(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년06월14일
(11) 등록번호 10-2408155
(24) 등록일자 2022년06월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *H04M 3/22* (2006.01)
H04W 12/02 (2021.01) *H04W 12/0431* (2021.01)
H04W 12/06 (2021.01) *H04W 12/72* (2021.01)
H04W 8/08 (2009.01) *H04W 84/04* (2009.01)
(52) CPC특허분류
H04L 63/0876 (2013.01)
H04L 63/30 (2013.01)
(21) 출원번호 10-2021-7008816(분할)
(22) 출원일자(국제) 2017년07월12일
심사청구일자 2021년04월23일
(85) 번역문제출일자 2021년03월24일
(65) 공개번호 10-2021-0035925
(43) 공개일자 2021년04월01일
(62) 원출원 특허 10-2019-7004674
원출원일자(국제) 2017년07월12일
심사청구일자 2019년02월18일
(86) 국제출원번호 PCT/EP2017/067527
(87) 국제공개번호 WO 2018/015243
국제공개일자 2018년01월25일
(30) 우선권주장
62/363,814 2016년07월18일 미국(US)
(56) 선행기술조사문헌
US20120252445 A1
US20130128873 A1

(73) 특허권자
텔레호낙티에볼라게트 엘엠 에릭슨(피유비엘)
스웨덴 스톡홀롬 83 에스이-164
(72) 발명자
나카르미, 프라즈올, 쿠마르
스웨덴 19142 솔렌투나 스투프베겐 17
토르비넨, 베사
핀란드 21570 사우보 사우본티 42
(뒷면에 계속)
(74) 대리인
장수길, 백만기

전체 청구항 수 : 총 19 항 심사관 : 문형섭

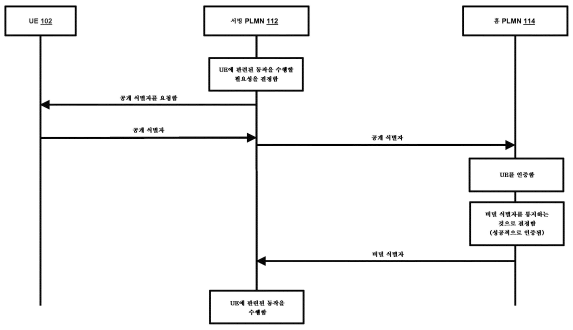
(54) 발명의 명칭 **비밀 식별자를 사용하는 사용자 장비에 관련된 동작**

(57) 요 약

사용자 장비(UE)(102)와 연관된 서빙 공중 육상 모바일 네트워크(PLMN)(112)의 네트워크 노드(106)에 의해 수행되는 방법은, UE를 고유하게 식별하는 비밀 식별자(110)를 획득하는 단계 - 여기서 비밀 식별자는 UE와 적어도 UE의 홈 PLMN 사이에서 공유되고 홈 PLMN에 의해 네트워크 노드와 공유되는 비밀임 -; 및 비밀 식별자를 사용하

(뒷면에 계속)

대 표 도



여 UE에 관련된 동작(108)을 수행하는 단계를 포함한다. 다른 방법들, 컴퓨터 프로그램들, 컴퓨터 프로그램 제품들, 네트워크 노드들 및 서빙 PLMN이 또한 개시된다.

(52) CPC특허분류
H04M 3/2281 (2013.01)
H04W 12/02 (2021.01)
H04W 12/0431 (2021.01)
H04W 12/06 (2021.01)
H04W 12/72 (2021.01)
H04W 8/082 (2013.01)
H04W 84/042 (2013.01)

(72) 발명자
벤 헨다, 노아멘
스웨덴 16247 스톡홀름 투물트그랜드 228
조스트, 크리스틴
스웨덴 22351 룬트 베스트라 마르텐스가탄 12

명 세 서

청구범위

청구항 1

사용자 장비(user equipment)(UE)와 연관된 서빙 공중 육상 모바일 네트워크(public land mobile network)(PLMN)의 네트워크 노드에 의해 수행되는 방법으로서,

상기 서빙 PLMN의 상기 네트워크 노드가 상기 UE로부터 상기 UE에 대응하는 공개 식별자 또는 가명을 수신하는 단계 - 상기 UE는 홈 PLMN을 갖고, 상기 서빙 PLMN은 상기 UE의 홈 PLMN이 아님 -;

상기 서빙 PLMN의 상기 네트워크 노드가 상기 UE에 대응하는 상기 공개 식별자 또는 가명을 상기 UE의 홈 PLMN에 전달하는 단계;

상기 서빙 PLMN의 상기 네트워크 노드가 상기 공개 식별자 또는 가명을 상기 UE의 홈 PLMN에 전달하는 것에 응답하여, 상기 UE의 홈 PLMN으로부터 IMSI(International Mobile Subscriber Identity)를 상기 서빙 PLMN의 상기 네트워크 노드가 수신하는 단계 - 상기 IMSI는 상기 UE를 고유하게 식별하고, 상기 UE와 적어도 상기 UE의 홈 PLMN 사이에서 공유되는 비밀 식별자임 -;

상기 홈 PLMN으로부터 인증 정보를 수신하는 단계 - 상기 인증 정보는 상기 서빙 PLMN이 상기 UE의 인증을 수행할 수 있도록 함 -;

상기 인증 정보를 사용하여 상기 서빙 PLMN에 의해 상기 UE가 성공적으로 인증되었음을 결정하는 단계; 및

상기 IMSI를 사용하여 상기 UE의 합법적 인터셉션(interception)에 관련된 동작을 수행하는 단계를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 IMSI는 상기 UE가 상기 홈 PLMN에 의해 성공적으로 인증된 것에 기초하여 수신되는 방법.

청구항 3

제1항에 있어서,

상기 IMSI를 수신하는 단계는 상기 홈 PLMN으로부터 확장가능 인증 프로토콜(Extensible Authentication Protocol)(EAP) 메시지를 수신하는 단계를 포함하는 방법.

청구항 4

제1항에 있어서,

상기 인증 정보는 진화된 패킷 시스템-인증 및 키 합의(Evolved Packet System-Authentication and Key Agreement)(EPS-AKA) 포맷으로 형성되고, 인증 벡터를 통해 상기 서빙 PLMN에 통신되는 방법.

청구항 5

제1항에 있어서,

상기 UE가 상기 서빙 PLMN에 의해 성공적으로 인증되었음을 상기 홈 PLMN에 통지하도록 인증 성공 메시지를 상기 홈 PLMN에 전달하는 단계를 더 포함하고, 상기 인증 성공 메시지는 상기 홈 PLMN이 상기 비밀 식별자를 상기 서빙 PLMN에 전송하도록 트리거하는 방법.

청구항 6

제1항에 있어서,

상기 IMSI를 획득하는 단계는 상기 UE가 상기 서빙 PLMN에 의해 인증되기 전에 상기 홈 PLMN으로부터 상기 IMSI

를 수신하는 단계를 포함하는 방법.

청구항 7

제6항에 있어서,

상기 홈 PLMN으로부터 상기 IMSI를 수신하는 단계는 상기 홈 PLMN으로부터 인증-정보-응답(authentication-information-answer) 메시지를 수신하는 단계를 포함하는 방법.

청구항 8

제1항에 있어서,

상기 IMSI를 수신하는 단계는 상기 UE가 상기 서빙 PLMN에 의해 인증된 후에 상기 홈 PLMN으로부터 상기 IMSI를 수신하는 단계를 포함하는 방법.

청구항 9

제8항에 있어서,

상기 홈 PLMN으로부터 상기 비밀 식별자를 수신하는 단계는 상기 홈 PLMN으로부터 업데이트-위치-응답(update-location-answer) 메시지를 수신하는 단계를 포함하는 방법.

청구항 10

제9항에 있어서,

상기 공개 식별자 또는 상기 가명, 그리고 상기 IMSI가 상기 UE에 대응하는지 검증하는 단계를 더 포함하는 방법.

청구항 11

제10항에 있어서,

상기 검증하는 단계는:

상기 IMSI를 암호화하기 위한 암호화 정보를 획득하는 단계;

상기 암호화 정보를 이용하여 상기 IMSI를 암호화하여 암호화된 IMSI를 생성하는 단계;

비교에 기초하여 상기 암호화된 IMSI 및 상기 공개 식별자가 매칭하는지 결정하는 단계; 및

상기 암호화된 IMSI 및 상기 공개 식별자가 매칭한다는 결정에 기초하여 상기 공개 식별자 및 상기 IMSI가 상기 UE에 대응하는지를 검증하는 단계를 포함하는 방법.

청구항 12

제11항에 있어서,

상기 암호화 정보는 상기 홈 PLMN의 공개 키를 포함하는 방법.

청구항 13

사용자 장비(UE)와 연관된 서빙 공중 육상 모바일 네트워크(PLMN)의 네트워크 노드로서,

프로세서 및 메모리를 포함하고,

상기 메모리는 상기 프로세서에 의해 실행가능한 명령어들을 포함하고, 상기 네트워크 노드는,

상기 UE로부터 상기 UE에 대응하는 공개 식별자 또는 가명을 수신하고 - 상기 UE는 홈 PLMN을 갖고, 상기 서빙 PLMN은 상기 UE의 홈 PLMN이 아님 -;

상기 공개 식별자 또는 가명을 상기 UE의 홈 PLMN에 전달하고;

상기 공개 식별자 또는 가명을 전달하는 것에 응답하여, 상기 홈 PLMN으로부터 IMSI를 수신하고 - 상기 IMSI는

상기 UE를 고유하게 식별하고, 상기 UE와 적어도 상기 홈 PLMN 사이에서 공유되는 비밀 식별자임 -;

상기 홈 PLMN으로부터 인증 정보를 수신하고 - 상기 인증 정보는 상기 서빙 PLMN이 상기 UE의 인증을 수행할 수 있도록 함 -;

상기 인증 정보를 사용하여 상기 서빙 PLMN에 의해 상기 UE가 성공적으로 인증됨을 결정하고;

상기 IMSI를 사용하여 상기 UE의 합법적 인터셉션에 관련된 동작을 수행하도록 구성되는 네트워크 노드.

청구항 14

제13항에 있어서, 상기 공개 식별자는 상기 IMSI의 암호화된 버전을 포함하는 네트워크 노드.

청구항 15

사용자 장비(UE)와 연관된 서빙 공중 육상 모바일 네트워크(PLMN)에 의해 수행되는 방법으로서,

상기 서빙 PLMN이 상기 UE에 대응하는 공개 식별자 또는 가명을 상기 UE로부터 수신하는 단계 - 상기 UE는 홈 PLMN을 갖고, 상기 서빙 PLMN은 상기 UE의 홈 PLMN이 아님 -;

상기 서빙 PLMN이 수신된 상기 공개 식별자 또는 가명을 상기 UE의 홈 PLMN에 전달하는 단계;

상기 UE가 상기 홈 PLMN 또는 상기 서빙 PLMN에 의해 성공적으로 인증된 후 상기 UE의 홈 PLMN으로부터 IMSI를 상기 서빙 PLMN이 수신하는 단계 - 상기 IMSI는 상기 UE를 고유하게 식별하고 상기 UE와 상기 홈 PLMN 사이에서 이미 공유된 비밀 식별자임 -;

상기 서빙 PLMN이 상기 홈 PLMN으로부터 인증 정보를 수신하는 단계 - 상기 인증 정보는 상기 서빙 PLMN이 상기 UE의 인증을 수행할 수 있도록 함 -;

상기 서빙 PLMN이 상기 인증 정보를 사용하여 상기 서빙 PLMN에 의해 상기 UE가 성공적으로 인증되었음을 결정하는 단계; 및

상기 UE와 관련된 합법적인 인터셉트를 수행하는 단계를 포함하는 방법.

청구항 16

제15항에 있어서,

상기 UE는 상기 서빙 PLMN에 의해 인증되는 방법.

청구항 17

제15항에 있어서,

상기 공개 식별자는 상기 IMSI의 암호화된 버전을 포함하는 방법.

청구항 18

서빙 PLMN의 보안 기능에 의해 수행되는 방법으로서,

사용자 장비(UE)에 의해 전송된 메시지를 상기 서빙 PLMN(S-PLMN)의 상기 보안 기능이 수신하는 단계 - 상기 UE는 상기 S-PLMN과 다른 홈 PLMN (H-PLMN)을 가지고, 상기 UE는 가입 식별자를 저장하며, 상기 메시지는 상기 가입 식별자의 암호화된 버전을 포함함 -;

상기 S-PLMN의 상기 보안 기능이 상기 가입 식별자의 암호화된 버전을 포함하는 제1 인증 메시지를 상기 UE의 H-PLMN의 인증 기능에 전송하는 단계;

상기 S-PLMN의 상기 보안 기능이 상기 UE의 H-PLMN의 상기 인증 기능에 의해 전송된 제1 인증 응답 메시지를 수신하는 단계 - 상기 제1 인증 응답 메시지는 상기 UE를 인증하는데 사용하기 위한 인증 정보를 포함함 -;

상기 S-PLMN의 상기 보안 기능이 상기 H-PLMN의 네트워크 노드에 의해 전송 된 상기 인증 정보를 수신한 후, 상기 S-PLMN의 상기 보안 기능이 상기 UE의 인증을 지원하는 동작을 수행하는 단계;

상기 S-PLMN의 상기 보안 기능이 상기 UE의 인증을 지원하는 상기 동작을 수행한 후, 상기 S-PLMN의 상기 보안

기능이 상기 UE의 H-PLMN의 상기 인증 기능에 제2 인증 메시지를 전송하는 단계 - 상기 제2 인증 메시지는 상기 UE의 H-PLMN의 상기 인증 기능이 상기 UE의 인증 여부를 검증할 수 있도록 함 -;

상기 S-PLMN의 상기 보안 기능이 상기 UE의 H-PLMN의 상기 인증 기능에 상기 인증 메시지를 전송한 후, 상기 S-PLMN의 상기 보안 기능이 상기 UE의 H-PLMN의 상기 인증 기능에 의해 전송된 제2 인증 응답을 수신하는 단계 - 상기 UE의 H-PLMN의 상기 인증 기능에 의해 전송된 상기 제2 인증 응답은 상기 가입 식별자를 포함하고 암호화 키를 더 포함함 -;

상기 제2 인증 응답을 수신한 후, 상기 S-PLMN의 상기 보안 기능은 상기 S-PLMN의 합법적인 인터셉트 기능에 상기 가입 식별자를 제공하는 단계; 및

상기 가입 식별자를 사용하여 상기 UE의 합법적 인터셉션과 관련된 동작을 상기 합법적인 인터셉트 기능이 수행하는 단계를 포함하는 방법.

