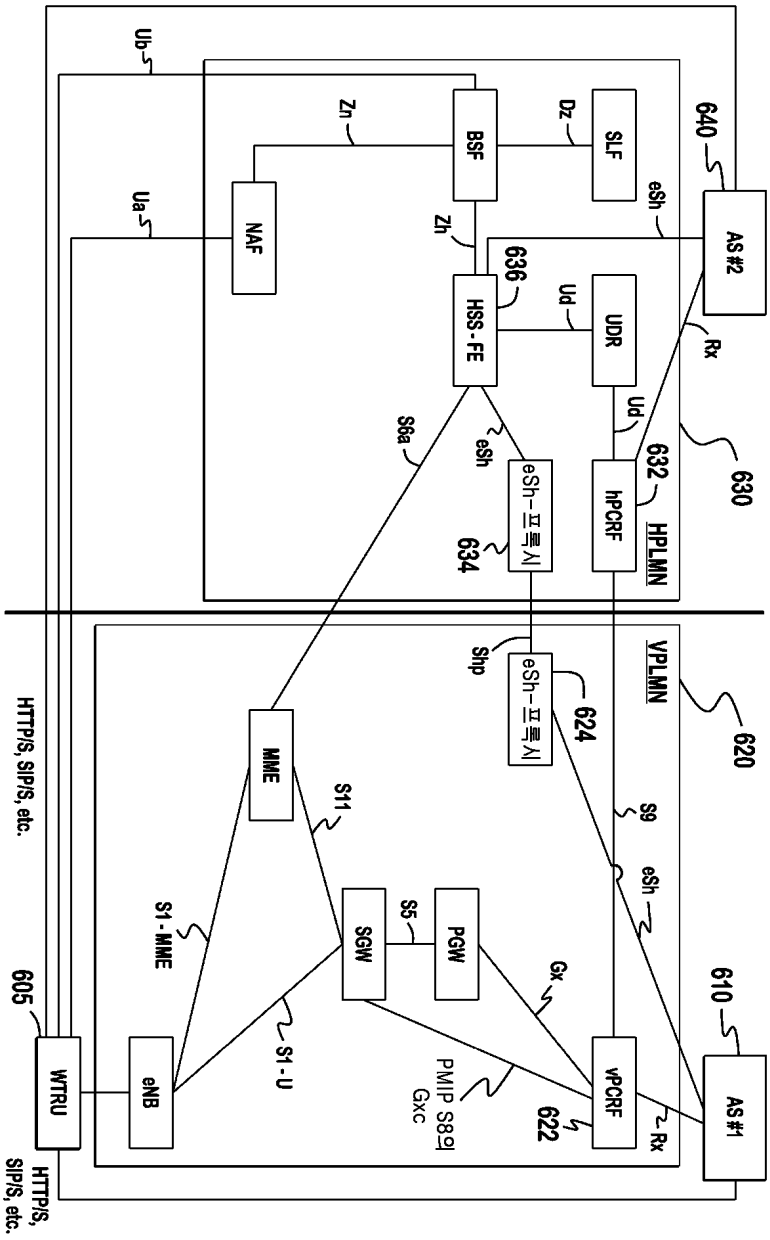
도면5b


도 5A로부터
도 5C로
사용자 데이터 요청(HPLMN 영역 또는 도메인을 포함함)
528
eSh-프록시는 WTRU와 연합하는 eSh-프록시를 검출하고, AS가 홈 네트워크로부터 이 유형의 데이터를 검색하도록 허용되는지를 체크한다
530
사용자 데이터 요청
532
사용자 데이터 응답
538
eSh-프록시는 AS가 홈 네트워크 및/또는 사용자로부터 데이터를 검색하도록 허용되는지를 체크한다
534
사용자 데이터 요청
536
AS는 자신이 HPLMN과의 협약을 이미 갖고 있는지 검출한다
540
AS는 HPLMN과 그 직접 Rx/eSh 인터페이스를 사용하도록 선택한다
542a
AS는 VPLMN과 그 Rx/eSh 인터페이스를 사용하도록 선택한다
542b

