



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0058577
(43) 공개일자 2020년05월27일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) H04L 29/06 (2006.01)
H04W 4/90 (2018.01)
(52) CPC특허분류
H04W 12/06 (2019.01)
H04L 63/162 (2013.01)
(21) 출원번호 10-2020-7014117(분할)
(22) 출원일자(국제) 2016년11월03일
심사청구일자 없음
(62) 원출원 특허 10-2018-7012772
원출원일자(국제) 2016년11월03일
심사청구일자 2018년05월03일
(85) 번역문제출일자 2020년05월18일
(86) 국제출원번호 PCT/EP2016/076588
(87) 국제공개번호 WO 2017/076986
국제공개일자 2017년05월11일
(30) 우선권주장
15306757.4 2015년11월05일
유럽특허청(EPO)(EP)

(71) 출원인
알까텔 루슨트
프랑스 91620 노제 루트 드 빌쥐스 노키아 파리
사클레
(72) 발명자
시에바우트 로렌트
프랑스 91620 노자이 루트 드 빌저스트 센트레 드
빌라루소 알카텔-루슨트 인터내셔널
랜다이스 브루노
프랑스 22304 라니온 뒤 루이스 드 브로길 4 알카
텔-루슨트 인터내셔널
드레본 니콜라스
프랑스 91620 노자이 루트 드 빌저스트 센트레 드
빌라루소 알카텔-루슨트 인터내셔널
(74) 대리인
제일특허법인(유)

전체 청구항 수 : 총 9 항

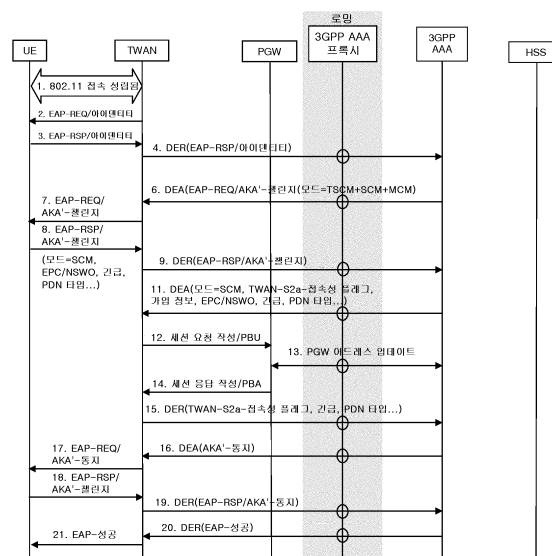
(54) 발명의 명칭 비인증 사용자에 대한 3GPP 진화된 패킷 코어로의 WLAN 액세스를 통한 긴급 서비스의 지원

(57) 요약

일 실시예에서, 비인증 사용자 장비에 대해서 3GPP EPC(Evolved Packet Core)로의 WLAN 액세스를 통한 긴급 서비스를 지원하기 위한 방법으로서,

- 액세스 인증을 위해 사용자 아이덴티티를 제공하라는 요청에 응답하여, 사용자 장비(UE)가 긴급 서비스를 위한 (뒷면에 계속)

대표도 - 도2



비인증 액세스를 나타내는 영역 부분을 갖는 특정 NAI 기반 사용자 아이덴티티를 제공하는 단계와,

- 신뢰 WLAN 액세스를 위한 TWAN 엔티티 또는 비신뢰 WLAN 액세스를 위한 ePDG와 같은 인증기가 UE로부터의 메시지를 영역 부분에 기초하여 긴급 서비스를 위한 비인증 액세스에 전용인 도메인을 서비스하는 특정 3GPP AAA 서버로 라우팅하는 단계와,

- 특정 3GPP AAA 서버가 UE로의 액세스를 승인하고, UE에 대해서 긴급 서비스를 위한 네트워크 액세스를 허용하는 특정 인가 데이터를 제공하는 단계

를 포함한다.

(52) CPC특허분류

H04W 4/90 (2018.02)

명세서

청구범위

청구항 1

장치로서,

프로세서와,

명령어가 저장된 메모리

를 포함하고,

상기 명령어는 실행될 때 상기 장치로 하여금,

진화된 패킷 코어 네트워크(evolved packet core network)로의 신뢰된 무선 로컬 영역 네트워크 액세스를 통해서 사용자 장비가 긴급 서비스에 액세스하도록, 상기 사용자 장비와 네트워크 사이에서 상호 인증을 행하지 않는 특정한 확장가능 인증 프로토콜(EAP:extensible authentication protocol) 기반 절차를 수행하게 하고,

상기 절차 동안, 상기 액세스가 인증이 필요없는 제한된 서비스에 대한 것이라는 표시를 상기 네트워크로부터 수신하게 하며,

상기 절차 동안, 상기 액세스의 접속 모드를 상기 네트워크와 협상하게 하고,

상기 접속 모드는 단일 접속 모드와 다중 접속 모드 중 하나를 포함하는

장치.