청구항 19

제18항에 있어서,

상기 UE의 인증을 지원하는 동작을 수행하는 단계는 상기 인증 정보를 포함하는 메시지를 상기 UE를 향해 전송하는 단계로 이루어지는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 사용자 장비(user equipment)(UE)에 관련된 식별자가 서빙 공중 육상 모바일 네트워크(public land mobile network)(PLMN)에 이용가능하게 되는 방법들에 관한 것이다. 본 발명은 또한 네트워크 노드들, 공중 모바일 육상 네트워크, 컴퓨터 프로그램들 및 컴퓨터 프로그램 제품들에 관한 것이다.

배 경 기 술

[0002] 기존의 무선 네트워크 시스템들(예를 들어, 2G, 3G, 4G 시스템들)에서, 특정 동작들은 (UE의 홈 PLMN 이외의) 서빙 PLMN들이 UE의 특정 식별자, 예컨대 국제 모바일 가입자 아이덴티티(International Mobile Subscriber Identity)(IMSI)로의 액세스를 가질 것을 요구한다. 그러나, UE에 대응하는 장기 식별자(long-term identifier)의 지식은, 예를 들어, 식별자에 기초하여 사용자의 위치를 결정하는 것에 의해 제3자들이 사용자의 프라이버시를 손상시키게 한다. 그 결과, 이 UE 식별자는 전형적으로 개인적으로 유지되고 비밀로서 취급되며, 이와 같이, UE, UE의 홈 PLMN, 및 아이덴티티로의 액세스가 홈 PLMN 또는 UE에 의해 승인된 임의의 다른 당사자 또는 디바이스에만 종종 이용가능하다. 일부 기존 네트워크들이 PLMN들과 디바이스들 사이에서 UE의 식별자를 통신하기 위해 UE 아이덴티티들에 대한 암호화 방법들 및/또는 가명들을 활용하지만, 통신된 식별자는 일부 서빙 PLMN 동작들에 의해 요구되는 UE의 비밀, 장기 식별자가 아니다.

[0003] 그에 따라, 비밀 UE 식별자들의 신뢰된 통신을 위한 개선된 기법들은 민감한 사용자 정보를 신뢰되지 않은 당사자들에게 노출시키는 일 없이 요구된 UE 기능성이 PLMN들에 걸쳐 유지된다는 것을 보장할 필요가 있다.

[0004] 차세대 시스템을 위한 3세대 파트너십 프로젝트 내에서 일반적인 보안 관련 논의들이 진행 중이다. 3GPP TR 33.899 V0.2.0은 그러한 시스템에 관련된 위협들, 잠재적 요건들 및 솔루션들을 논의한다. 그 문헌은, 새로운 시스템을 설계할 때 합법적 인터셉션(interception) 및 다른 로컬 규제들이 고려되어야 하지만, 또한 가입자의 아이덴티티의 노출이 프라이버시 침해들을 초래할 수도 있다고 명시하고 있다. 서빙 PLMN이, 예를 들어, 부적절한 가입자의 인터셉션, 잘못된 과금, 및 네트워크 리소스들로의 비인가된 액세스의 위험을 무릅쓰는 일 없이 합법적 인터셉션을 수행할 수 있게 하는 복잡한 문제에 대한 어떠한 솔루션도 제공되지 않는다.

발명의 내용

[0005] 본 발명의 하나 이상의 실시예의 목적은 민감한 사용자 정보를 신뢰되지 않은 당사자들에게 노출시키는 일 없이 PLMN들에 걸친 비밀 UE 식별자의 개선된 신뢰된 통신을 가능하게 하는 것이다.

[0006] 본 명세서의 하나 이상의 실시예는 UE의 홈 PLMN으로부터의 UE의 비밀 식별자를 서빙 PLMN으로 통신하는 것을 가능하게 한다. 일단 서빙 PLMN에 의해 획득된다면, 비밀 식별자는 UE에 관련된 동작을 수행하기 위해 서빙

PLMN에 의해 활용될 수 있다. 이로써, 가명 식별자에 기초하는 서빙 PLMN에서의 동작들에 관련하여 네트워크 시스템 복잡성 및 보안 위협들이 감소될 수 있다는 것도 또한 달성된다.

[0007] 본 발명의 제1 양태는 UE와 연관된 서빙 PLMN의 네트워크 노드에 의해 수행되는 방법에 관한 것이다. 이 방법에서, 네트워크 노드는 UE를 고유하게 식별하는 비밀 식별자를 획득한다. 비밀 식별자는, UE와 적어도 UE의 홈 PLMN 사이에서 공유되고 홈 PLMN에 의해 네트워크 노드와 공유되는 비밀이다. 이 방법은 또한, 네트워크 노드가 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하는 단계를 포함한다.

[0008] 본 발명의 제2 양태는 UE와 연관된 홈 PLMN의 네트워크 노드에 의해 수행되는 방법에 관한 것이다. 네트워크 노드는, UE의 서빙 PLMN에, UE를 고유하게 식별하는 비밀 식별자를 통지하는 것으로 결정한다. 비밀 식별자는, UE와 적어도 홈 PLMN 사이에서 공유되는 비밀이다. 이 방법에 따르면, 홈 PLMN의 네트워크 노드는 서빙 PLMN에 비밀 식별자를 통지한다. 서빙 PLMN에 비밀 식별자를 통지하는 것은, 서빙 PLMN이 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하게 한다.

[0009] 제3 양태는 UE와 연관된 서빙 PLMN의 네트워크 노드에 관한 것이다. 네트워크 노드는 UE를 고유하게 식별하는 비밀 식별자를 획득하고 - 여기서 비밀 식별자는, UE와 적어도 UE의 홈 PLMN 사이에서 공유되고 홈 PLMN에 의해 네트워크 노드와 공유되는 비밀임 -; 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하도록 구성된다.

[0010] 제4 양태는 UE와 연관된 홈 PLMN의 네트워크 노드에 관한 것이다. 이 네트워크 노드는, UE의 서빙 PLMN에, UE를 고유하게 식별하는 비밀 식별자를 통지하는 것으로 결정하고 - 여기서 비밀 식별자는, UE와 적어도 홈 PLMN 사이에서 공유되는 비밀임 -; 서빙 PLMN에 비밀 식별자를 통지하도록 - 비밀 식별자는 서빙 PLMN이 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하게 함 - 구성된다.

[0011] 제5 양태는 UE와 연관된 서빙 PLMN의 네트워크 노드에 관한 것이고, 네트워크 노드는 프로세서 및 메모리를 포함하고, 메모리는, 네트워크 노드가 UE를 고유하게 식별하는 비밀 식별자를 획득하고 - 여기서 비밀 식별자는, UE와 적어도 UE의 홈 PLMN 사이에서 공유되고 홈 PLMN에 의해 네트워크 노드와 공유하는 비밀임 -; 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하도록 구성되게 하는, 프로세서에 의해 실행가능한 명령어들을 포함한다.

[0012] 제6 양태는 UE와 연관된 홈 PLMN의 네트워크 노드에 관한 것이고, 네트워크 노드는 프로세서 및 메모리를 포함하고, 메모리는, 네트워크 노드가, UE의 서빙 PLMN에, UE를 고유하게 식별하는 비밀 식별자를 통지하는 것으로 결정하고 - 여기서 비밀 식별자는, UE와 적어도 홈 PLMN 사이에서 공유되는 비밀임 -; 서빙 PLMN에 비밀 식별자를 통지하도록 - 비밀 식별자는 서빙 PLMN이 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하게 함 - 구성되게 하는, 프로세서에 의해 실행가능한 명령어들을 포함한다.

[0013] 제7 양태는 UE와 연관된 서빙 PLMN의 네트워크 노드에 관한 것이다. 네트워크 노드는, UE를 고유하게 식별하는 비밀 식별자를 획득하도록 구성되는 제1 모듈 - 여기서 비밀 식별자는, UE와 적어도 UE의 홈 PLMN 사이에서 공유되고 홈 PLMN에 의해 네트워크 노드와 공유되는 비밀임 -; 및 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하기 위한 제2 모듈을 포함한다.

[0014] 제8 양태는 UE와 연관된 홈 PLMN의 네트워크 노드에 관한 것이다. 네트워크 노드는, UE의 서빙 PLMN에, UE를 고유하게 식별하는 비밀 식별자를 통지하는 것으로 결정하도록 구성되는 제1 모듈 - 여기서 비밀 식별자는, UE와 적어도 홈 PLMN 사이에서 공유되는 비밀임 -; 및 서빙 PLMN에 비밀 식별자를 통지하도록 구성되는 제2 모듈 - 비밀 식별자는 서빙 PLMN이 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하게 함 - 을 포함한다.

[0015] 제9 양태는, 네트워크 노드의 적어도 하나의 프로세서에 의해 실행될 때, 네트워크 노드로 하여금 상기의 방법들 중 임의의 하나의 방법을 수행하게 하는 명령어들을 포함하는 컴퓨터 프로그램에 관한 것이다.

[0016] 제10 양태는 컴퓨터 프로그램을 포함하는 캐리어에 관한 것이고, 여기서 캐리어는 전기 신호, 광 신호, 무선 신호(radio signal), 또는 컴퓨터 판독가능 저장 매체 중 하나이다.

[0017] 제11 양태는 UE와 연관된 서빙 PLMN에 의해 수행되는 방법에 관한 것이다. 이 방법은, UE가 UE의 홈 PLMN 또는 서빙 PLMN에 의해 성공적으로 인증된 후에 홈 PLMN으로부터, UE를 고유하게 식별하는 비밀 식별자를 수신하는 단계 - 여기서 비밀 식별자는, UE와 UE의 홈 PLMN 사이에서 이전에 공유된 비밀임 -; 및 UE에 관련된 동작을 수행하는 단계를 포함한다.

[0018] 제12 양태는 UE와 연관된 홈 PLMN에 의해 수행되는 방법에 관한 것이다. 이 방법은, UE의 서빙 PLMN에, UE를 고유하게 식별하는 비밀 식별자를 통지하는 것으로 결정하는 단계 - 여기서 비밀 식별자는, UE와 홈 PLMN 사이에서 공유되는 비밀임 -; UE가 홈 PLMN 또는 서빙 PLMN에 의해 성공적으로 인증된 후에 서빙 PLMN에 비밀 식별

자를 통지하는 단계 - 비밀 식별자는 서빙 PLMN이 UE에 관련된 동작을 수행하게 함 - 를 포함한다.

[0019] 제13 양태는 UE와 연관된 서빙 PLMN에 관한 것이다. 여기서 서빙 PLMN은 적어도 2개의 네트워크 노드들을 포함하고, 여기서 제1 네트워크 노드는, UE가 UE의 홈 PLMN 또는 서빙 PLMN에 의해 성공적으로 인증된 후에 홈 PLMN으로부터, UE를 고유하게 식별하는 비밀 식별자를 수신하도록 구성되고, 여기서 비밀 식별자는, UE와 홈 PLMN 사이에서 공유된 비밀이다. 제2 네트워크 노드는 이 서빙 PLMN에서 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하도록 구성된다.

[0020] 비밀 식별자는 상기에 언급된 양태들의 하나 이상의 실시예에서 암호화되지 않은 장기 식별자, 예를 들어, IMSI일 수도 있다.

[0021] UE는 상기에 언급된 양태들의 하나 이상의 실시예에서 서빙 PLMN에 의해 인증될 수도 있다. 그러한 실시예들에서, 비밀 식별자는 홈 PLMN으로부터의 업데이트-위치-응답 메시지에서 홈 PLMN으로부터 전송될 수도 있다.

[0022] 동작은 상기에 언급된 양태들의 하나 이상의 실시예에서 UE에 관련된 합법적 인터셉션 또는 과금 제어일 수도 있다.

도면의 간단한 설명

[0023] 도 1은 본 발명의 예시적인 실시예들에 대응하는 통신 네트워크를 예시한다.

도 2는 하나 이상의 실시예에 따른 서빙 PLMN의 네트워크 노드에 의해 수행되는 방법을 예시한다.

도 3은 하나 이상의 실시예에 따른 홈 PLMN의 네트워크 노드에 의해 수행되는 방법을 예시한다.

도 4는 본 발명의 예시적인 실시예들에서 구현되는 프로세스 및 신호 흐름을 예시한다.

도 5는 본 발명의 예시적인 실시예들에서 구현되는 프로세스 및 신호 흐름을 예시한다.

도 6은 본 발명의 예시적인 실시예들에서 구현되는 프로세스 및 신호 흐름을 예시한다.

도 7은 본 발명의 예시적인 실시예들에서 서빙 PLMN의 예시적인 네트워크 노드의 양태들을 예시한다.

도 8은 본 발명의 예시적인 실시예들에서 홈 PLMN의 예시적인 네트워크 노드의 양태들을 예시한다.

도 9는 서빙 PLMN의 실시예를 예시한다.