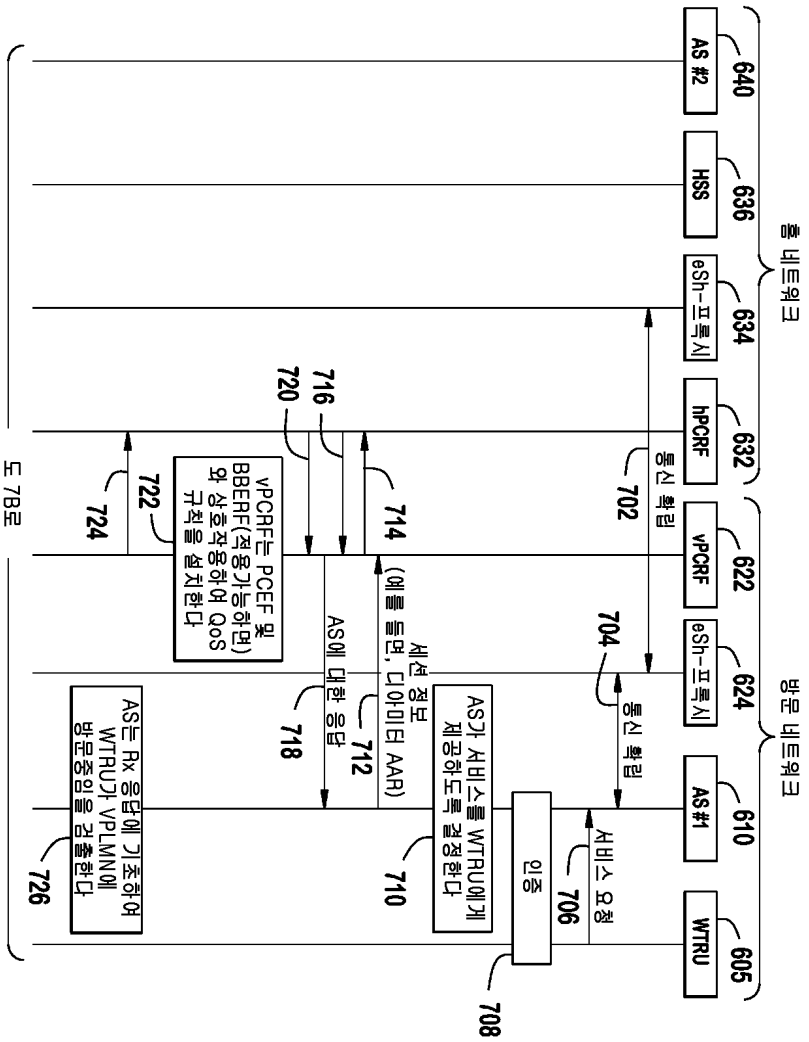
도면5c


542d
542c
도 5B로부터
eSh
Shp
eSh
Rx(HPLMN과의 협약에 따름)
AS는 VPLMN에 대하여 eSh의 사용을 계속하고 (eSh-프록시를 통하여), HPLMN에 대하여 Rx의 사용을 시작하도록 선택한다
eSh(HPLMN과의 협약에 따름)
S9
Rx
AS는 VPLMN에 대하여 Rx의 사용을 계속하고, HPLMN에 대하여 eSh의 사용을 시작하도록 선택한다

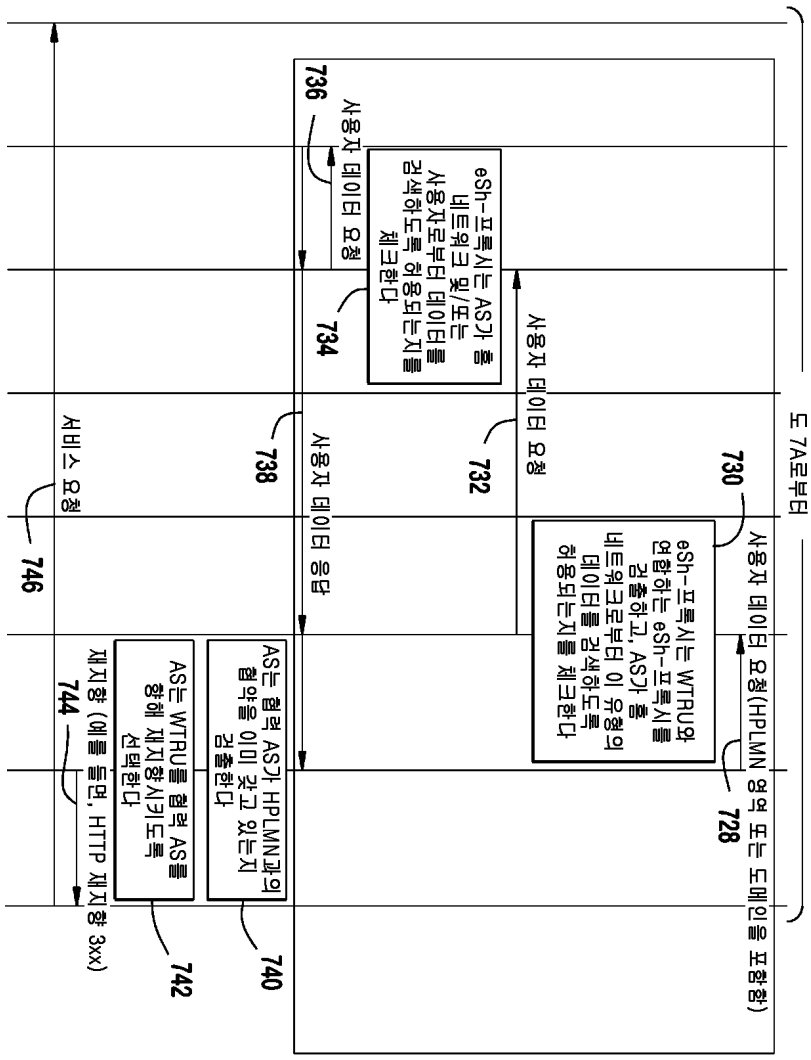
도면6


Ub
Zn
BSF
Dz
SLF
640
Ua
NAF
eSh
AS #2
Zh
636
HSS-FE
Ud
UDR
Rx
Ud
S6a
eSh
632
630
eSh-프록시
634
hPCRF
HPLMN
Shp
VPLMN
eSh-프록시
624
620
MME
S11
S9
eSh
S1-MME
S5
SGW
PGW
Gx
610
605
WTRU
eNB
S1-U
PMIP S8의
Gxc
622
vPCRF
Rx
AS #1
HTTP/S, SIP/S, etc.
HTTP/S, SIP/S, etc.