청구항 2

제 1 항에 있어서,

상기 명령어는 실행될 때 상기 장치로 하여금 또한,

국제 모바일 가입자 아이덴티티(international mobile subscriber identity) 기반 사용자 아이덴티티가 상기 네트워크에 의해서 인증받을 수 없는 경우에, 상기 표시를 수신하게 하는

장치.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 명령어는 실행될 때 상기 장치로 하여금 또한,

암호화 키 및 무결성 키를 사용하지 않고 사용자 아이덴티티를 사용해서 상기 액세스에 대한 마스터 키를 도출하게 하는

장치.

청구항 4

방법으로서,

진화된 패킷 코어 네트워크로의 신뢰된 무선 로컬 영역 네트워크 액세스를 통해서 사용자 장비가 긴급 서비스에 액세스하도록, 상기 사용자 장비와 네트워크 사이에서 상호 인증을 행하지 않는 특정한 확장가능 인증 프로토콜

기반 절차를 수행하는 단계와,

상기 절차 동안, 상기 액세스가 인증이 필요없는 제한된 서비스에 대한 것이라는 표시를 상기 네트워크로부터 수신하는 단계와,

상기 절차 동안, 상기 액세스의 접속 모드를 상기 네트워크와 협상하게 하는 단계를 포함하며,

상기 접속 모드는 단일 접속 모드와 다중 접속 모드 중 하나를 포함하는 방법.

청구항 5

제 4 항에 있어서,

국제 모바일 가입자 아이덴티티 기반 사용자 아이덴티티가 상기 네트워크에 의해서 인증받을 수 없는 경우에, 상기 표시를 수신하는 단계

를 더 포함하는 방법.

청구항 6

제 4 항 또는 제 5 항에 있어서,

암호화 키 및 무결성 키를 사용하지 않고 사용자 아이덴티티를 사용해서 상기 액세스에 대한 마스터 키를 도출하는 단계

를 더 포함하는 방법.

청구항 7

장치로서,

프로세서와,

명령어가 저장된 메모리

를 포함하고,

상기 명령어는 실행될 때 상기 장치로 하여금,

진화된 패킷 코어 네트워크(evolved packet core network)로의 신뢰된 무선 로컬 영역 네트워크 액세스를 통해서 사용자 장비가 긴급 서비스에 액세스하도록, 상기 사용자 장비와 네트워크 사이에서 상호 인증을 행하지 않는 특정한 확장가능 인증 프로토콜 기반 절차를 수행하게 하고,

상기 절차 동안, 상기 액세스가 인증이 필요없는 제한된 서비스에 대한 것이라는 표시를 상기 사용자 장비로 송신하게 하며,

상기 절차 동안, 상기 액세스의 접속 모드를 상기 네트워크와 협상하게 하고,

상기 접속 모드는 단일 접속 모드와 다중 접속 모드 중 하나를 포함하는 장치.

청구항 8

제 7 항에 있어서,

상기 명령어는 실행될 때 상기 장치로 하여금 또한,

국제 모바일 가입자 아이덴티티 기반 사용자 아이덴티티가 상기 네트워크에 의해서 인증받을 수 없는 경우에, 상기 표시를 수신하게 하는

장치.

청구항 9

제 7 항 또는 제 8 항에 있어서,

상기 명령어는 실행될 때 상기 장치로 하여금 또한,

암호화 키 및 무결성 키를 사용하지 않고 사용자 아이덴티티를 사용해서 상기 액세스에 대한 마스터 키를 도출하게 하는

장치.

발명의 설명

기술 분야

[0001] 본 발명은 전반적으로 모바일 통신 네트워크 및 시스템에 관한 것이다.

배경 기술

[0002] 모바일 네트워크 및 시스템의 설명은 문헌, 특히, 예를 들어, 3GPP(3세대 파트너십 프로젝트)와 같은 표준화 기구에 의해 발행된 기술 사양에서 찾을 수 있다.

[0003] 3GPP 모바일 시스템의 일례는 EPS(진화된 패킷 시스템)이다. EPS 네트워크는, 3GPP 액세스(예를 들어, E-UTRAN)에 의해서나, 또는 신뢰 혹은 비신뢰 비3GPP 액세스(예를 들어, 신뢰 혹은 비신뢰 WLAN)에 의해서 액세스될 수 있는 EPC(진화된 패킷 코어)라고 지칭되는 코어 네트워크를 포함한다. EPC로의 3GPP 액세스는 특히 E-UTRAN 액세스를 위한 3GPP TS 23.401에 명시되어 있다. EPC로의 비3GPP 액세스는 특히 3GPP TS 23.402에 명시되어 있다. EPC로의 3GPP 및 비3GPP(신뢰 및 비신뢰) 액세스는 3GPP TS 23.402로부터 취한 도 1에서 상기된다.