발명을 실시하기 위한 구체적인 내용

[0024] 도 1은 UE(102)에 대한 홈 PLMN(114) 및 네트워크 액세스 및 서비스들을 UE(102)에 제공하는 서빙 PLMN(112)을 포함하는 통신 시스템(100)을 예시한다. 도 1에 도시된 바와 같이, 서빙 PLMN(112)은, UE(102)에 관련된 적어도 하나의 동작(108)(수행되는 다른 UE 관련 동작들이 존재할 수도 있지만 도시되지 않는다)을 수행하도록 구성되는 (명시적으로 도시되지 않은 복수의 네트워크 디바이스들 중에서의) 네트워크 노드(106)를 포함한다. 일부 예들에서, UE(102)의 비밀 식별자(110)는 동작(108)이 수행되기 위해 네트워크 노드(106)에(또는 일반적으로는 서빙 PLMN(112)에) 이용가능해야 한다. 그러나, 디폴트로, 이 비밀 식별자(110)는 홈 PLMN(114)과 UE(102)(그리고 잠재적으로는 비밀 식별자(110)가 이전에 통지된 다른 디바이스들 및/또는 네트워크들) 사이의 비밀로서 유지될 수도 있다. 이와 같이, 적어도 일부의 예들에서, 서빙 PLMN(112)은 동작(108)을 수행하기 위한 전제조건으로서 비밀 식별자(110)를 획득하도록 요구될 수도 있다. UE는, 예를 들어, 모바일 폰, 랩톱, 태블릿 및 예를 들어 백색 가전제품(white goods)(예컨대, 냉장고) 또는 차량(예컨대, 자동차 또는 트럭의 대시보드에서의 인포테인먼트 시스템(infotainment system))에서의 임베디드 디바이스일 수도 있다. 네트워크 노드(106)는 예를 들어 액세스 및 이동성 관리 펑션(Access and Mobility Management Function)(AMF), 보안 앵커 펑션(Security Anchor Function)(SEAF), 보안 콘텍스트 관리 펑션(Security Context Management Function)(SCMF), 세션 관리 펑션(Session management Function)(SMF) 및 정책 제어 펑션(Policy Control Function)(PCF)일 수도 있다.

[0025] 본 발명의 피처(feature)에서, 서빙 PLMN(112)의 네트워크 노드(106)는, 예를 들어, 홈 PLMN(114)의 네트워크 노드(116)(또는 임의의 다른 허용된 디바이스)에 의해 전송된 하나 이상의 메시지(101)를 통해, UE(102)의 비밀 식별자(110)를 획득한다. 이 비밀 식별자(110)를 서빙 PLMN(112)에 통지하는 것에 의해, 홈 PLMN(114)은 서빙 PLMN(112)의 네트워크 노드(106)가 동작(108)을 수행하게 한다. 도 1에 도시된 통신 시스템(100) 및 그 내부의 디바이스들 및 네트워크들의 동작, 구조체, 및 피처들의 다른 피처들이 나머지 도면들을 참조하여 아래에 소개

되고 설명될 것이다. 네트워크 노드(116)는 예를 들어 인증 서버 평션(Authentication Server Function)(AUSF), 인증 크리덴셜 리포지토리 및 프로세싱 평션(Authentication Credential Repository and Processing Function)(ARPF), 단일화된 데이터 관리(Unified Data Management)(UDM), AAA-서버(Authentication, Authorization and Accounting server; 인증, 인가 및 어카운팅 서버), 구조화된 데이터 저장 평션(Structured Data Storage Function)(SDSF), 및 비구조화된 데이터 저장 평션(Unstructured Data Storage Function)(UDSF)일 수도 있다.

[0026] 예시적인 실시예들의 추가의 상세한 설명을 진행하기 전에, 특정 PLMN을 지칭하는 임의의 개시내용은 특정 PLMN과 연관된 네트워크 노드를 또한 지칭하는 것으로 이해될 수 있다는 것에 주목해야 한다. 마찬가지로, 특정 네트워크 노드를 지칭하는 임의의 개시내용은 특정 네트워크 노드와 연관된 PLMN을 또한 지칭하는 것으로 이해될 수 있다. 예를 들어, 홈 PLMN(114)에 대응하는 것으로서 또는 그에 의해 수행되는 것으로서 개시되는 임의의 피처는 마찬가지로, 임의로 도 1의 네트워크 노드(116)에 대응하는 것으로서 또는 그에 의해 수행되는 것으로서 이해되어야 한다. 유사하게, 서빙 PLMN(112)에 대응하는 것으로서 또는 그에 의해 수행되는 것으로서 개시되는 임의의 피처는 마찬가지로, 임의로 도 1의 네트워크 노드(106)에 대응하는 것으로서 또는 그에 의해 수행되는 것으로서 이해되어야 한다. 언급된 바와 같이, PLMN에 의해 수행되는 것으로서 설명된 임의의 2개 이상의 피처들 또는 기능성들은 반드시 PLMN에서의 정확히 동일한 디바이스와 연관되는 것으로서 또는 그에 의해 수행되는 것으로서 판독되어서는 안 된다. 그 대신에, 특정 PLMN에 의해 수행되는 것으로서 또는 그와 연관되는 것으로서 개시되거나, 또는 특정 PLMN의 네트워크 노드에 의해 수행되는 것으로서 또는 그와 연관되는 것으로서 개시되는 임의의 2개 이상의 피처들은 임의로 PLMN의 상이한 예시적인 네트워크 노드들과 연관되는 것으로서 또는 이들에 의해 수행되는 것으로서 판독되어야 한다. 이것의 예는 서빙 PLMN의 2개의 네트워크 노드들을 포함하는 장치일 것이고, 여기서 제1 네트워크 노드는 홈 PLMN으로부터 비밀 식별자(110)를 수신한 후에, 비밀 식별자(110)의 지식을 통해, 제2 네트워크 노드가 UE(102)에 관련된 동작을 수행할 수 있게 한다.

[0027] 이 지시문의 예에서, 본 개시내용이 "서빙 PLMN(112)이 그것의 메모리에 공개 식별자를 저장한다"는 것을 명시하는 경우, "네트워크 노드(106)는 네트워크 노드(106)의 메모리에 또는 공개 식별자가 저장될 수도 있는 메모리를 포함하는 서빙 PLMN(112)의 임의의 다른 네트워크 노드 또는 디바이스에 공개 식별자를 저장한다"는 것을 마찬가지로 개시하는 것으로 또한 이해되어야 한다. 게다가, 본 개시내용이 "서빙 PLMN(112)이 공개 식별자를 암호화된 비밀 식별자와 비교한다"는 것을 부가적으로 명시하는 경우, "공개 식별자 및 암호화된 비밀 식별자의 비교는 상기의 공개 식별자를 저장한 동일한 네트워크 노드(106)에서, 또는 그러한 비교를 수행하는 것으로서 이해될 수 있는 서빙 PLMN의 (공개 식별자가 메모리에 저장된 특정 네트워크 노드 이외의) 임의의 다른 네트워크 노드에서 수행될 수도 있다"는 것을 마찬가지로 개시하는 것으로 이해되어야 한다. 다시 말해, 홈 및 서빙 PLMN들은 복수의 네트워크 노드들을 임의로 포함하는 것으로서 이해되어야 하는데, 이들 중 하나 이상은 PLMN에 또는 그것의 네트워크 노드에 기인하는 개시된 평션들 또는 피처들을 수행할 수 있다.

[0028] 도 2는 서빙 PLMN(112)에 의해 서빙되는 UE(102)의 비밀 식별자(110)의 지식(또는 그 비밀 식별자(110)로의 액세스)을 요구하는 동작(108)을 수행하기 위해 서빙 PLMN(112)의 네트워크 노드(106)에 의해 수행되는 예시적인 방법(200)을 예시한다. 일부 예들에서, 요구되는 비밀 식별자(110)는 UE 자체를 식별할 수도 있지만, 그것은 UE에 대응하는 특정 사용자 또는 가입자 어카운트와 부가적으로 또는 대안적으로 연관될 수도 있고, 여기서 가입자 어카운트는 특정 인증 크리덴셜들, 과금 어카운트 또는 레코드들, 토큰링 및 액세스 정책들(tokening and access policies), 하나 이상의 서비스에 대한 QoS 또는 가입자 레벨을 포함하는 서비스 파라미터들 등을 가질 수도 있고, 이들 각각은 UE(102)의 홈 PLMN(114)에서 확립 및/또는 유지될 수도 있다. 이에 따라, 본 개시내용의 목적들을 위해, 사용자 장비라는 용어는 특정 디바이스를 지칭할 뿐만 아니라, 연관된 홈 PLMN을 갖는 가입자 또는 사용자를 또한 지칭할 수도 있다. 다시 말해, UE(102)를 고유하게 식별하는 국제 모바일 가입자 아이덴티티(IMSI)의 형태의 비밀 식별자(110)는 UE보다는 오히려 홈 PLMN(114)에 대한 가입자/사용자를 고유하게 식별한다고 유사하게 말할 수 있는데, 이는 IMSI가 UE를 형성하기 위해 모바일 장비(Mobile Equipment)(ME)에 연결된 범용 집적 회로 카드(Universal Integrated Circuit Card)(UICC)/가입자 아이덴티티 모듈(Subscriber Identity Module)(SIM) 카드에 전형적으로 저장되고, SIM 카드는 다른 ME로 스위칭될 수 있기 때문이다. 이와 같이, UE(102)를 고유하게 식별한다는 것은, IMSI가 홈 PLMN에 포함 또는 연결된 데이터베이스에서의 홈 PLMN의 특정 가입자와 연관된다는 것을 의미할 것이다. 적어도 일부의 현재 4G 시스템들과 같은 일부 시스템들에서의 IMSI가 실제로, UE 자체뿐만 아니라 가입자를 식별하는 데 사용된다는 것은 통상의 기술자에게 물론 또한 알려져 있다.

[0029] "고유한" 그리고 "고유하게"라는 단어들은 물론 본 발명의 맥락에서 보여질 것이다. 냉철한 관점에서, 예를 들

어 홈 PLMN에 관련된 데이터베이스들의 클러스터에서 또는 하나의 데이터베이스에서 고유한, 2진수와 같은, 예를 들어 특정 수는, 완전히 상이한 가입자 또는 UE에 대해 어딘가 다른 곳에서, 예컨대 완전히 상이한 컴퓨터 네트워크에서 또는 개인적인 리스트에서 발견될 수 없다는 것이 아마도 지금까지 보증된 적이 없을 수 없다.

[0030] 부가적으로, 비밀 식별자(110)는, 본 출원의 목적들을 위해, 가입의 유효한 지속기간 전체에 대해 변경을 요구하는 정상 참작이 가능한 상황들이 없다면 변경되지 않은 채로 유지되어야 한다는 전제, 이해, 및 의도에 기초하여 확립되는 정적 세트의 영숫자 문자들(또는 대응하는 디지털 비트 값들)에 대응하는 "장기" 식별자일 수도 있다. 비밀 식별자(110)는, IMSI 및/또는 그 IMSI를 구성하는 하나 이상의 값, 예컨대 모바일 가입 식별 번호(MSIN), 모바일 네트워크 코드(MNC), 및/또는 모바일 국가 코드(MCC)와 같은, 그러나 이에 제한되지 않는, 장기 식별자일 수도 있다. 대안적으로 또는 부가적으로, 비밀 식별자(110)는 국제 모바일 장비 아이덴티티(IMEI), 인터넷 프로토콜(IP) 어드레스 등과 같은 장기 식별자, 또는 전역 고유 임시 아이덴티티(Globally Unique Temporary Identity)(GUTI), 셀 무선 네트워크 임시 아이덴티티(Cell Radio Network Temporary Identity)(C-RNTI)와 같은 단기 식별자, 또는 개인적으로 유지되거나 또는 개인적으로 이루어질 수 있거나 또는 그렇지 않으면 제한된 세트의 디바이스들 사이의 비밀로서 유지될 수 있는 임의의 유사한 알려진 식별자를 포함할 수도 있다. 장기 식별자로서의 IP 어드레스에 관련하여, 정적 IP 어드레스는 명백히 그러한 예이지만, 유스 케이스에 따라 또한 동적 호스트 구성 프로토콜 서버에 의해 할당된 IP 어드레스가 장기 식별자일 수도 있다. 다른 상황들에서, 동적으로 할당된 IP 어드레스가 단기 식별자로서 간주된다. 본 기술분야의 통상의 기술자에 의해 이해되는 바와 같은 장기 식별자는 반드시 영구 식별자일 필요는 없다. 영구/장기 식별자는 때때로 5세대(5G) 논의들에서 가입자 영구 식별자(Subscriber Permanent Identifier)(SUPI)라고 불린다.

[0031] 방법(200)으로 리턴하면, 블록 202에서, 네트워크 노드(106)는 UE를 고유하게 식별하는 비밀 식별자(110)를 획득한다. 상기에 논의된 바와 같이, 비밀 식별자(110)는, UE와 적어도 UE의 홈 PLMN 사이에서 공유되고 홈 PLMN에 의해 네트워크 노드(106)에 전송되는 비밀이다(즉, 제한된 개별적인 세트의 네트워크들 및 디바이스들에 의해 개인적으로 홀딩된다).

[0032] 게다가, 방법(200)의 블록 204에서, 네트워크 노드(106)는 UE(102)에 관련된 동작(108)을 수행하고, 획득된 비밀 식별자(110)를 사용하여 그와 같이 행한다. 모든 동작들이 아니라 네트워크 노드 또는 서빙 PLMN에 의해 수행되는 UE 관련 동작들은 비밀 식별자(110)가 알려질 것을 요구하지만, 일부 동작들(일부가 법에 의해 요구되는 것을 포함함)은 실행 전에 비밀 식별자(110)를 요구한다(또는 임의로 활용할 수 있다). 예를 들어, 동작(108)은 UE의 합법적 인터셉션에 관련된 동작일 수도 있다. 그에 따라, UE(102)의 비밀 식별자(110)를 알고 있는 서빙 PLMN은 홈 PLMN의 보조 또는 가시성(visibility) 없이 합법적 인터셉션을 지원할 수 있다. 다른 예들에서, 동작(108)은, 특정 PLMN에 의해 이전에 서빙되었던 하나 이상의 UE를 인식하고 이들 UE들을 서빙 PLMN에 연결하기 위한 하나 이상의 인센티브(또는, 임의적인 재선택 또는 핸드오버가 임박한 경우, 서빙 PLMN에 연결된 채로 유지하기 위한 인센티브)를 제공하기 위한 동작과 같은, 본질적으로 경제학적이거나 또는 마케팅일 수도 있다. 또 다른 예들에서, 동작은 UE(또는 사용자/가입자)와 연관된 하나 이상의 서비스 품질 파라미터를 설정 또는 수정하는 것과 같은 특정 UE-특정 동작 서비스 파라미터들 또는 보증들에 관련될 수도 있다. 동작은 UE(102)와 연관된 정책 및/또는 과금 제어에 대안적으로 관련될 수 있다. 이들 몇몇 예들은 UE 또는 네트워크 가입자의 비밀 식별자(110)를 활용할 수도 있는 일부 예시적인 동작들의 제한된 모습을 제공하지만, 서빙 PLMN에 의해 비밀 식별자를 획득하거나 또는 홈 PLMN에 의해 비밀 식별자를 통지하는 피처는 단일-UE 입상도(single-UE granularity)로 적용될 수도 있는 임의의 동작 또는 프로세스로 확장될 수 있다.