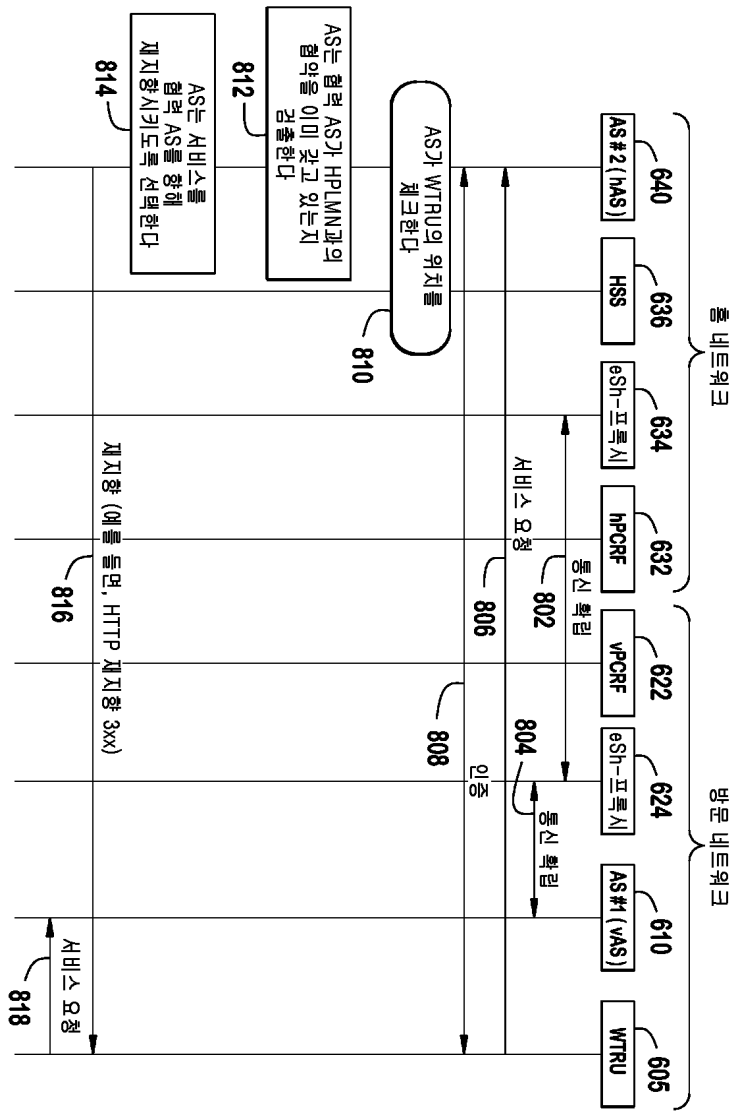
도면7a


홈 네트워크
방문 네트워크
AS #2
640
HSS
636
eSh-프록시
634
hPCRF
632
vPCRF
622
eSh-프록시
624
AS #1
610
WTRU
605
도 7B로
통신 확립
702
704
통신 확립
716
720
714
vPCRF는 PCEF 및 BBERF(적용가능하면)와 상호작용하여 QoS 규칙을 설치한다
722
724
세션 정보 (예를 들면, 디아미터 AAR)
712
AS에 대한 응답
718
AS가 서비스를 WTRU에게 제공하도록 결정한다
710
서비스 요청
706
인증
708
AS는 Rx 응답에 기초하여 WTRU가 VPLMN에 방문중임을 검출한다
726

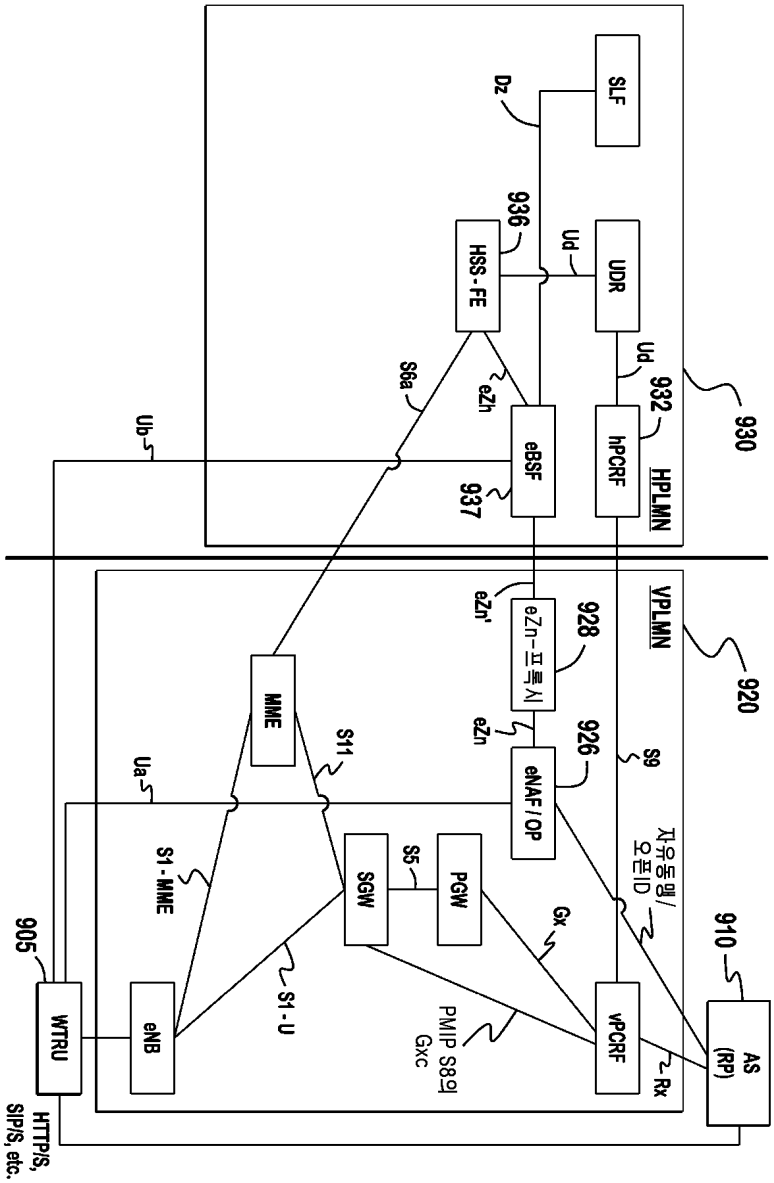
도면7b


도 7A로부터
사용자 데이터 요청(HPLMN 영역 또는 도메인을 포함함)
728
eSh-프록시는 WTRU와 연합하는 eSh-프록시를 검출하고, AS가 홈 네트워크로부터 이 유형의 데이터를 검색하도록 허용되는지를 체크한다
730
사용자 데이터 요청
732
사용자 데이터 응답
738
서비스 요청
746
사용자 데이터 요청
736
eSh-프록시는 AS가 홈 네트워크 및/또는 사용자로부터 데이터를 검색하도록 허용되는지를 체크한다
734
AS는 협력 AS가 HPLMN과의 협약을 이미 갖고 있는지 검출한다
740
AS는 WTRU를 협력 AS를 향해 재지향시키도록 선택한다
742
재지향 (예를 들면, HTTP 재지향 3xx)
744