[0004] 예를 들어, EPS와 같은 시스템에서, UE는 EPC 제공 접속(PDN 접속이라고 함) 서비스를 통해 다양한 외부 네트워크(예컨대, 패킷 데이터 네트워크 PDN이라고 하며, 운영자의 IMS 네트워크가 될 수 있음)에 접속될 수 있다. 인증은 일반적으로 액세스를 승인하고 접속 서비스를 제공하기 이전에 수행된다. 그러나, 비인증 사용자 장비에 대해 긴급 서비스와 같은 특정 서비스가 또한 지원될 필요가 있다. 본 문서에서, 비인증 사용자 장비란, 인증된 사용자 아이덴티티 없이 예를 들어, 사용자 아이덴티티가 네트워크에 제공되지 않거나(예를 들어, USIM을 포함하지 않는 사용자 장비), 사용자 아이덴티티(예를 들어, IMSI)이 네트워크에 의해 인증되지 않고, 사용자 장비를 설계하는 것을 의미한다.

발명의 내용

[0005] 이러한 시스템에서 긴급 서비스 지원을 향상시키는 것이 요구되고 있다. 특히, 비인증 사용자 장비에 대한 3GPP EPC로의 신뢰 혹은 비신뢰 WLAN 액세스를 통한 긴급 서비스는 현재 지원되고 있지 않으며, 이러한 지원을 제공하는 것이 요구되고 있다.

[0006] 본 발명의 실시예는 특히 이러한 요구를 달성한다.

[0007] 상기 목적 및 기타 목적은, 일 측면에서 사용자 장비 UE에 의해 달성되고,

[0008] UE는, 비인증 사용자 장비에 대해서 3GPP 진화된 패킷 코어(EPC)로의 WLAN 액세스를 통한 긴급 서비스를 지원하기 위해서,

- [0009] - 액세스 인증을 위해 사용자 아이덴티티를 제공하라는 요청에 응답하여, 긴급 서비스를 위한 비인증 액세스를 나타내는 영역 부분(realm part)을 갖는 특정 NAI(네트워크 액세스 아이덴티티)-기반 사용자 아이덴티티를 제공하도록 구성된다.
- [0010] 상기 목적 및 기타 목적은, 다른 측면에서, EPC로의 신뢰 WLAN 액세스를 위한 TWAN 엔티티 또는 EPC로의 비신뢰 WLAN 액세스를 위한 ePDG와 같은, 인증자에 의해 달성되고,
- [0011] 인증자는, 비인증 사용자 장비에 대해서 3GPP 진화된 패킷 코어(EPC)로의 WLAN 액세스를 통한 긴급 서비스를 지원하기 위해서,
- [0012] - 사용자 장비(UE)로부터 메시지를, 비인증 액세스를 나타내는 NAI(네트워크 액세스 아이덴티티)-기반 사용자 아이덴티티의 영역 부분에 기초하여, 긴급 서비스를 위한 비인증 액세스에 전용인 도메인을 서비스하는 특정 3GPP AAA 서버를 향해 라우팅하도록 구성된다.
- [0013] 상기 목적 및 기타 목적은, 또 다른 측면에서, 3GPP AAA 서버에 의해 달성되고,
- [0014] 3GPP AAA 서버는, 비인증 사용자 장비에 대해서 3GPP 진화된 패킷 코어(EPC)로의 WLAN 액세스를 통한 긴급 서비스를 지원하기 위해서,
- [0015] - 긴급 서비스를 위한 비인증 액세스에 전용인 도메인을 서비스하고,
- [0016] - 비인증 사용자 장비(UE)로의 액세스를 승인하며,
- [0017] - 상기 UE에 대해서 긴급 서비스를 위한 네트워크 액세스를 허용하는 특정 인가 데이터를 제공하도록 구성된다.
- [0018] 상기 목적 및 기타 목적은, 또 다른 측면에서, 3GPP AAA 프록시에 의해 달성되고,
- [0019] 3GPP AAA 프록시는, 비인증 사용자 장비에 대해서 3GPP 진화된 패킷 코어(EPC)로의 WLAN 액세스를 통한 긴급 서비스를 지원하기 위해서,
- [0020] - 사용자 장비에 대한 긴급 상황과 연관된 액세스 인증 시도를 위해 HPLMN의 3GPP AAA 서버와 접촉하는 것이 불가능하다는 것을 검출했을 때, 로컬 정책에 기초해서, 액세스 인증 요청을 긴급 서비스에 대한 비인증 액세스에 전용인 도메인을 서비스하는 로컬 AAA 서버로 방향 전환하도록 구성된다.
- [0021] 상기 목적 및 기타 목적은, 또 다른 측면에서, 상술한 사용자 장비, 인증자, 3GPP AAA 서버, 3GPP AAA 프록시와 같은 다양한 엔티티 중 하나 이상에서 수행되는 단계들을 포함하는 다양한 방법에 의해 달성된다.