[0033] 블록들 202 및 204의 피처들에 부가적으로, 방법(200)은, 도 2에 명시적으로 도시되지 않은 부가적인 또는 대안적인 양태들을 포함할 수도 있다. 예를 들어, 서빙 PLMN(112)의 네트워크 노드(106)는, UE로부터, UE에 대응하는 가명 및/또는 공개 식별자(즉, UE와 연관된, 비밀이 아닌 또는 암호화되지 않은 식별자)를 수신할 수도 있다. 공개 식별자 및/또는 가명을 수신한 후에, 네트워크 노드(106)는 공개 식별자 및/또는 가명을 UE의 홈 PLMN(114)에 포워딩할 수도 있다. 홈 PLMN에 전송된 공개 식별자 및/또는 가명은 홈 PLMN(114)이 비밀 식별자(110)를 서빙 PLMN(112)에(예를 들어, 네트워크 노드(106)에) 통지하라는 암시적인 요청으로서 기능할 수도 있거나, 또는 네트워크 노드(106)는 비밀 식별자(110)에 대한 명시적인 요청을 생성하고 그 명시적인 요청을 포워딩된 공개 식별자 및/또는 가명과 함께 홈 PLMN(114)에 전송할 수도 있다. 이와 같이, 블록 202에서 비밀 식별자를 획득하는 것은 UE(102)에 대응하는 공개 식별자 및/또는 가명의 포워딩에 응답할 수도 있다.

[0034] 아래에 추가로 논의되는 바와 같이, 서빙 PLMN 및/또는 홈 PLMN(114)의 네트워크 노드들은, 비밀 식별자(110)를 획득하도록 인가되지 않은 제3자에 의한 악의적인 요청에 응답하여 비밀 식별자(110)가 통지되지 않는다는 것을 보장하는 것을 돕기 위해 인증을 수행할 수도 있다. 이와 같이, 일부 예들에서, 네트워크 노드(106)는 UE가 홈

PLMN(및/또는 서빙 PLMN, 아래 참조)에 의해 성공적으로 인증된 후에만 단지 비밀 식별자(110)를 수신할 수도 있다. 그에 따라, 홈 PLMN에서 인증이 성공하지 못한 경우, 홈 PLMN(114)은 (예를 들어, 실패 메시지를 통해) 인증이 실패하였음을 서빙 PLMN에게 알릴 수도 있거나 또는 비밀 식별자를 서빙 PLMN에 단순히 통지하지 않을 수도 있는데, 이는 일부 예들에서 인증 실패의 암시적인 표시로서 기능할 수 있다. 그러나, 비밀 식별자(101)가 홈 PLMN에 의해 서빙 PLMN에 전송될 때(예를 들어, 일부 예들에서, 서빙 PLMN 인증 성공의 확인 또는 홈 PLMN UE 인증 후에), 그것은 홈 PLMN(114)으로부터의 확장가능 인증 프로토콜(Extensible Authentication Protocol)(EAP) 메시지를 통해 서빙 PLMN(112)에 통신될 수도 있다.

[0035] 상기에 소개된 바와 같이, UE(102)의 인증은 서빙 PLMN(112)의 네트워크 노드들(106)에 의해 또한 수행될 수도 있다. 이 인증을 수행하기 위해, 네트워크 노드(106)는 (인증을 위해 목표로 하는 UE의 식별을 위한) UE(102)의 공개 식별자 및/또는 가명, 및 네트워크 노드(106)에서 인증 프로시저를 수행하는 데 필요한 규칙들 및/또는 프로세스들을 포함하는 인증 정보를 요구할 수도 있다. 그에 따라, 방법(200)은, 일부 예들에서, UE 자체로부터(또는 이 정보를 소유하는 다른 디바이스로부터) UE(102)의 공개 식별자 및/또는 가명을 획득하고 홈 PLMN(114)으로부터(예를 들어, 네트워크 노드(116)로부터) 인증 정보를 수신하는 단계를 포함할 수도 있다. 양태에서, 인증 정보는, 진화된 패킷 시스템-인증 및 키 합의(Evolved Packet System-Authentication and Key Agreement)(EPS-AKA) 포맷으로 형성되는 하나 이상의 메시지에서 홈 PLMN에 의해 서빙 PLMN에 통신되고, 하나 이상의 통신된 메시지에 포함되는 인증 벡터를 통해 통신된다.

[0036] 일단 공개 식별자 및/또는 가명 및 인증 정보가 네트워크 노드(106)에 의해 또는 서빙 PLMN(112)에 의해 획득/수신된다면, 일반적으로, 네트워크 노드(106)는 인증 동작들을 수행하여 UE가 인증되는지 여부를(즉, UE(102)가 진실로 홈 PLMN(114)의 가입자이거나 또는 그렇지 않으면 서빙 PLMN(112)에 비밀 식별자(110)를 통지하도록 홈 PLMN(114)을 프롬프트하도록 허용된다는 것을) 결정한다. 인증 동작들이 성공적인 경우(예를 들어, 동작들이 UE(102)(또는 그로부터의 요청)가 진본이라고(즉, UE(102)가 홈 PLMN(114)에 대해 검증된 가입자라고) 결정하는 경우), 네트워크 노드(106)는 인증 성공 메시지를 홈 PLMN에 통신하여 UE가 서빙 PLMN에 의해 성공적으로 인증되었음을 홈 PLMN에게 알릴 수도 있다. 부가적으로, 홈 PLMN(114)에서 수신 및 프로세싱될 때, 인증 성공 메시지는 비밀 식별자(110)를 서빙 PLMN에 전송하도록 홈 PLMN을 트리거할 수 있다.

[0037] 상술된 예에서, 서빙 PLMN(112)은 UE(102)가 서빙 PLMN에 의해 또는 홈 PLMN에 의해 인증된 후에 홈 PLMN으로부터 비밀 식별자(110)를 수신한다. 이들 실시예들에서, 네트워크 노드(106)는 UE(102)의 인증이 성공한 후에 홈 PLMN으로부터 생성 및 전송되는 인증-정보-응답(authentication-information-answer)(AIA) 메시지를 통해(예를 들어, 다이어미터(Diameter) 인증, 인가, 및 어카운팅(AAA) 프로토콜에 따라) 홈 PLMN으로부터 비밀 식별자를 수신할 수도 있다. 홈 PLMN이 비밀 식별자(110)를 서빙 PLMN에 전송하기 전에 인증을 수행하는 것이 방법(200)에 대해 부가된 보안 레벨을 제공할 수 있지만, 그것은 모든 실시예들에 대한 요건이 아니다. 이에 따라, 일부 실시예들에서, UE(102)가 서빙 PLMN(112) 또는 홈 PLMN(112)에 의해 인증되기 전에 서빙 PLMN은 (예를 들어, 네트워크 노드(106)를 통해) 홈 PLMN(114)으로부터 비밀 식별자(110)를 수신할 수도 있다. 이들 대안적인 실시예들에서, 비밀 식별자는 UE(102)의 인증이 서빙 PLMN 또는 홈 PLMN 중 어느 하나에서 성공하기 전에 홈 PLMN으로부터 생성 및 전송되는 업데이트-위치-응답(update-location-answer)(ULA) 메시지를 통해(예를 들어, 다이어미터 인증, 인가, 및 어카운팅(AAA) 프로토콜에 따라) 전송될 수도 있다.

[0038] 방법(200)의 일부 실시예들의 부가적인 양태에서, 비밀 식별자(110)의 비인가된 보급을 회피하고 홈 PLMN에 의해 전송된 비밀 식별자가 진품인지를 체크하기 위한 추가의 보안 조치로서, 서빙 PLMN(112)이 (예를 들어, 네트워크 노드(106)를 통해) 공개 식별자 및 획득된 비밀 식별자(101)가 동일한 UE에 대응한다는 것을 검증할 수도 있다. 이 검증 프로시저가 네트워크 노드(106)에 의해(또는 일반적으로는 서빙 PLMN(112)에 의해) 수행되는 것으로서 본 개시내용에 의해 주로 설명되지만, 이것은 제한적인 피처가 아니다. 그 대신에, 검증은 홈 PLMN(114)에서 그리고/또는 도 1에 도시되지 않은 다른 디바이스 또는 네트워크(예를 들어, 전용 보안 시스템 또는 예를 들어 AAA 서비스)에 의해 대안적으로 또는 부가적으로 수행될 수 있다.

[0039] 그러나, 서빙 PLMN(112)에서 수행될 때, 검증 프로시저는 방법(200)을 실행함에 있어서 네트워크 노드(106)에 의해 수행될 수 있는 상술된 그룹의 피처들을 확장시킬 수도 있다. 예를 들어, 홈 PLMN의 공개 키에 기초하여 비대칭 암호화 스킴을 사용하는 것 - 그 공개 키는 UE 및 홈 PLMN 양측 모두에 알려져 있음 - 은 검증의 일 실시예에서 다음과 같은 것일 수도 있다. 검증은, 네트워크 노드(106)가, 예를 들어, 홈 PLMN(114)으로부터, 비밀 식별자(110)를 암호화하기 위한 암호화 정보를 획득하는 것을 포함한다. 이 암호화 정보는, 비밀 식별자(110)를 UE의 공개된 암호화된 식별자로 암호화하는 데 사용될 수 있는 홈 PLMN(114)의 공개 키를 포함한다. 상기에 언급된 바와 같이, 이 공개 식별자는 UE(102)로부터 네트워크 노드(106)(또는 일반적으로는 서빙

PLMN(112))에 의해 초기에 획득될 수도 있는데, 즉, UE는 그것의 IMSI를 홈 PLMN의 공개 키로 암호화하는 것에 의해 공개 식별자를 이전에 생성하였고 이 공개 식별자(즉, 홈 PLMN의 공개 키로 암호화된 IMSI)를 네트워크 노드(106)에 전송할 수도 있다. 일단 네트워크 노드(106)에 의해 획득된다면, 암호화 정보는 획득된 비밀 식별자(110)를 홈 PLMN의 공개 키로 암호화하는 것에 의해 암호화된 비밀 식별자를 생성하도록 네트워크 노드(106)에 의해 활용될 수 있다. 이제, 네트워크 노드(106)는 결과적인 암호화된 비밀 식별자 및 UE로부터 수신되는 이전에 수신된(그리고 저장된) 공개 식별자를 비교하는 것으로 진행할 수도 있다. 이 비교는 암호화된 비밀 식별자 및 공개 식별자가 매칭한다는 네트워크 노드(106)에 의한 결과를 발생시킬 수도 있다. 그러한 매치는 검증이 성공하였음을 표시할 수도 있다. 양태에서, "매치"를 정의하는 기준들은 사용자에 의해 또는 홈 PLMN 또는 서빙 PLMN에 의해 미리 구성될 수도 있다. 매치가 존재한다는 것을 결정하기 위한 이들 기준들은 정확한 비트-레벨 매치를 요구하는 것으로부터 또는 미리 정의된 검증 임계 기준을 충족시키는 퍼센티지, 비율, 또는 원시 수(raw number)의 매칭 비트들을 정의하는 것에 의해 원하는 레벨의 정밀도로 조정될 수도 있다. 검증 성공을 정의하기 위한 특정한 구현된 기준들에 관계없이, 기준들이 충족되는 경우, 네트워크 노드(106)는 암호화된 비밀 식별자 및 공개 식별자가 매칭한다고 결정하는 것에 기초하여 공개 식별자 및 비밀 식별자가 동일한 UE에 대응한다는 것을 검증할 수 있다. 그 결과, 통지된 비밀 식별자(110)와 "매칭"하지 않는 공개 식별자를 갖는 비인가된 UE들로부터의 요청들은 비인가된 당사자들에 대한 비밀 식별자(110)의 보급을 제한하기 위해 효과적으로 발견 및 교정될 수 있다. 다시 말해, 합법적 인터셉션과 같은 동작은 UE 및 홈 PLMN이 서빙 PLMN을 속이고 있지 않다고 결정하는 것에 의해 더 신뢰성있게 된다.

[0040] 검증의 제1 대안적인 실시예에서, 타원 곡선 통합 암호화 스킴(Elliptic Curve Integrated Encryption Scheme)(ECIES)이 사용된다. 상술된 실시예와 유사하게, 홈 PLMN의 공개 키는 UE(102) 및 홈 PLMN(114)에 알려져 있지만, 여기서 UE(102)는 또한 그 자신의(즉, UE(102)의) 쌍의 공개 및 개인 키들을 갖는다. UE(102)는 그 자신의 개인 키 및 홈 PLMN(114)의 공개 키에 기초하여 제1 대칭 암호화 키를 생성한다. 그 후에, 공개 식별자는 비밀 식별자(예를 들어, IMSI)를 제1 대칭 암호화 키로 암호화하는 것에 의해 UE(102)에 의해 생성된다. UE(102)의 공개 키 및 공개 식별자는 서빙 PLMN(112)에 전송되는데, 이 서빙 PLMN(112)은 이들을 수신하고 또한 이들을 홈 PLMN(114)에 포워딩한다. 그 후에, 서빙 PLMN에 비밀 식별자를 전송하는 것에 부가적으로, 홈 PLMN은 UE(102)의 수신된 공개 키 및 홈 PLMN의 개인 키를 사용하여 홈 PLMN에 의해 생성되는 제2 대칭 암호화 키의 형태로 암호화 정보를 또한 생성 및 전송한다. 이제, 서빙 PLMN(112)은 홈 PLMN(114)으로부터 수신된 비밀 식별자를 제2 대칭 암호화 키로 암호화한 후에, 암호화된 비밀 식별자를 공개 식별자와 비교하는 것에 의해 검증을 수행할 수도 있다. 디피-헬만(Diffie-Hellman)과 같은 키 교환 알고리즘들에 의해 제공되는 암호화 속성들로 인해 제2 대칭 키가 제1 대칭 키와 동일하다는 사실로 인해 매치가 가능해진다.