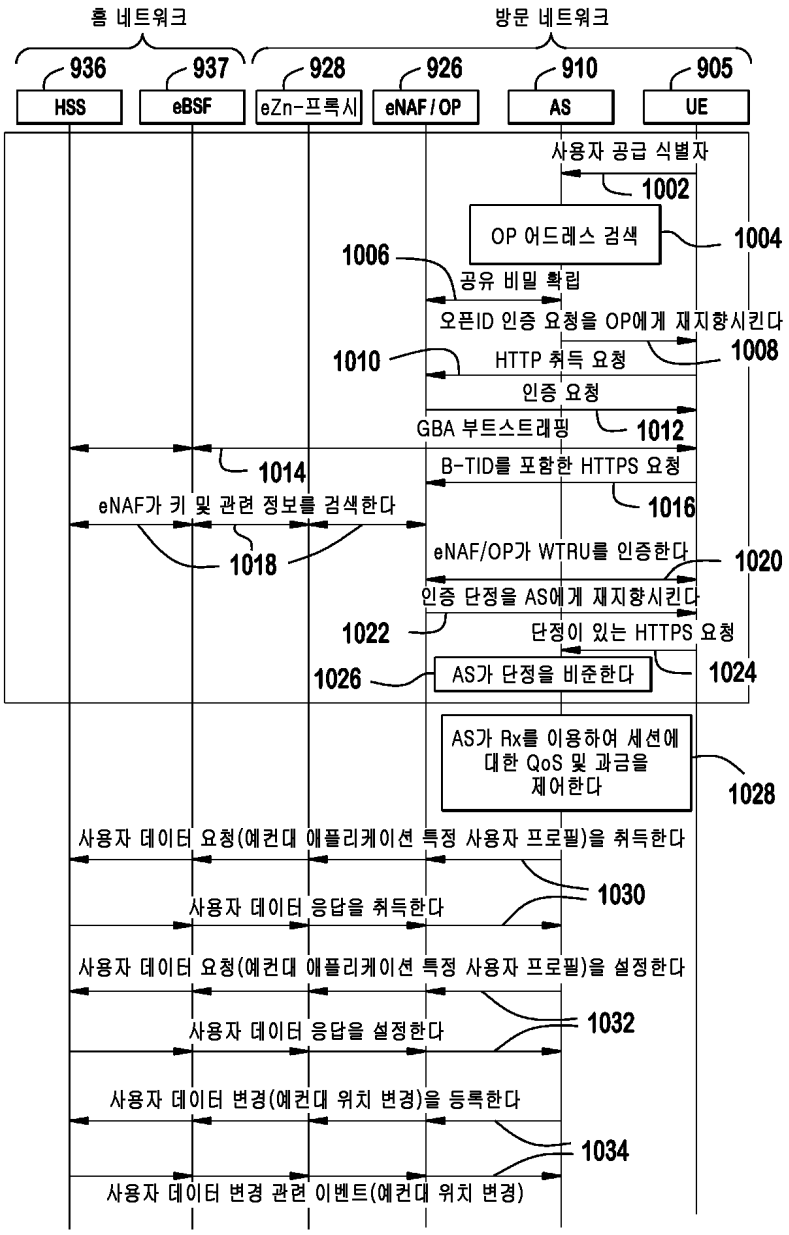
도면8


홈 네트워크
방문 네트워크
AS#2 (hAS)
640
HSS
636
eSh-프록시
634
hPCRF
632
vPCRF
622
eSh-프록시
624
AS#1 (vAS)
610
WTRU
605
AS가 WTRU의 위치를 체크한다
810
AS는 협력 AS가 HPLMN과의 결합을 이미 갖고 있는지 검출한다
812
AS는 서비스를 협력 AS를 향해 재지향시키도록 선택한다
814
서비스 요청
806
통신 확립
802
인증
808
통신 확립
804
재지향 (예를 들면, HTTP 재지향 3xx)
816
서비스 요청
818