도면의 간단한 설명

- [0022] 본 발명의 실시예에 따른 장치 및/또는 방법의 일부 실시예는 단지 예시적으로 설명되는 것이며, 첨부 도면을 참조하고 있다.
- 도 1은 EPC로의 3GPP 및 비3GPP(신뢰 혹은 비신뢰) 액세스를 위한 아키텍처의 일례를 상기하기 위한 것이다.
- 도 2는 본 발명의 실시예에 따른 시그널링 흐름의 일례를 도시하는 것이다.

발명을 실시하기 위한 구체적인 내용

- [0023] 약어
- [0024] AAA 인증 인가 과금
- [0025] AKA 인증 및 키 합의
- [0026] APN 액세스 포인트 이름
- [0027] AVP 속성 값 쌍
- [0028] CK 암호화 키
- [0029] DEA 다이얼미터 EAP 응답
- [0030] DER 다이얼미터 EAP 요청
- [0031] EAP 확장가능 인증 프로토콜

- [0032] EPC 진화된 패킷 코어
- [0033] ePDG 진화된 패킷 데이터 게이트웨이
- [0034] EPS 진화된 패킷 시스템
- [0035] E-UTRAN 진화된 유니버설 지상과 무선 액세스 네트워크
- [0036] HPLMN 홈 공중 육상 모바일 네트워크
- [0037] HSS 홈 가입자 서버
- [0038] IK 무결성 키
- [0039] IMSI 국제 모바일 가입자 아이덴티티
- [0040] IMEI 국제 모바일 장비 아이덴티티
- [0041] IMS IP 멀티미디어 서브시스템
- [0042] LTE 롱 텀 에볼루션
- [0043] MCM 다중 접속 모드
- [0044] MK 마스터 키
- [0045] MSK 마스터 세션 키
- [0046] NAI 네트워크 액세스 식별자
- [0047] PDN 패킷 데이터 네트워크
- [0048] PDN GW PDN 게이트웨이
- [0049] PLMN 공중 육상 모바일 네트워크
- [0050] PRF 의사 랜덤 함수
- [0051] SCM 단일 접속 모드
- [0052] SIM 가입자 아이덴티티 모듈
- [0053] TSCM 투명 단일 접속 모드
- [0054] TWAN 신뢰 WLAN 액세스 네트워크
- [0055] UWAN 비신뢰 WLAN 액세스 네트워크
- [0056] UE 사용자 장비
- [0057] USIM 범용 가입자 식별 모듈
- [0058] WLAN 무선 로컬 영역 네트워크
- [0059] WLCP WLAN 제어 프로토콜
- [0060] 기술 배경
- [0061] - 3GPP TS 33.402 § 6.1은 "EPS에서 비 3GPP 액세스에 대한 액세스 인증은 EAP-AKA(RFC 4187 [7]) 또는 EAP-AKA'(RFC 5448 [23])에 기초해야 한다"라는 일반 규칙으로서 위임된다.
- [0062] - 3GPP TS 23.402 § 16.2에 정의된 바와 같이, TWAN에 액세스하기 위해, UE는 먼저 EAP를 사용하여 인증해야 한다("EAP 인증 절차는 UE, TWAN 및 3GPP AAA 서버를 포함하여 개시되고 수행됨").
- [0063] - 3GPP TS 33.402 § 8.2 "UE로 개시된 IPsec 터널의 셋업을 위한 메커니즘"에 정의된 바와 같이, "RFC 5996 [30]에 명시된 바와 같이 IKEv2 내에서 RFC 4187 [7]에 명시된 바와 같이 EAP-AKA는 UE를 인증하는 데 사용되어야 한다".
- [0064] - 3GPP TS 29.273은 현재 AAA 인터페이스를 통해 비인증 UE에 대한 인증 및 인가 절차를 지원하지 않는다.