[0041] 검증의 제2 대안적인 실시예는 제1 대안적인 실시예와 유사하지만, 수신된 비밀 식별자를 제2 대칭 암호화 키로 암호화하는 대신에, 서빙 HPLMN은 공개 식별자를 제2 대칭 암호화 키로 암호화해제하고, 암호화해제된 공개 식별자를 비밀 식별자와 비교한다. 도 3은, 이종 서빙 PLMN(112)에, 서빙 PLMN(112)에 의해 서빙되는 UE(102)의 비밀 식별자(110)를 통지하기 위해 홈 PLMN(114)의 네트워크 노드(116)에 의해 수행되는 예시적인 방법(300)을 예시한다. 예시적인 방법(300)에 따르면, 블록 302에서, 네트워크 노드(116)는, UE(102)의 서빙 PLMN(112)에, UE(102)를 고유하게 식별하는 비밀 식별자(110)를 통지하는 것으로 결정한다. 상술된 바와 같이, 이 비밀 식별자(110)는, UE(102)와 적어도 홈 PLMN(114) 사이에서 공유되는 비밀이다. 부가적으로, 예시적인 방법(300)은, 네트워크 노드(116)가 서빙 PLMN에 비밀 식별자를 통지하는 단계를 포함한다. 일부 비제한적인 예들에서, 서빙 PLMN에 비밀 식별자를 통지하는 단계는, 비밀 식별자(110)를 포함하는 EAP 메시지를 서빙 PLMN에 전송하는 단계를 포함할 수 있다. 서빙 PLMN(112)에 비밀 식별자(110)를 전송하기 위해 활용되는 특정 메시지 포맷에 관계없이, 서빙 PLMN(112)은 통지된 비밀 식별자(110)를 사용하여 UE(102)에 관련된 동작(108)을 수행할 수 있다.

[0042] 도 3에 명시적으로 도시되지 않았지만, 방법(300)은 추가의 양태들을 임의로 포함할 수 있는데, 이들 중 일부는 서빙 PLMN(112)측에서 수행되는 방법(200)을 참조하여 상기에 소개되었다. 예를 들어, 네트워크 노드(116)는 방법(300)의 임의적인 부가적 양태로서 UE(102)의 인증을 수행할 수 있다. 홈 PLMN에서 인증이 행해질 때, UE는 서빙 PLMN에 존재한다는 것이 보증된다. 이 인증을 수행함에 있어서, 네트워크 노드(116)는, 예를 들어, UE(102)의 공개 식별자 및/또는 가명을 수신할 수 있는데, 이 공개 식별자 및/또는 가명은, 예를 들어, (예를 들어, 홈 PLMN(114)이 비밀 식별자(110)를 통지하라는 그리고/또는 UE(102)를 검증하라는 명시적인 또는 암시적인 요청 시에) 서빙 PLMN에 의해 홈 PLMN(114)에 포워딩될 수도 있거나 또는 이전 인증으로부터 홈 PLMN에 저장될 수도 있다. 인증 프로시저의 실행 시에, 네트워크 노드(116)는 공개 식별자 및/또는 가명에 기초하여 UE(102)가 성공적으로 인증되었다는 것을 결정할 수 있다. 일부 구현들에서, 서빙 PLMN(112)에 비밀 식별자를 통지하기 위한 네트워크 노드(116)에 의한 결정은 UE(102)의 성공적인 인증을 요구한다. 그러나, 일부 예들에

서, 비인가된 당사자들에 대한 비밀 식별자(110)의 보급의 연관된 증가된 리스크에도 불구하고, 그러한 앞선 인증 성공은 특정 서빙 PLMN(112)에 비밀 식별자(110)를 통지할 필요가 없다.

[0043] 서빙 PLMN이 인증 프로시저를 수행하는 특정 실시예들에서, 홈 PLMN(114)은 인증 정보를 서빙 PLMN(112)에 통신할 수 있는데, 이 인증 정보는 UE(102)의 독립적인 인증을 수행하기 위해 (예를 들어, 네트워크 노드(106)에서) 서빙 PLMN(112)에 의해 활용된다. 인증 정보는 EPS-AKA 포맷으로 형성될 수 있고, 인증 벡터를 통해 서빙 PLMN(112)에 통신될 수도 있다. 부가적으로, 일부 예들에서, 네트워크 노드(116)는 UE(102)가 서빙 PLMN(112)에 의해 성공적으로 인증되었음을 홈 PLMN(114)에게 알리는 인증 성공 메시지를 서빙 PLMN(112)으로부터 수신할 수도 있다. 인증 성공 메시지를 수신하면 일부 경우들에서 서빙 PLMN(112)에 비밀 식별자를 통지하도록 홈 PLMN(114)을 트리거할 수 있다. 비밀 식별자(110)를 통지하는 것은, 네트워크 노드(116)가 ULA 메시지를 통해 서빙 PLMN에 비밀 식별자(110)를 전송하는 것을 포함할 수도 있다. 그러나, 다른 예시적인 구현들에서, 앞선 UE 인증이 위임되지 않고, 이와 같이, 네트워크 노드(116)는 UE가 (예를 들어, 서빙 PLMN 또는 홈 PLMN(114)에 의해) 인증되기 전에 비밀 식별자(110)를 서빙 PLMN(112)에 전송하는 것에 의해 그 비밀 식별자(110)를 임의로 통지할 수 있다. 이들 예들에서, 네트워크 노드(116)는 (예를 들어, AIA 메시지를 통해) UE(102)가 서빙 PLMN에 의해 인증된 후에 서빙 PLMN(112)에 비밀 식별자(110)를 전송할 수 있다. 서빙 PLMN에서 인증이 행해질 때, UE가 서빙 PLMN에 존재한다는 것이 아마도 보증되지 않지만, 서빙 PLMN은 여전히 책임을 질 수 있다.

[0044] 도 4, 도 5, 및 도 6은 UE(102)의 서빙 PLMN(112)에 UE(102)의 비밀 식별자(110)를 통지하기 위한 상이한 예시적인 실시예들에 대한 상이한 예시적인 프로세스 및 신호 흐름들을 제시한다. 도 4, 도 5, 및 도 6에 예시된 예시적인 실시예들은 모든 가능한 실시예들의 배타적인 세트이도록 결코 의도된 것이 아니다. 그 대신에, 이들 예시된 예시적인 실시예들은 본 개시내용에 의해 고려되는 가능한 실시예들의 서브세트를 나타낸다.

[0045] 이들 예시된 예시적인 실시예들을 참조하면, 도 4는 서빙 PLMN(112)에 비밀 식별자(110)를 통지하기 전에 UE(102)의 인증이 요구되고 공개(즉, 비밀이 아닌) 식별자(예컨대, UE(102)의 가명 또는 암호화된 장기 식별자)를 사용하여 홈 PLMN에서 인증이 수행되게 하는 예시적인 구현을 예시한다. 도 4에 도시된 바와 같이, 서빙 PLMN은 UE의 개인 식별자가 실행을 위한 전제조건인 UE에 관련된 동작을 수행할 필요성을 결정하는 것에 의해 프로세스를 개시할 수도 있다. 이 결정에 기초하여, 서빙 PLMN(112)은 UE의 공개 식별자(일부 예들에서, 서빙 PLMN에 의해 이미 알려져 있지 않은 경우)에 대한 요청을 UE(102)에 전송한다. 그 요청에 응답하여, UE(102)는 이 공개 식별자를 서빙 PLMN(112)에 전송하고, 공개 식별자를 수신한 후에, 서빙 PLMN(112)은 공개 식별자를 홈 PLMN(114)에 포워딩한다. 공개 식별자를 홈 PLMN(114)에 포워딩하는 것에 의해, 서빙 PLMN(112)은 홈 PLMN(114)이 UE(112)의 비밀 식별자(110)를 통지하라고 서빙 PLMN(112)이 요청함을 홈 PLMN(114)에게 암묵적으로 표시할 수 있다. 대안적인 예들에서, 서빙 PLMN(112)은 홈 PLMN(114)이 UE(112)의 비밀 식별자(110)를 통지하라는 별개의 명시적인 요청을 홈 PLMN(114)에 전송할 수도 있다.

[0046] 도 4의 예시적인 실시예에서, 공개 식별자를 수신한 후에, 홈 PLMN(114)은 인증 동작들을 수행하고, 인증이 성공적이라고 결정한다. 이 성공적인 인증은 UE(102)가 서빙 PLMN(112)에 실제로 존재함(예를 들어, 서빙 PLMN(112)에 의해 현재 서빙되고 있음)을 표시한다. 이 성공적인 인증에 기초하여, 홈 PLMN(114)은 서빙 PLMN(112)에 UE(102)의 비밀 식별자를 통지하는 것으로 결정을 행하고, 서빙 PLMN(112)에 비밀 식별자를 통지하는 것으로 진행한다. 이것은 비밀 식별자를 전용 메시지에서 전송하는 것에 의해 또는 서빙 PLMN에 전송될 스케줄링된 또는 큐잉된(그리고/또는 장래의) 메시지들에 비밀 식별자 데이터를 피기백하는 것에 의해 달성될 수 있다. 비밀 식별자를 수신한 후에, 서빙 PLMN(112)은 UE에 관련된 동작을 수행한다.

[0047] 도 5는 UE 검증 프로시저가 서빙 PLMN(112)에 의해 수행되게 하는 다른 예시적인 구현을 예시한다. 다시 도 5의 예시적인 실시예에서, UE(102)의 인증은 서빙 PLMN(112)에 비밀 식별자(110)를 통지하기 전에 요구되고 여기서 인증은 공개 식별자를 사용하여 홈 PLMN에서 수행된다. 가독성을 보장하기 위해, UE 관련 동작을 수행할 필요성을 결정하고 UE로부터 공개 식별자를 요청하고 서빙 PLMN이 동작을 수행하는 초기 단계들은 도 5에 도시되지 않지만, 이들 피처들은 이 예시적인 구현에 임의로 포함된다.

[0048] 도시된 바와 같이, 일단 요청된 공개 식별자(예를 들어, 홈 PLMN(114)의 공개 키로 암호화된 UE(102)의 IMSI)가 UE(102)에 의해 리턴된다면, 서빙 PLMN은 공개 식별자를 메모리에(예를 들어, 하나 이상의 네트워크 노드의 메모리에) 저장한 후에, 공개 식별자를 홈 PLMN(114)에 포워딩하는데, 이 공개 식별자는 인증을 수행하도록 홈 PLMN(114)을 다시 트리거한다. 인증이 성공적일 때, 홈 PLMN(114)은 서빙 PLMN(112)에 비밀 식별자를 통지하는 것으로 결정한다. 게다가, 홈 PLMN(114)은, 암호화 정보(즉, 홈 PLMN(114) 및 그 홈 PLMN(114)이 암호화 정보 액세스를 허용하는 임의의 다른 디바이스들에 의해서만 단지 유지될 수도 있는 비밀)가 개인적이기 때문에, 비

밀 식별자와 함께 암호화 정보를 서빙 PLMN(112)에 전송할 수도 있다. 암호화 정보는, 홈 PLMN(114)과 연관된 공개 키를 포함할 수도 있다. 대안적인 구현들에서, 암호화 정보는 홈 PLMN(114)이 비밀 식별자를 전송하기 전에(또는 후에) 전송될 수도 있고, 별개의 프로세스 반복 동안 암호화 정보가 서빙 PLMN(112)에 의해 이전에 획득된 다른 예들에서는, 후속 프로세스 반복들을 위해 전혀 전송되지 않을 수도 있다.

[0049] 홈 PLMN(114)으로부터의 비밀 식별자 및 암호화 정보의 수신 시에, 서빙 PLMN(112)은 검증 동작을 수행하는데, 이 검증 동작은 통지된 비밀 식별자가 대응하는 UE(102)와는 상이한 UE에 공개 식별자가 대응하지 않는다는 것을 보장하는 것을 도울 수 있다. 이전 도면들을 참조하여 설명된 바와 같이, 이 검증은, 암호화 정보를 활용하여 비밀 식별자의 암호화된 버전을 생성하는 것을 포함할 수도 있는 수 개의 단계들을 수반할 수 있다. 일단 암호화된 비밀 식별자가 생성된다면, 서빙 PLMN은 그것을 저장된 공개 식별자와 비교할 수도 있다. 비교가 공개 식별자 및 암호화된 비밀 식별자가 매칭한다고(예를 들어, 매치를 정의하는 특정 정적 또는 변경가능 기준들을 충족한다고) 통지하는 경우, 검증 프로시저는 공개 식별자 및 비밀 식별자가 홈 PLMN(114)의 인증된 가입자인 단일 UE에 대응한다고 결정함에 있어서 성공적일 수도 있다. 다시, 도 5에 명시적으로 도시되지 않았지만, 서빙 PLMN은 검증 후에 UE에 관련된 동작을 수행할 수도 있다.

[0050] 도 6은 UE 인증 프로시저가 서빙 PLMN(112)에 의해 수행되게 하는 다른 예시적인 구현을 예시한다. 또한, 도 6의 서빙 PLMN(112)은 도 5에 관련하여 상기에 약술되는 UE 검증 프로시저를 수행한다. 도 4 및 도 5에서 진행되는 실시예들과는 달리, 도 6의 예시적인 실시예에서, 서빙 PLMN(112)에 비밀 식별자(110)를 통지하기 전에 UE(102)의 인증은 임의적인 것이다. 이와 같이, 홈 PLMN(114)은 UE의 임의의 인증이 수행되기 전에(여기서, 인증이 서빙 PLMN(112)에서 수행되기 전에) 서빙 PLMN(112)에 비밀 식별자를 통지할 수도 있다. 대안적으로, 홈 PLMN(114)은 서빙 PLMN(112)에 비밀 식별자를 전송하는 것으로 결정을 행하기 전에 UE가 성공적으로 인증되었다는 확인을 서빙 PLMN(112)으로부터 요구하도록 구성될 수도 있다. 이들 옵션들 양측 모두가 도 6의 프로세스 및 신호 흐름에 예시되어 있고, 이들 옵션들과 연관된 신호들은 파선의 신호 라인들에 의해 임의적인 것으로서 표시된다(이는 "다른" 옵션이 매 경우마다 구현될 수도 있기 때문이다).