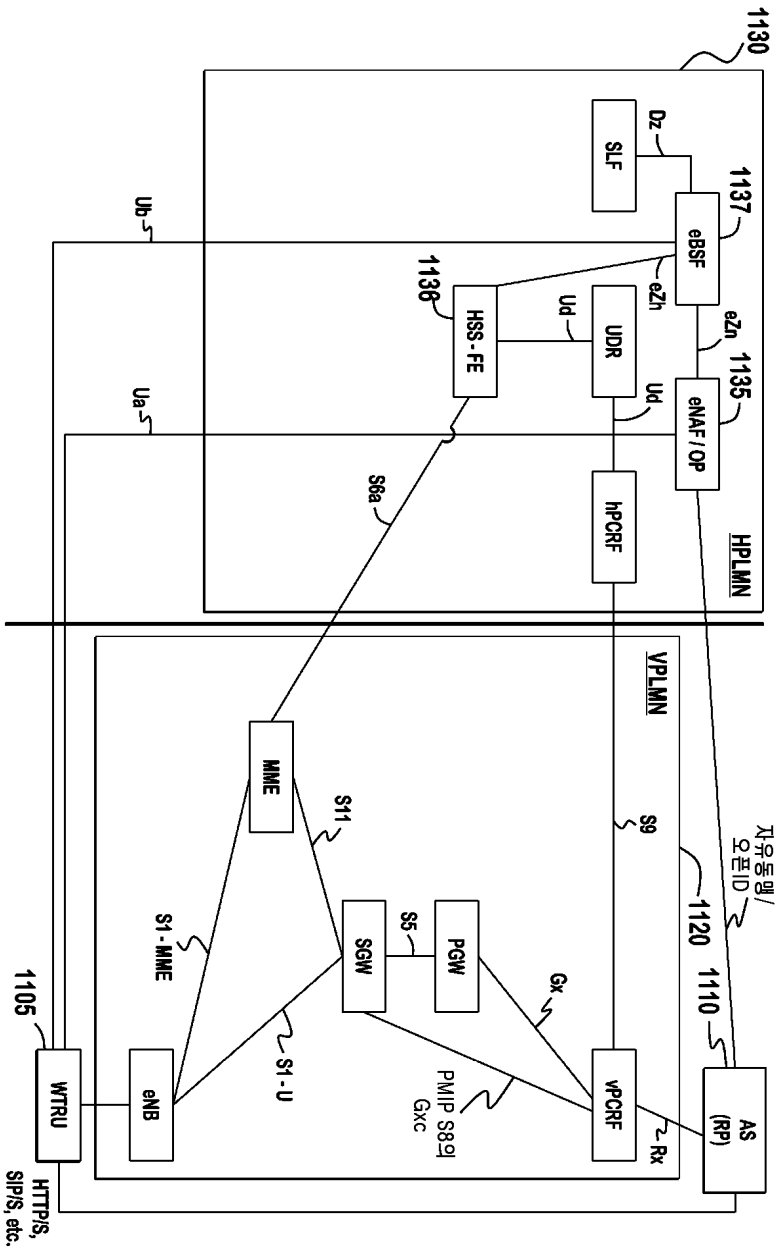
도면9


SLF
Dz
936
HSS-FE
Ud
UDR
Ud
932
930
S6a
eZh
Ub
eBSF
937
hPCRF
HPLMN
eZn'
928
eZn-프록시
VPLMN
920
MME
S11
eZn
926
S9
Ua
eNAF/OP
자유동맹/
오픈ID
S1-MME
SGW
S5
PGW
Gx
910
905
WTRU
eNB
S1-U
PMIP S8의
Gxc
vPCRF
Rx
AS
(RP)
HTTP/S,
SIP/S, etc.

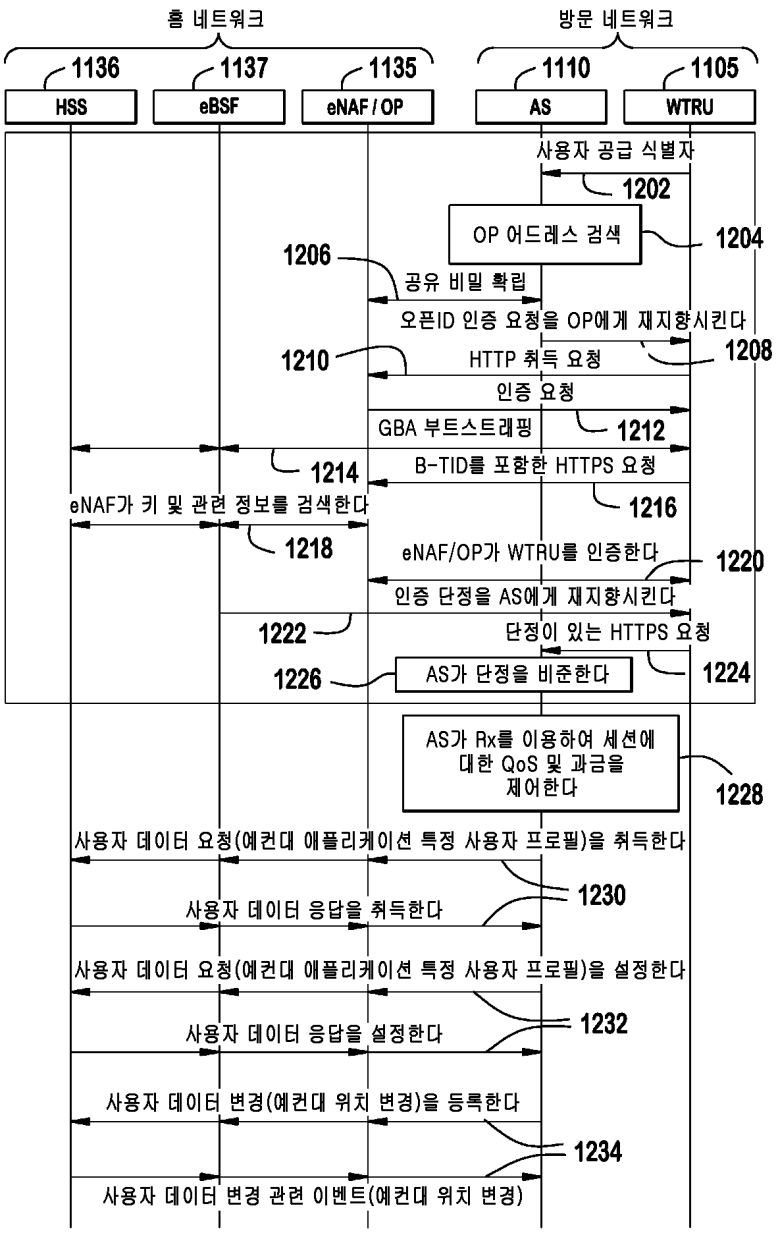
도면10


홈 네트워크
방문 네트워크
936
937
928
926
910
905
HSS
eBSF
eZn-프록시
eNAF/OP
AS
UE
사용자 공급 식별자
1002
OP 어드레스 검색
1004
1006
공유 비밀 확립
오픈ID 인증 요청을 OP에게 재지향시킨다
1010
HTTP 취득 요청
1008
인증 요청
GBA 부트스트래핑
1012
1014
B-TID를 포함한 HTTPS 요청
1016
eNAF가 키 및 관련 정보를 검색한다
1018
eNAF/OP가 WTRU를 인증한다
1020
인증 단정을 AS에게 재지향시킨다
1022
단정이 있는 HTTPS 요청
1026
AS가 단정을 비준한다
1024
AS가 Rx를 이용하여 세션에 대한 QoS 및 과금을 제어한다
1028
사용자 데이터 요청(예컨대 애플리케이션 특정 사용자 프로필)을 취득한다
1030
사용자 데이터 응답을 취득한다
사용자 데이터 요청(예컨대 애플리케이션 특정 사용자 프로필)을 설정한다
1032
사용자 데이터 응답을 설정한다
사용자 데이터 변경(예컨대 위치 변경)을 등록한다
1034
사용자 데이터 변경 관련 이벤트(예컨대 위치 변경)