- [0065] 본 발명의 다양한 측면 및/또는 실시예의 설명
- [0066] 일부 국가에서, (PLMN이라고 불리는) 모바일 네트워크는 로컬 규정 때문에 비인증 UE(예컨대, USIM을 포함하지 않은 모바일폰 UE)를 위한 긴급 세션을 지원해야 한다. 이 특징은 네트워크 액세스 계층과 서비스 계층 모두 비인증 UE가 긴급 세션을 발행하는 것을 지원한다는 것을 의미한다.
- [0067] 3GPP는 이미 이 기능을 다음과 같이 제공하였다.
- [0068] - 액세스 계층과 서비스 계층 모두에 적용되는 CS(회선 교환) 도메인. 이는 예를 들어 3GPP TS 24.008에 정의된다.
- [0069] - IP에 의존하는 세션 셋업의 서비스 계층에 적용되는 IMS 도메인. 이는 3GPP TS 23.167에 정의된다.
- [0070] - IP에 의존하는 세션 셋업의 3GPP 액세스 계층에 적용되는 EUTRAN(LTE) 액세스. 이는 3GPP TS 23.401에 정의된다.
- [0071] 비인증 UE에 대해서 WLAN을 통한 긴급 세션을 지원하는 것은 3GPP 사양으로는 부족하다. 이 지원은 3GPP TS 23.402에서 정의된 EPC에 대한 신뢰 액세스(TWAN) 및 비신뢰 액세스(UWAN)의 경우 모두에 제공되어야 한다.
- [0072] 이러한 지원을 허용하는 발명의 다양한 측면 및/또는 실시예가 후술될 것이다.
- [0073] 일부 실시예에서, 긴급 세션을 발행하기 위해 WLAN을 통해 EPC 액세스를 셋업해야 하는 UE의 경우, UE가 인증자로부터 자신의 아이덴티티를 제공하라는 요청을 (EAP-아이덴티티 요청의 일부로서) 수신하면,
- [0074] - UE가 EPC에 액세스하기 위한 크리덴셜이 없더라도(UE는 USIM을 갖지 않음), UE는 NAI 포맷을 지원하고 그 IMEI(3GPP TS 23.003에 정의된 바와 같은 국제 이동국 장비 아이덴티티) 및 3GPP 네트워크 내의 긴급 서비스 지원에 전용된 특정 영역에 기초하여 구축된 특정 아이덴티티를 전송한다.
- [0075] - UE가 크리덴셜(USIM)은 있지만 인증받을 수 없다는 것을 알고 있을 때, UE는 NAI 포맷을 지원하고 그 IMSI 및 3GPP 네트워크 내의 긴급 서비스의 지원에 전용된 특정 영역에 기초하여 구축된 특정 아이덴티티를 전송한다.
- [0076] 일부 실시예에서, 이 액세스 요청은 NAI의 영역에 기초하여 액세스를 항상 승인하지만 긴급 서비스에 대해서만 네트워크 액세스를 허용하는 특정 인가 데이터를 제공하는 특정 3GPP AAA 서버 기능으로 라우팅된다.
- [0077] 일부 동작 경우에, UE가 정상적으로 인증되어야 하지만, 긴급 요청을 발행하는 UE의 적합한 인증을 막는 일부 네트워크 문제를 3GPP AAA 프로키가 발견하는 경우, 3GPP AAA 프로키는 (로컬 정책을 기초하여) UE의 인증/인가와 관련된 AAA 시그널링을 동일한 특정 3GPP AAA 서버 기능으로 전환할 수 있다. 이는 액세스가 규칙적으로 인증될 수 없다(예컨대, 표준 EAP-AKA/EAP-AKA' 인증이 발생할 수 없음)는 것을 알려주는 특정 표시가 특정 3GPP AAA 서버에 의해 UE로 다시 전송되기를 요구한다.
- [0078] 일부 실시예에서, 인증 및 MSK 결정과 관련된 예외사항을 제외하고, EAP-AKA/EAP-AKA' 및 AAA 절차는 규칙적으로 인증된 UE의 경우에서와 같이 발생한다. EAP 절차는 UE 및 네트워크에 무선 인터페이스 상의 보안을 위해 사용되는 MSK(Master Session Key)를 제공한다. MSK는 UE가 실제로 인증되는 경우와 다른 방식에 기초하여 결정된다.
- [0079] 본 발명의 실시예의 이점은 다음을 포함한다.
- [0080] - 정규 UE에 대한 액세스의 원칙(그리고, 특히 TWAN 액세스의 경우에 UE와 네트워크 간의 정보 교환(*)), 즉, EAP 절차의 사용, 보안 자료를 또한 제공하는 3GPP AAA 서버에 의해 부여된 EPC 네트워크로의 액세스에 대한 UE 인가를, 긴급 서비스에 대한 액세스에 재사용한다.
- [0081] o (*) 예를 들어, 인증 없이 긴급 서비스에 액세스하기 위한 특정 EAP 절차가 실행되어 UE와 네트워크로 하여금 정규 인증의 경우에 EAP-AKA'를 통해 교환되는 파라미터를 교환할 수 있게 한다.
- [0082] - 로밍의 경우에 HPLMN에 의한 지원이 필요하지 않다.
- [0083] 몇몇 실시예에서, UE가 긴급 서비스를 발행할 필요가 있고 네트워크에 액세스하기 위한 크리덴셜을 가지지 않을 때(예컨대, UE는 (U)SIM을 갖지 않음), UE는 인증자(*)로부터의 EAP-Identity 요청에 대한 응답으로서 다음 속성들 중 일부 또는 전부를 갖는 특정 아이덴티티를 전송한다.
- [0084] - NAI 포맷을 지원함. 즉, 아이덴티티는 NAI의 형태를 취해야 하며, IETF RFC 4282의 2.1 절에 명시된 것처럼