[0051] 다시 가독성을 보장하기 위해, UE 관련 동작을 수행할 필요성을 결정하고 UE로부터 공개 식별자를 요청하고 서빙 PLMN이 동작을 수행하는 초기 단계들은 도 6에 도시되지 않지만, 이들 피처들은 이 예시적인 구현에 임의로 포함된다.

[0052] 도 6의 프로세스 및 신호 흐름의 상단에 예시된 바와 같이, 일단 요청된 공개 식별자가 UE(102)에 의해 서빙 PLMN(112)에 전송된다면, 서빙 PLMN(112)은 공개 식별자를 메모리에(예를 들어, 하나 이상의 네트워크 노드의 메모리에) 저장한 후에 공개 식별자를 홈 PLMN(114)에 포워딩한다. 그러나, 도 4 및 도 5에서와 같이 홈 PLMN(114)에 의해 인증을 트리거하기보다는 오히려, 공개 식별자를 수신하면 서빙 PLMN(112)에 UE 인증에 필요한 인증 정보를 전송하도록 홈 PLMN(114)을 트리거한다. 게다가, 상기에 언급된 바와 같이, 홈 PLMN(114)은 (비밀 식별자를 통지하기 전에 인증 또는 그것의 확인이 홈 PLMN(114)에 의해 요구되지 않는 하나의 옵션에서) 인증이 서빙 PLMN(112)에 의해 수행되기 전에 비밀 식별자를 임의로 전송할 수도 있다. 이것은 도 6의 최상단의 파선의 신호 라인에 의해 나타내어진다.

[0053] 인증 정보의 수신 시에, 서빙 PLMN(112)은 UE 인증 프로시저를 수행할 수도 있다. 인증이 실패하는 경우, 프로세스는 종료될 수 있고, 그러한 실패의 표시(도시되지 않음)는 홈 PLMN(114)에 임의로 전송될 수도 있다. 그러나, 인증이 성공적이고 홈 PLMN(114)이 비밀 식별자를 통지하기 전에 성공적인 UE 인증의 확인을 요구하는 경우, 서빙 PLMN은 인증 확인 메시지를 생성하고 이 인증 확인 메시지를 홈 PLMN(114)에 전송한다. 인증 확인 메시지를 수신하는 것에 응답하여, 홈 PLMN(114)은 서빙 PLMN(112)에 비밀 식별자를 통지하는 것으로 결정한다.

[0054] 게다가, 도 5를 참조하여 이전에 도시된 바와 같이, 홈 PLMN(114)은 비밀 식별자와 함께 암호화 정보를 서빙 PLMN(112)에 전송할 수도 있는데, 이는 서빙 PLMN(112)으로 하여금 공개 식별자 및 비밀 식별자가 홈 PLMN(114)의 인증된 가입자인 단일 UE에 대응한다는 것을 결정하도록 검증 동작의 단계들을 수행하게 한다. 다시, 도 5에 명시적으로 도시되지 않았지만, 서빙 PLMN은 검증 후에 UE에 관련된 동작을 수행할 수도 있다.

[0055] 도 7은 하나 이상의 실시예에 따른 서빙 PLMN(112)의 예시적인 네트워크 노드(106)의 부가적인 세부사항들을 예시한다. 네트워크 노드(106)는 도 2 및 도 4 내지 도 6을 참조하여 상술된 특정 양태들을 수행하기 위한 프로세싱을 구현하도록, 예를 들어, 기능 수단들 또는 유닛들(본 명세서에서 모듈들 또는 컴포넌트들이라고도 또한 지칭될 수도 있음)을 통해, 구성된다. 일부 실시예들에서 네트워크 노드(106)는 예를 들어, UE의 비밀 식별자를 획득하기 위한 획득 수단 또는 유닛(750), 특정 UE의 비밀 식별자를 요구하는 하나 이상의 동작을 수행하기 위한 동작 수행 수단 또는 유닛(760), UE 인증 프로세싱을 수행하기 위한 인증 수단 또는 유닛(770), 및/또는

특정 UE와 연관된 검증 프로시저들을 수행하기 위한 검증 수단 또는 유닛(780)을 포함한다. 이들 그리고 잠재적으로 다른 기능 수단들 또는 유닛들(도시되지 않음)은 서빙 PLMN(112) 및/또는 네트워크 노드(106)에 관련된 것으로서 도 4 내지 도 6에 설명된 피처들 및/또는 도 2에 제시된 방법(200)의 양태들을 함께 수행한다.

[0056] 적어도 일부의 실시예들에서, 네트워크 노드(106)는, 예컨대 상기의 기능 수단들 또는 유닛들을 구현하는 것에 의해, 도 4 내지 도 6에 관련하여 설명된 피처들의 특정한 연관된 프로세싱 및 도 2의 방법(200)의 프로세싱을 구현하도록 구성되는 하나 이상의 프로세싱 회로(720)를 포함한다. 일 실시예에서, 예를 들어, 프로세싱 회로(들)(720)는 각각의 회로들로서 기능 수단들 또는 유닛들을 구현한다. 따라서, 기능 유닛들은 ASIC들 또는 FPGA들과 같은 순수 하드웨어로 구현될 수도 있다. 다른 실시예에서, 이와 관련하여 그 회로들은, 메모리(730)의 형태의 컴퓨터 프로그램 제품과 협력하는 하나 이상의 마이크로프로세서 및/또는 특정 기능 프로세싱을 수행하도록 전용된 회로들을 포함할 수도 있다. 판독 전용 메모리(ROM), 랜덤 액세스 메모리, 캐시 메모리, 플래시 메모리 디바이스들, 광 저장 디바이스들 등과 같은 하나 또는 수 개의 타입들의 메모리를 포함할 수도 있는 메모리(730)를 채용하는 실시예들에서, 메모리(730)는, 하나 이상의 마이크로프로세서에 의해 실행될 때, 본 명세서에 설명된 기법들을 수행하는 프로그램 코드를 저장한다.

[0057] 하나 이상의 실시예에서, 네트워크 노드(106)는 또한 하나 이상의 통신 인터페이스들(710)을 포함한다. 하나 이상의 통신 인터페이스(710)는, 데이터 및 제어 신호들을 전송 및 수신하기 위한 다양한 컴포넌트들(예를 들어, 안테나들(740))을 포함한다. 더 구체적으로는, 인터페이스(들)(710)는, 전형적으로 하나 이상의 표준에 따라, 알려진 신호 프로세싱 기법들을 사용하도록 구성되는 송신기를 포함하고, (예를 들어, 하나 이상의 안테나(740)를 통해 오버 디 에어(over the air)로) 송신하기 위한 신호를 컨디셔닝하도록 구성된다. 유사하게, 인터페이스(들)는, 하나 이상의 프로세싱 회로에 의한 프로세싱을 위해 (예를 들어, 안테나(들)(740)를 통해) 수신된 신호들을 디지털 샘플들로 변환하도록 구성되는 수신기를 포함한다. 양태에서, 획득 모듈 또는 유닛(750)은 수신기를 포함할 수도 있거나 또는 수신기와 통신할 수도 있다. 송신기 및/또는 수신기는 또한 하나 이상의 안테나(740)를 포함할 수도 있다.

[0058] 본 기술분야의 통상의 기술자는 또한 본 명세서의 실시예들이 대응하는 컴퓨터 프로그램들을 더 포함한다는 것을 인식할 것이다. 컴퓨터 프로그램(790)은, 네트워크 노드(106)의 적어도 하나의 프로세서 상에서 실행될 때, 네트워크 노드(106)로 하여금 상술된 각각의 프로세싱 중 임의의 것을 수행하게 하는 명령어들을 포함한다. 게다가, 네트워크 노드(106)의 프로세싱 또는 기능성은 단일 인스턴스 또는 디바이스에 의해 수행되는 것으로서 고려될 수도 있거나, 또는 주어진 서빙 PLMN에 존재할 수도 있는 네트워크 노드(106)의 복수의 인스턴스들에 걸쳐 분할될 수도 있어서, 디바이스 인스턴스들이 함께 모든 개시된 기능성을 수행하도록 한다. 부가적으로, 네트워크 노드(106)는 주어진 개시된 프로세스 또는 평션을 수행하는 것으로 알려져 있는 PLMN과 연관된 임의의 알려진 타입의 디바이스일 수도 있다. 그러한 네트워크 노드들(106)의 예들은 eNB들, 이동성 관리 엔티티(Mobility Management Entity)(MME)들, 게이트웨이들, 서버들 등을 포함한다. 다시 말해, 네트워크 노드(106)는 서빙 PLMN의 액세스 네트워크 부분 또는 코어 네트워크 부분에 상주하는 노드일 수도 있다.

[0059] 도 8은 하나 이상의 실시예에 따른 홈 PLMN(114)의 예시적인 네트워크 노드(116)의 부가적인 세부사항들을 예시한다. 네트워크 노드(116)는 도 2 및 도 4 내지 도 6을 참조하여 상술된 특정 양태들을 수행하기 위한 프로세싱을 구현하도록, 예를 들어, 기능 수단들 또는 유닛들(본 명세서에서 모듈들 또는 컴포넌트들이라고도 또한 지칭될 수도 있음)을 통해, 구성된다. 일부 실시예들에서 네트워크 노드(116)는 예를 들어, UE의 비밀 식별자를 통지할지 여부를 결정하기 위한 결정 수단 또는 유닛(850), 비밀 식별자를 통지하기 위한 통지 수단 또는 유닛(860), 및 UE들의 인증을 수행하기 위한 인증 수단 또는 유닛(870)을 포함한다. 이들 그리고 잠재적으로 다른 기능 수단들 또는 유닛들(도시되지 않음)은 홈 PLMN(114) 및/또는 네트워크 노드(116)에 관련된 것으로서 도 4 내지 도 6에 설명된 피처들 및/또는 도 3에 제시된 방법(300)의 양태들을 함께 수행한다.

[0060] 적어도 일부의 실시예들에서, 네트워크 노드(116)는, 예컨대 상기의 기능 수단들 또는 유닛들을 구현하는 것에 의해, 도 4 내지 도 6의 홈 PLMN(114) 및/또는 네트워크 노드(116)에 관련하여 설명된 피처들의 특정한 연관된 프로세싱 및 도 3의 방법(200)의 프로세싱을 구현하도록 구성되는 하나 이상의 프로세싱 회로(820)를 포함한다. 일 실시예에서, 예를 들어, 프로세싱 회로(들)(820)는 각각의 회로들로서 기능 수단들 또는 유닛들을 구현한다. 따라서, 기능 유닛들은 ASIC들 또는 FPGA들과 같은 순수 하드웨어로 구현될 수도 있다. 다른 실시예에서, 이와 관련하여 그 회로들은, 메모리(830)의 형태의 컴퓨터 프로그램 제품과 협력하는 하나 이상의 마이크로프로세서 및/또는 특정 기능 프로세싱을 수행하도록 전용된 회로들을 포함할 수도 있다. 판독 전용 메모리(ROM), 랜덤 액세스 메모리, 캐시 메모리, 플래시 메모리 디바이스들, 광 저장 디바이스들 등과 같은 하나 또는 수 개의 타입들의 메모리를 포함할 수도 있는 메모리(830)를 채용하는 실시예들에서, 메모리(830)는, 하나 이상의 마이크

로프로세서에 의해 실행될 때, 본 명세서에 설명된 기법들을 수행하는 프로그램 코드를 저장한다.

[0061] 하나 이상의 실시예에서, 네트워크 노드(116)는 또한 하나 이상의 통신 인터페이스(810)를 포함한다. 하나 이상의 통신 인터페이스(810)는, 데이터 및 제어 신호들을 전송 및 수신하기 위한 다양한 컴포넌트들(예를 들어, 안테나들(840))을 포함한다. 더 구체적으로는, 인터페이스(들)(810)는, 전형적으로 하나 이상의 표준에 따라, 알려진 신호 프로세싱 기법들을 사용하도록 구성되는 송신기를 포함하고, (예를 들어, 하나 이상의 안테나(840)를 통해 오버 디 에어로) 송신하기 위한 신호를 컨디셔닝하도록 구성된다. 양태에서, 통지 모듈 또는 유닛(860)은 송신기를 포함할 수도 있거나 또는 송신기와 통신할 수도 있다. 유사하게, 인터페이스(들)는, 하나 이상의 프로세싱 회로에 의한 프로세싱을 위해 (예를 들어, 안테나(들)(840)를 통해) 수신된 신호들을 디지털 샘플들로 변환하도록 구성되는 수신기를 포함한다. 송신기 및/또는 수신기는 또한 하나 이상의 안테나(840)를 포함할 수도 있다.

[0062] 본 기술분야의 통상의 기술자는 또한 본 명세서의 실시예들이 대응하는 컴퓨터 프로그램들을 더 포함한다는 것을 인식할 것이다. 컴퓨터 프로그램(880)은, 네트워크 노드(116)의 적어도 하나의 프로세서 상에서 실행될 때, 네트워크 노드(116)로 하여금 상술된 각각의 프로세싱 중 임의의 것을 수행하게 하는 명령어들을 포함한다. 게다가, 네트워크 노드(116)의 프로세싱 또는 기능성은 단일 인스턴스 또는 디바이스에 의해 수행되는 것으로서 고려될 수도 있거나, 또는 주어진 홈 PLMN에 존재할 수도 있는 네트워크 노드(116)의 복수의 인스턴스들에 걸쳐 분할될 수도 있어서, 디바이스 인스턴스들이 함께 모든 개시된 기능성을 수행하도록 한다. 부가적으로, 네트워크 노드(116)는 주어진 개시된 프로세스 또는 평션을 수행하는 것으로 알려져 있는 하나 이상의 UE에 대한 무선 통신 서비스들 및/또는 네트워크 액세스를 제공하는 PLMN과 연관된 임의의 알려진 타입의 디바이스일 수도 있다. 그러한 네트워크 노드들(116)의 예들은 eNB들, 이동성 관리 엔티티(MME)들, 게이트웨이들, 서버들 등을 포함한다. 다시 말해, 네트워크 노드(116)는 홈 PLMN의 액세스 네트워크 부분 또는 코어 네트워크 부분에 상주하는 노드일 수도 있다.