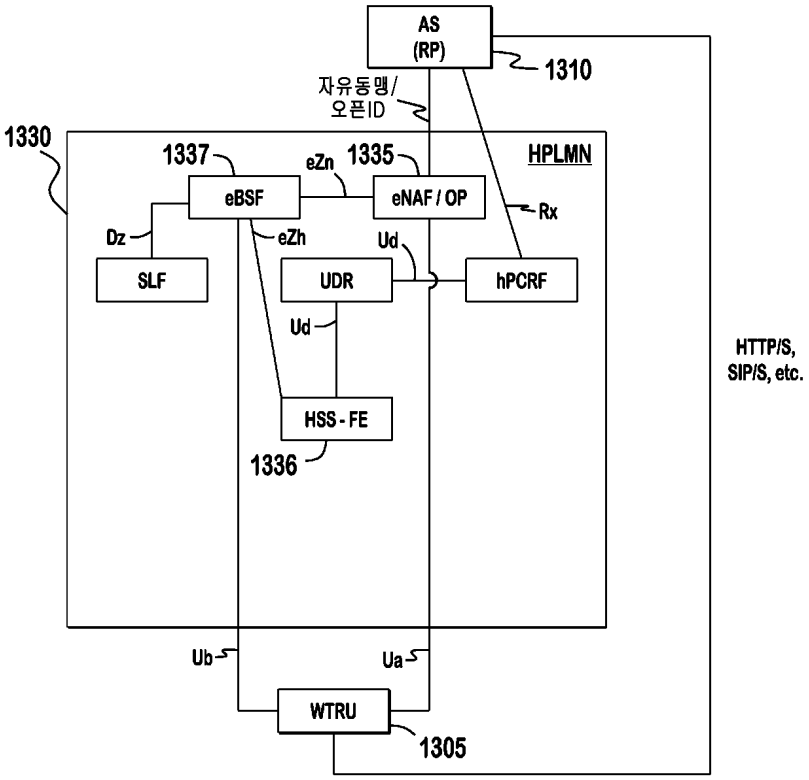
도면11


1130
SLF
Dz
1137
eBSF
Ub
1136
HSS-FE
eZh
Ud
UDR
eZn
1135
eNAF/OP
Ud
Ua
S6a
hPCRF
HPLMN
VPLMN
MME
S11
S9
자유동일/
오픈ID
S1-MME
SGW
S5
PGW
Gx
1120
1110
1105
S1-U
PMIP S8의
Gxc
vPCRF
Rx
AS
(RP)
WTRU
eNB
HTTP/S,
SIP/S, etc.

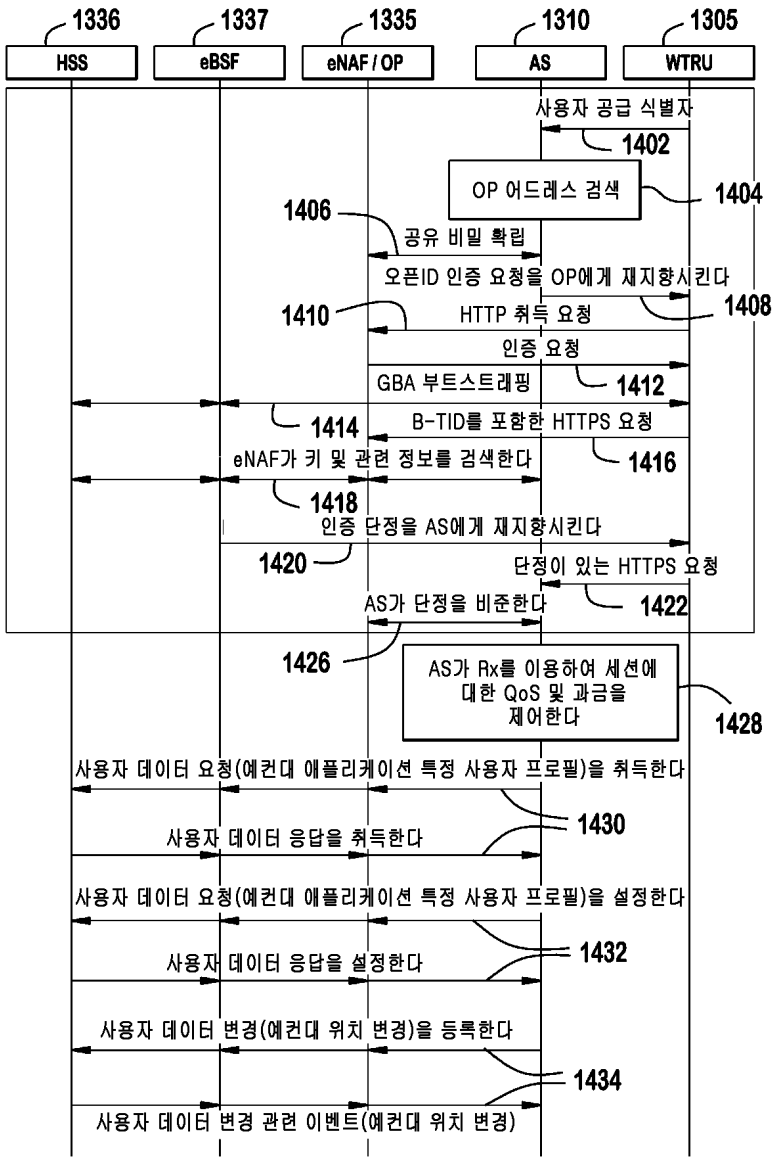
도면12


홈 네트워크
방문 네트워크
1136
1137
1135
1110
1105
HSS
eBSF
eNAF / OP
AS
WTRU
사용자 공급 식별자
1202
OP 어드레스 검색
1204
1206
공유 비밀 확립
오픈ID 인증 요청을 OP에게 재지향시킨다
1210
HTTP 취득 요청
1208
인증 요청
GBA 부트스트래핑
1212
1214
B-TID를 포함한 HTTPS 요청
1216
eNAF가 키 및 관련 정보를 검색한다
1218
eNAF/OP가 WTRU를 인증한다
1220
인증 단정을 AS에게 재지향시킨다
1222
단정이 있는 HTTPS 요청
1226
AS가 단정을 비준한다
1224
AS가 Rx를 이용하여 세션에 대한 QoS 및 과금을 제어한다
1228
사용자 데이터 요청(예컨대 애플리케이션 특정 사용자 프로필)을 취득한다
1230
사용자 데이터 응답을 취득한다
사용자 데이터 요청(예컨대 애플리케이션 특정 사용자 프로필)을 설정한다
1232
사용자 데이터 응답을 설정한다
사용자 데이터 변경(예컨대 위치 변경)을 등록한다
1234
사용자 데이터 변경 관련 이벤트(예컨대 위치 변경)