사용자명(username)@영역의 형태를 가져야 한다.

- [0085] - NAI의 사용자명 부분에 IMEI를 가짐.
- [0086] - NAI의 영역 부분에 3GPP 단말기에 대한 비인증 긴급 서비스 지원을 나타내는 특정 값을 가짐. 이 영역 부분(본 발명의 실시예의 일부임)은 3GPP와 같은 표준에 의해 정의된다.
- [0087] (*) 인증자는 (3GPP) AAA 서버로부터 도래하는 인가 정보에 기초하여 네트워크에 대한 UE 액세스를 제어하는 엔티티이다. TWAN(EPC에 대한 신뢰할 수 있는 WLAN 액세스)의 경우에 인증자는 TWAN 내에 있고, UWAN(EPC에 대한 신뢰할 수 없는 WLAN 액세스)의 경우에 인증자는 ePDG이다.
- [0088] 몇몇 실시예에서, 인증자는 NAI의 영역 부분을 담당하는 AAA 서버와 접촉을 시도한다. 몇몇 실시예에서, 이 영역 부분이 긴급 서비스의 지원에 전용될 때, 인증자는 전용 AAA 서버와 접촉된다. 이 전용 AAA 서버는 인증자와 동일한 국가에 위치해야 한다. UE가 USIM을 가지지 않아서 로컬 네트워크가 UE에 대한 HPLMN을 결정할 수 없기 때문에 "HPLMN" 내의 AAA 서버 엔티티는 접촉될 수 없다.
- [0089] 몇몇 실시예에서, 후속하는 단계들의 일부 또는 전부는 신뢰할 수 있는 WLAN 액세스의 경우에 제공될 수 있다
- [0090] - 인증 없이 긴급 서비스에 액세스하기 위한 특정 EAP 절차가 실행되어 UE와 네트워크로 하여금 정규 인증의 경우에 EAP-AKA'를 통해 교환되는 파라미터(예컨대, SCM의 IP 버전에 대한 UE로부터의 요청; MCM의 TWAN 제어 평면 주소)를 교환할 수 있게 한다. 이 절차는 EAP-AKA'를 재사용하지만 UE와 네트워크 간에 상호 인증이 없으므로 이를 수정한다. 그럼에도 불구하고, UE와 네트워크 사이에서 TWAN 모드(SCM/MCM)를 협상하고 SCM에서 PDN 접속의 파라미터를 협상하기 위해 EAP-AKA'에서 지금까지 정의된 모든 메커니즘을 재사용한다
- [0091] - 단일 접속 모드(SCM)와 다중 접속 모드(MCM) 모두에서, UE는 EAP-AKA' 내의 긴급 PDN 접속의 설정을 AAA 서버에 표시하기 위한 새로운 긴급 표시 정보를 포함한다(이 표시는 정규 인증의 경우 3GPP TR 23.771에서 이미 언급되었지만, EAP-AKA'의 일부로서의 포함은 본 발명의 실시예의 일부이다). 다중 접속 모드(MCM)에서 신뢰할 수 있는 WLAN 액세스에 대해, UE는 또한 네트워크에의 부착(attachment)에 이어지는 WLCP PDN 접속 요청의 일부로서 새로운 긴급 표시(이미 3GPP TR 23.771에서 언급됨)를 포함한다.
- [0092] 몇몇 실시예에서, 로컬 규정이 비인증 긴급 세션을 허용할 때, 긴급 서비스를 위한 전용 영역을 서비스하는 AAA 서버는 액세스 요청을 항상 수락하며(인증 백터와 같은 보안 자료가 HSS로부터 검색되지 않으며, 가입 데이터가 HSS로부터 다운로드되지 않음), UE로 하여금 긴급 세션을 진행하게 하지만 임의의 다른 서비스를 금지하게 하는 인가 데이터를 제공한다. 즉, AAA 서버는 일반적인 인가 확인(예컨대, 가입된 APN인지, UE가 EPC에 대한 비-3GPP 액세스를 요청할 수 있는 위치인지, 사용자 비-3GPP 액세스 가입을 갖는지 여부 등을 고려함)을 생략한다. 신뢰할 수 있는 WLAN 액세스에 대해, AAA 서버는 STA를 통해 TWAN에 대한 새로운 긴급 표시 AVP(이미 3GPP TR 23.771에서 언급됨)를 포함시켜, 이것이 긴급 부착이며, 따라서,
- [0093] · SCM에서 TWAG는 긴급 서비스를 위한 PDN 접속을 설정해야 하고,
- [0094] · MCM에서 TWAG는 긴급 서비스에 대한 PDN 접속을 위한 UE로부터의 WLCP 요청만을 수락해야 한다
- [0095] 는 것(이미 3GPP TR 23.771에서 언급됨)을 TWAN에 표시한다.
- [0096] 두 가지 경우(SCM/MCM)에서 TWAG는 설정할 PDN 접속의 파라미터를 결정하기 위해 (UE가 제공하는 접속 파라미터를 사용하는 대신) 로컬로 구성된 긴급 구성 데이터(Emergency Configuration Data)를 사용한다.
- [0097] 일부 실시예에서, 전용 AAA 서버가 인증자와 동일한 국가에 위치하기 때문에, 로밍의 경우 로컬 국가의 엔티티만이 비인증 UE에 대한 긴급 서비스를 지원하는 것과 관련된다. 이를 통해 비인증 UE에 대한 긴급 세션이 허용되지 않거나 배포되지 않은 국가의 로밍자(roamer)가 이러한 것이 허용된 국가에서 비인증 긴급 세션을 발행할 수 있다.
- [0098] 구현 옵션으로서, 이러한 전용 AAA 서버는 인증자(ePDG) 또는 인증자(TWAP)가 접속한 AAA 프록시와 함께 배치될 수 있다.
- [0099] 본 발명의 일부 실시예에서, WLAN을 통한 EPC로의 신뢰/비 신뢰 액세스를 위한 기존 절차의 사용은 UE, TWAN 및 ePDG 레벨에서 허용되는데, 즉
- [0100] - EAP의 사용, 즉 UE 액세스를 네트워크에 개시하고 네트워크가 비인증 긴급 서비스에 대한 네트워크 액세스를 진행할 것을 UE에 알리는 절차. 그러한 액세스가 허용되지 않는 경우 로컬 AAA 엔티티는 EAP 요청을 거부해야