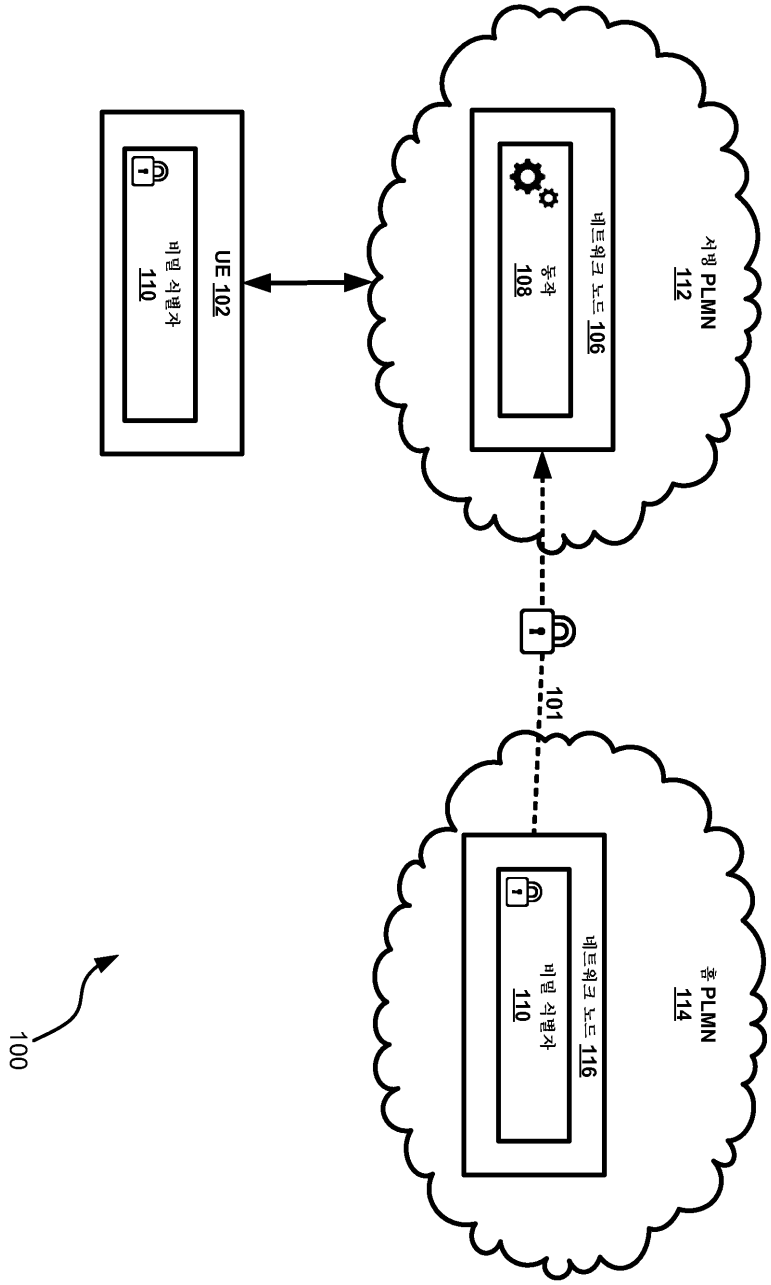
[0063] 실시예들은, 그러한 컴퓨터 프로그램을 포함하는 캐리어를 더 포함한다. 이 캐리어는 (메모리들(730 및 830) 각각과 같은) 전자 신호, 광 신호, 무선 신호, 또는 컴퓨터 판독가능 저장 매체 중 하나를 포함할 수도 있다. 이와 관련하여 컴퓨터 프로그램은, 상술된 수단들 또는 유닛들에 대응하는 하나 이상의 코드 모듈 또는 코드 부분을 포함할 수도 있다.

[0064] 도 1에 관련하여 상기에 언급된 바와 같이, 서빙 PLMN(112)의 다양한 노드들은 서빙 PLMN 또는 네트워크 노드(106)에 기인하는 단계들을 수행할 수도 있다. 도 9는 그 개념 내의 서빙 PLMN의 실시예를 예시한다. 여기서 서빙 PLMN은 적어도 2개의 네트워크 노드들을 포함한다. 제1 네트워크 노드(900)는 네트워크 노드(106)와 유사하게 UE(102)가 성공적으로 인증된 후에 홈 PLMN으로부터 비밀 식별자(110)를 수신하도록 구성된다. 그 후에, 제1 네트워크 노드는 비밀 식별자를 사용하여 동작(108)을 수행하도록 제2 네트워크 노드(902)를 개시할 수도 있다. 서빙 PLMN이 인증을 수행하는 경우에, 서빙 PLMN의 제3 네트워크 노드(906)는 UE(102)를 인증하고 홈 PLMN과 통신하여, 즉, 비밀 식별자(110)를 서빙 PLMN/제1 네트워크 노드(900)에 전송하라고 홈 PLMN에 명시적으로 요청하거나 또는 성공적인 인증을 홈 PLMN에 알리도록 구성될 수도 있다.

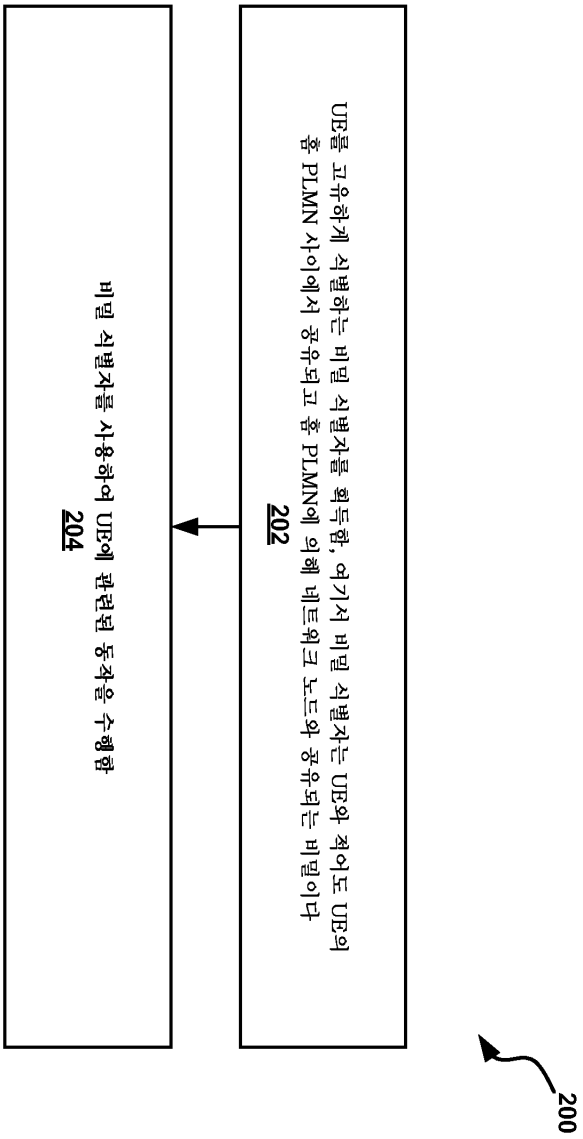
[0065] 물론, 본 실시예들은 본 발명의 본질적인 특성들로부터 벗어남이 없이 본 명세서에 구체적으로 제시된 것들 이외의 다른 방식들로 수행될 수도 있다. 본 실시예들은 모든 관점들에서 예시적이고 제한적이지 않은 것으로서 간주되어야 하고, 첨부된 청구범위의 의미 및 등가 범위 내에 있는 모든 변경들이 그 안에 포괄되도록 의도된다.

도면

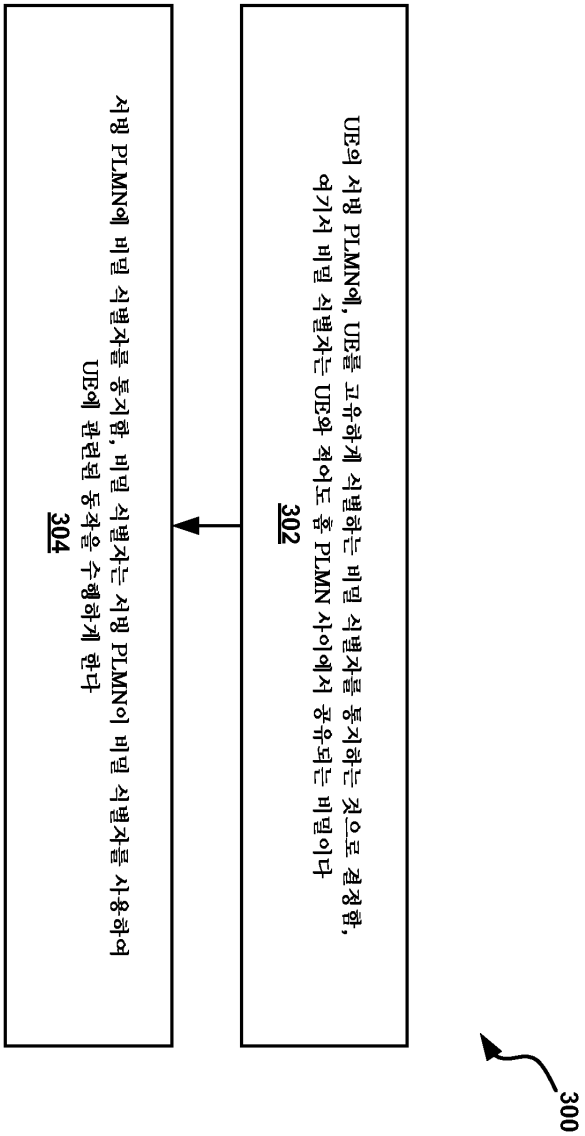
도면1


100
UE 102
비밀 식별자
110
서빙 PLMN
112
네트워크 노드 106
동작
108
101
홈 PLMN
114
네트워크 노드 116
비밀 식별자
110

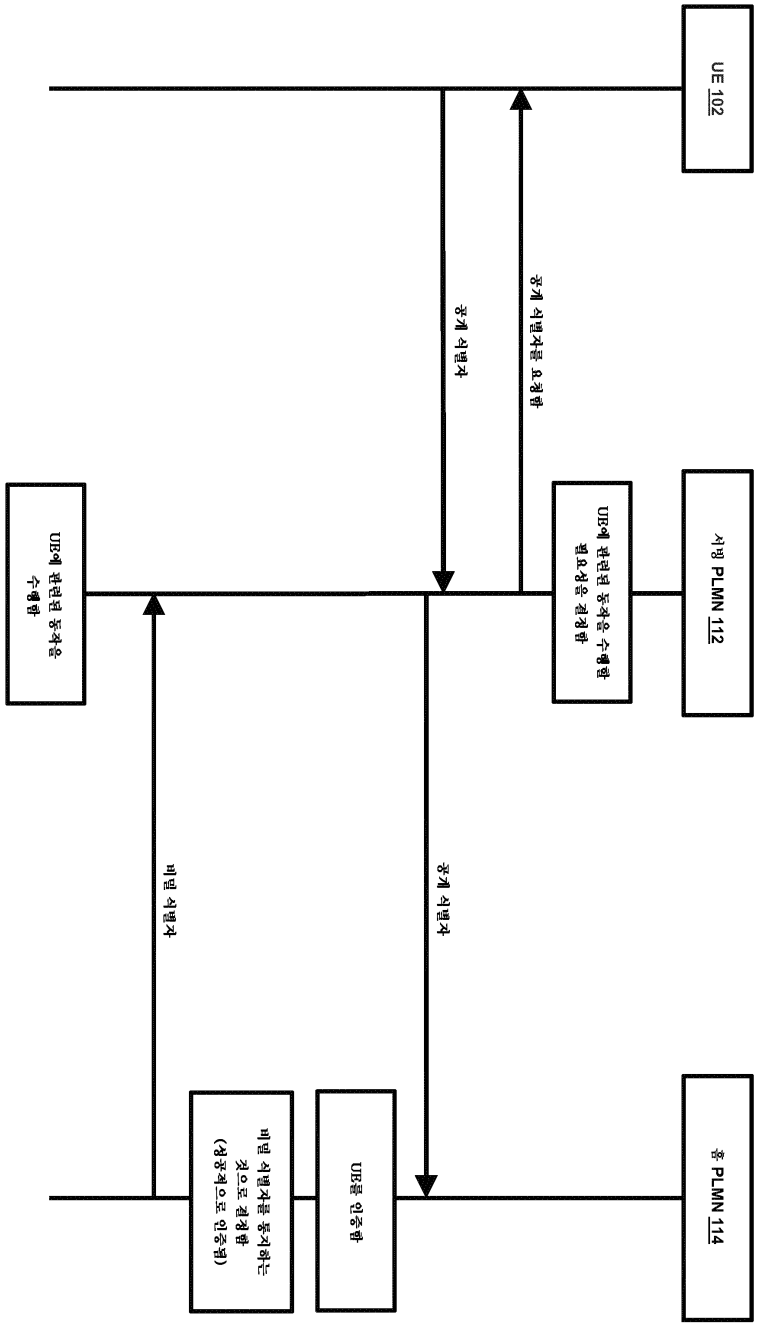
도면2


UE를 고유하게 식별하는 비밀 식별자를 획득함, 여기서 비밀 식별자는 UE와 적어도 UE의 홈 PLMN 사이에서 공유되고 홈 PLMN에 의해 네트워크 노드와 공유되는 비밀이다
202
비밀 식별자를 사용하여 UE에 관련된 동작을 수행함
204
200