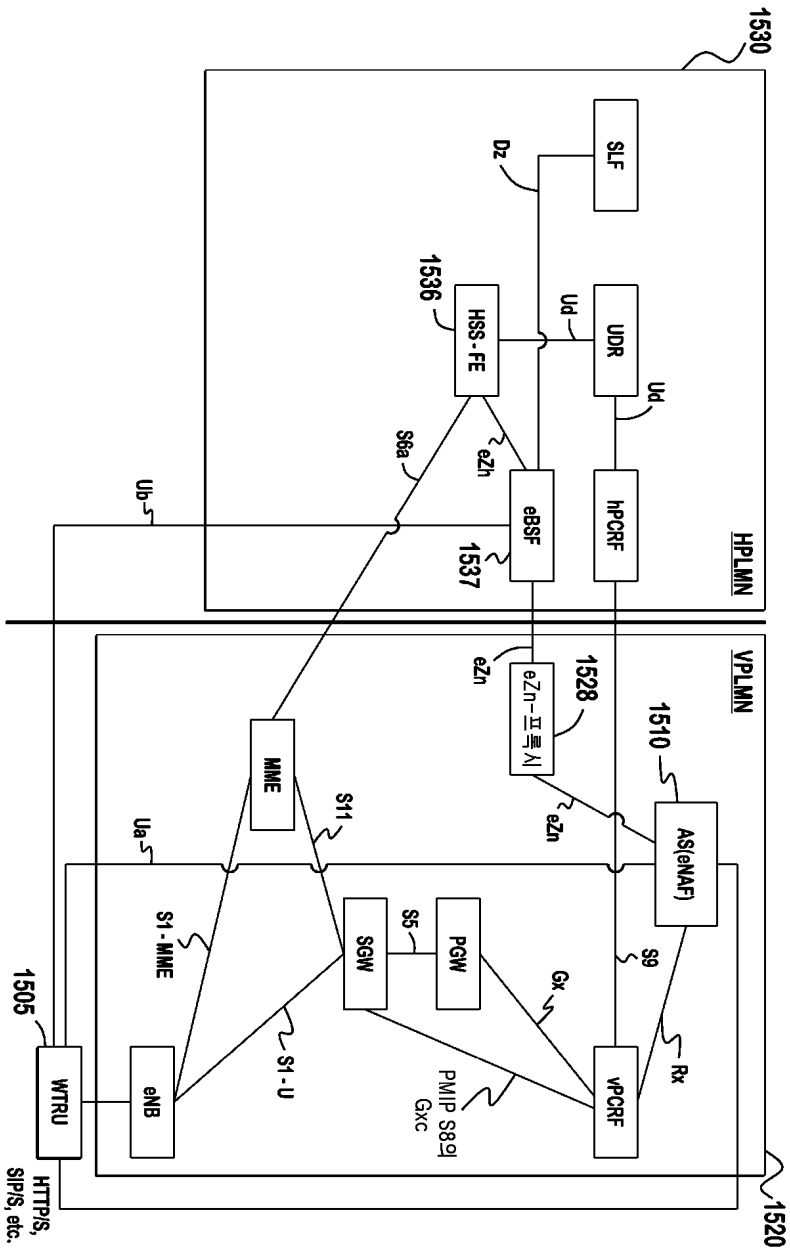
도면13


AS
(RP)
1310
자유동맹/
오픈ID
1330
1337
eZn
1335
HPLMN
eBSF
eNAF / OP
Rx
Dz
eZh
Ud
SLF
UDR
hPCRF
Ud
HSS - FE
1336
HTTP/S,
SIP/S, etc.
Ub
Ua
WTRU
1305