함; EAP를 거부하는 것은 신뢰할 수 있는 WLAN 액세스(SCM 및 MCM에서)를 통해 비인증 UE에 대한 긴급 PDN 접속을 지원하는 것이 필수적인데, 이는 SCM에서 UE로부터 TWAN으로 파라미터를 전송하기 위해 EAP가 사용되고 TWAN 파라미터(예를 들어, TWAN 제어 평면 IPv4 또는 IPv6 주소)를 MCM에서 UE로 전달하기 위해 EAP가 사용되기 때문이다.

- [0101] - 네트워크에 대한 UE 액세스를 제어하는 AAA 서버의 사용(신뢰할 수 있는 WLAN 액세스 및 신뢰할 수 없는 WLAN 액세스 모두에 대해).
- [0102] 일부 실시예에서, EAP가 사용될 때 (WLAN을 통해 EPC에 액세스하기 위한 기존 절차의 일부로서), 인증자(TWAN/EPDG) 및 UE는 EAP 절차가 무선 인터페이스에서 보안을 위해 사용되는 MSK(마스터 세션 키)를 출력할 것을 예상한다(이러한 MSK는 3GPP AAA 서버 및 UE에서 계산됨). 일부 실시예에서, 유사한 원리가 재사용된다:
- [0103] - 신뢰할 수 있는 WLAN 액세스의 경우에, UE 및 3GPP AAA 서버는 NAI의 사용자 부분을 입력으로서 사용하는 키 파생 함수(Key derivation function)에 기초하여 MSK를 로컬에서 결정함; 정규 3GPP 액세스에 대한 MSK 결정(IETF RFC 5448 마다)과의 차이점은 AKA 기반 인증 프로세스의 암호화 키(ciphering keys) CK/IK 출력은 EPC에 대한 비인증 액세스의 경우 인증이 없으므로 사용할 수 없다는 것임. 이러한 MSK는 3GPP AAA 서버에서 TWAN로 전달된 다음 WLAN AN으로 전달되며 수정되지 않은 WLAN AN의 사용을 가능하게 함.
- [0104] o IETF RFC 5448에서 키 파생은 다음과 같이 이루어진다: "MK는 다음과 같이 파생되어 사용된다.
- [0105] $MK = PRF'(IK' || CK', "EAP-AKA" || Identity)$ (PRF = RFC 5448에 정의된 의사 랜덤 함수)
- [0106] $K_{encr} = MK[0..127]$,
- [0107] $K_{aut} = MK[128..383]$,
- [0108] $K_{re} = MK[384..639]$,
- [0109] $MSK = MK[640..1151]$ "
- [0110] o 일부 실시예에서, MK는 파생되어 다음과 같이 사용된다:
- [0111] $MK = PRF'("EAP-AKA" || Identity)$, 여기서 아이덴티티(Identity)는 UE가 EAP를 통해 제공한 것에 기초함: IMEI(SIMless 액세스) 또는 IMSI(SIM을 가진 UE이나 인증될 가능성 없음)
- [0112] K_{encr} , K_{aut} , K_{re} 및 MSK는 IETF RFC 5448에 기술된 MK에 기초하여 결정됨.