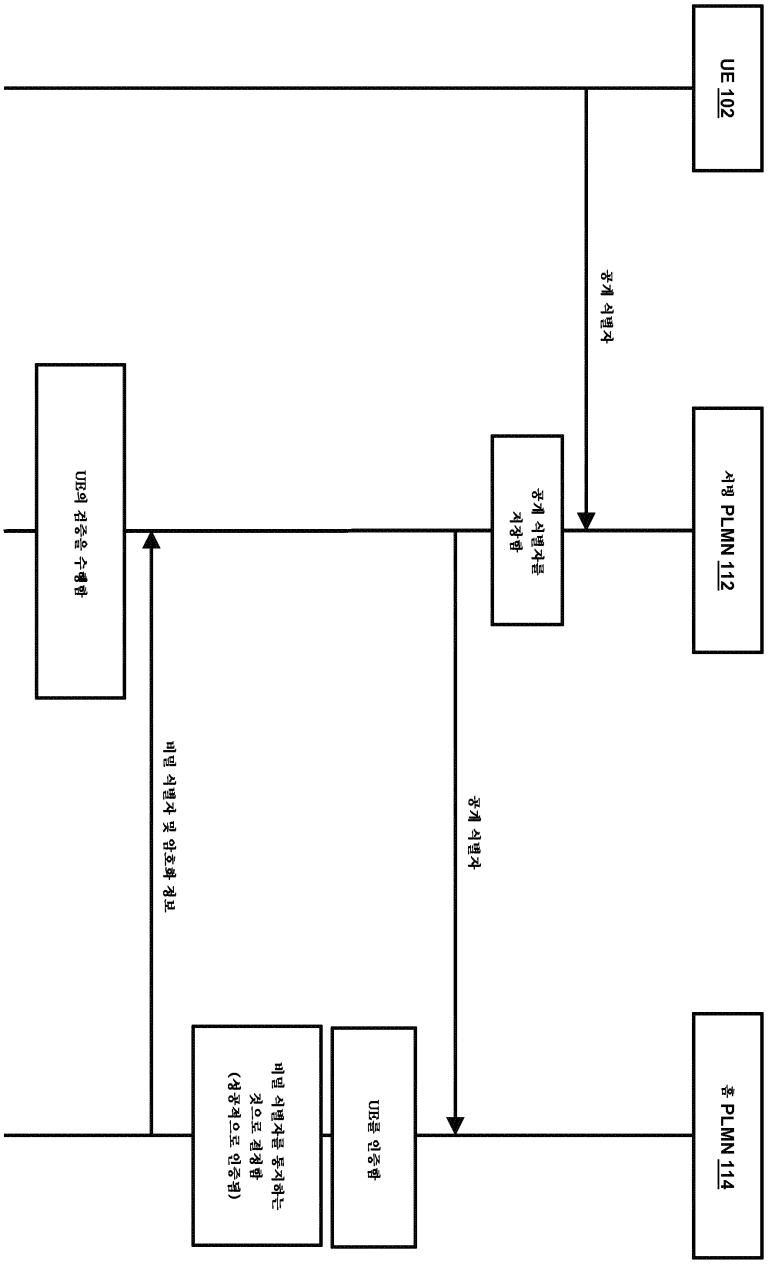
도면3


UE의 서빙 PLMN에, UE를 고유하게 식별하는 비밀 식별자를 통지하는 것으로 결정함, 여기서 비밀 식별자는 UE와 적어도 홈 PLMN 사이에서 공유되는 비밀이다
302
서빙 PLMN에 비밀 식별자를 통지함, 비밀 식별자는 서빙 PLMN이 비밀 식별자를 사용하여 UE에 관련된 동작을 수행하게 한다
304
300

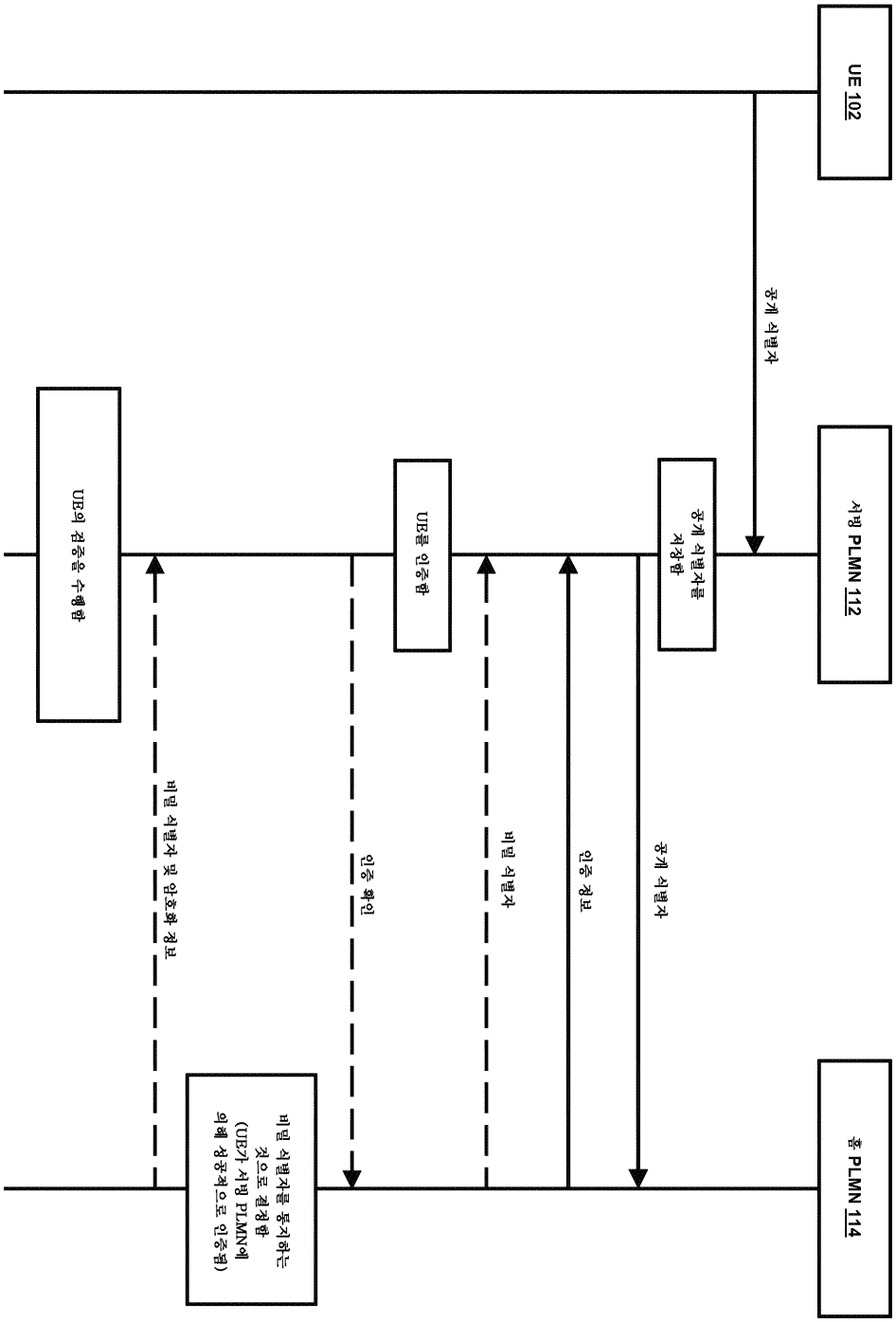
도면4


UE 102
공개 식별자
공개 식별자를 요청함
UE에 관련된 동작을 수행함
UE에 관련된 동작을 수행할 필요성을 결정함
서빙 PLMN 112
비밀 식별자
공개 식별자
비밀 식별자를 동기하는 것으로 결정함 (성공적으로 인증됨)
UE를 인증함
홈 PLMN 114

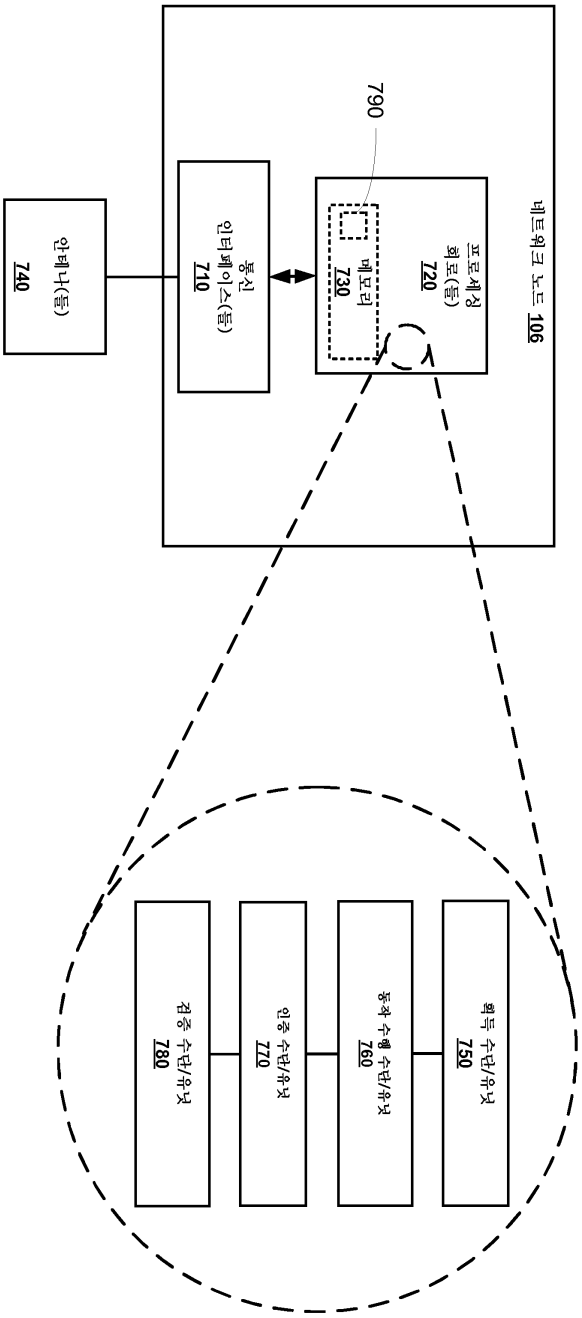
도면5


UE 102
공개 식별자
UE의 검증을 수행함
공개 식별자를 저장함
서빙 PLMN 112
비밀 식별자 및 암호화 정보
공개 식별자
비밀 식별자를 동기하는 것으로 결정함 (성공적으로 인증됨)
UE를 인증함
홈 PLMN 114

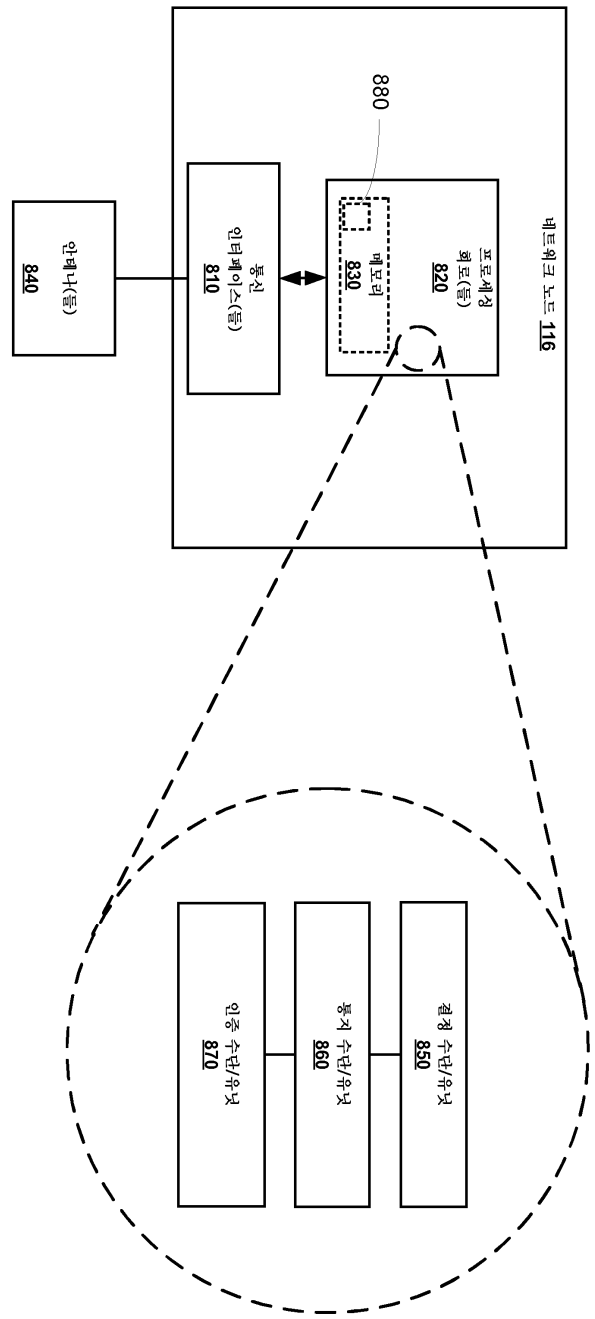
도면6


UE 102
공개 식별자
서빙 PLMN 112
공개 식별자를 처장함
UE를 인증함
UE의 검증을 수행함
비밀 식별자 및 암호화 정보
인증 확인
비밀 식별자
인증 정보
공개 식별자
비밀 식별자를 통지하는 것으로 결정 함 (UE가 서빙 PLMN에 의해 성공적으로 인증됨)
홈 PLMN 114

도면7


790
네트워크 노드 106
프로세싱 회로(들) 720
메모리 730
통신 인터페이스(들) 710
안테나(들) 740
획득 수단/유닛 750
포착 수행 수단/유닛 760
인증 수단/유닛 770
검증 수단/유닛 780

도면8


네트워크 노드 116
880
프로세싱 회로(들) 820
메모리 830
통신 인터페이스(들) 810
안테나(들) 840
결정 수단/유닛 850
통지 수단/유닛 860
얻을 수단/유닛 870

도면9