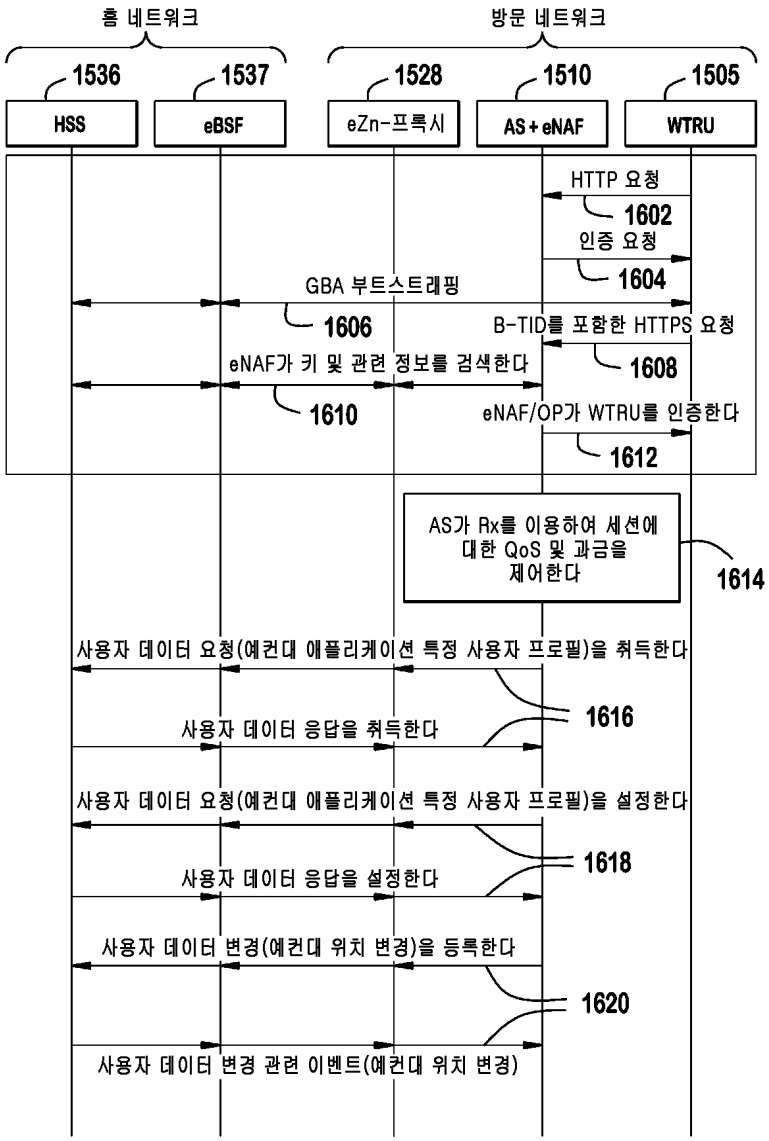
도면14


1336
1337
1335
1310
1305
HSS
eBSF
eNAF / OP
AS
WTRU
사용자 공급 식별자
1402
OP 어드레스 검색
1404
1406
공유 비밀 확립
오픈ID 인증 요청을 OP에게 재지향시킨다
1410
HTTP 취득 요청
1408
인증 요청
GBA 부트스트레핑
1412
1414
B-TID를 포함한 HTTPS 요청
eNAF가 키 및 관련 정보를 검색한다
1416
1418
인증 단정을 AS에게 재지향시킨다
1420
단정이 있는 HTTPS 요청
AS가 단정을 비준한다
1422
1426
AS가 Rx를 이용하여 세션에 대한 QoS 및 과금을 제어한다
1428
사용자 데이터 요청(예컨대 애플리케이션 특정 사용자 프로필)을 취득한다
1430
사용자 데이터 응답을 취득한다
사용자 데이터 요청(예컨대 애플리케이션 특정 사용자 프로필)을 설정한다
1432
사용자 데이터 응답을 설정한다
사용자 데이터 변경(예컨대 위치 변경)을 등록한다
1434
사용자 데이터 변경 관련 이벤트(예컨대 위치 변경)

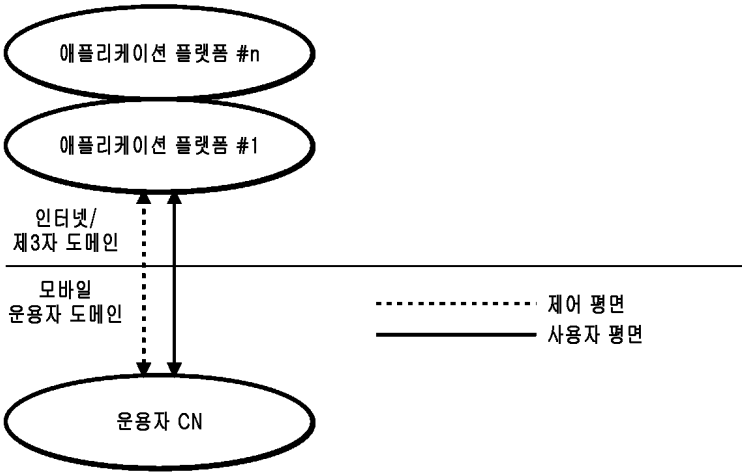
도면15


1530
SLF
Dz
1536
HSS-FE
Ud
UDR
Ud
S6a
eZh
Ub
eBSF
hPCRF
1537
HPLMN
VPLMN
eZn
1528
eZn-프록시
1510
MME
S11
eZn
AS(eNAF)
Ua
S1-MME
SGW
S5
PGW
S9
Gx
1505
WTRU
eNB
S1-U
PMIP S8의 Gxc
vPCRF
Rx
HTTP/S, SIP/S, etc.
1520

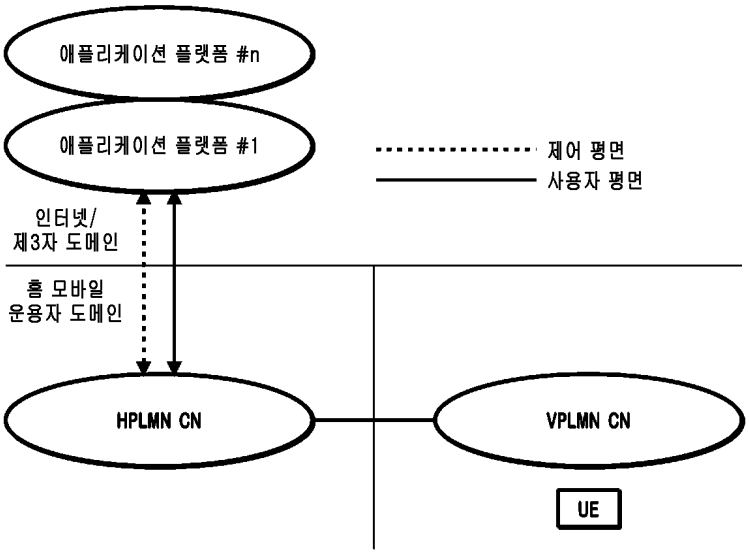
도면16


홈 네트워크
방문 네트워크
1536
1537
1528
1510
1505
HSS
eBSF
eZn-프록시
AS+eNAF
WTRU
HTTP 요청
1602
인증 요청
1604
GBA 부트스트래핑
1606
B-TID를 포함한 HTTPS 요청
1608
eNAF가 키 및 관련 정보를 검색한다
1610
eNAF/OP가 WTRU를 인증한다
1612
AS가 Rx를 이용하여 세션에 대한 QoS 및 과금을 제어한다
1614
사용자 데이터 요청(예컨대 애플리케이션 특정 사용자 프로필)을 취득한다
1616
사용자 데이터 응답을 취득한다
사용자 데이터 요청(예컨대 애플리케이션 특정 사용자 프로필)을 설정한다
1618
사용자 데이터 응답을 설정한다
사용자 데이터 변경(예컨대 위치 변경)을 등록한다
1620
사용자 데이터 변경 관련 이벤트(예컨대 위치 변경)

도면17


애플리케이션 플랫폼 #n
애플리케이션 플랫폼 #1
인터넷/
제3자 도메인
모바일
운용자 도메인
제어 평면
사용자 평면
운용자 CN

도면18


애플리케이션 플랫폼 #n
애플리케이션 플랫폼 #1
제어 평면
사용자 평면
인터넷/
제3자 도메인
홈 모바일
운용자 도메인
HPLMN CN
VPLMN CN
UE