- [0113] 일부 실시예에서, 인증자의 로컬 국가에서 허용되는 경우, 전술한 것과 동일한 메커니즘이, UE가 USIM을 가졌지만 인증될 수 없는 경우(로컬 네트워크는 UE의 HPLMN과 (직접 또는 간접적인) AAA 관계를 갖지 않고, 따라서 UE의 인증을 진행할 수 없음)를 지원하도록 적용된다.
- [0114] 이 경우, UE는 특정 영역을 갖는 NAI를 생성하나, 인증자에 의해 개시된 EAP-Identity의 응답으로서 제공된 NAI의 사용자 이름 부분에 IMSI(또한 IMEI가 아님)를 제공한다.
- [0115] 이는 긴급 세션을 설정해야 하지만 적절한 WLAN 네트워크(이의 HPLMN에 의해 UE가 인증되게 할 수 있는 WLAN 네트워크)를 찾지 못한 USIM이 있는 UE에 해당된다.
- [0116] 나머지 절차는 IMSI가 IMEI 대신 사용자 식별자로 사용되는 것(예를 들어, IMSI가 IMEI 대신 MK를 파생시키고 이에 따라 MSK를 파생시키기 위해 사용됨) 보다는 심리스(SIMless) UE에 대한 절차와 동일하다. 이 경우에, EAP-AKA' 인증의 출력에 기초하여 MSK가 결정되지 않도록 UE는 인증받을 수 없다는 것을 미리 인지한 다.
- [0117] 일부 실시예에서, AAA 프록시(예를 들어, 로밍의 경우 3GPP AAA 프록시)가 HPLMN에서 3GPP AAA 서버와 접촉하는 것이 불가능하고 액세스 시도가 로컬 정책에 기초하여 긴급 상황과 관련되어 있다고 검출하는 경우, 3GPP 단말기에 대한 비인증 긴급 서비스를 지원하기 위해 사용된 것과 동일한 영역을 서비스하는 로컬 AAA 서버로 액세스 요청(EAP-AKA 시그널링)을 방향 전환할 수 있다.
- [0118] 이는 예를 들어, 정규 3GPP 서버가 서비스를 제공받지 못하거나, 혼잡하거나 도달 범위를 벗어났기 때문일 수 있다.
- [0119] 로컬 정책은 로컬 규정이 인증되지 않는 긴급 세션을 수락하는지 여부에 따라 달라진다.
- [0120] 이 경우, 동일한 절차가 적용된다: UE는 실제로 인증되지 않으며, MSK는 고정된 캐릭터 시퀀스 및 사용자 아이

덴티티(IMSI)를 고려하지만 AKA 기반 인증 프로세스의 암호화 키 CK/IK 출력을 고려하지 않는 의사 랜덤 함수에 기초하여 결정되됨; 또한, UE는 이 경우에 네트워크를 인증하려고 시도하지 않아야 함.

- [0121] 일부 실시예들에서, UE는 긴급 서비스에 대한 자신의 EPC 액세스에 대해 어떠한 인증도 일어나지 않을 것이라는 것을 미리 알 수 없기 때문에, 네트워크는 이것이 UE로 전송된 EAP-AKA' 시그널링에서 그리고 인증자에게 전송된 AAA 시그널링에서 인증이 필요없는 제한된 서비스에 대한 액세스임을 표시한다.
- [0122] 절차를 보다 견고하고(robust) 보다 일반적으로 만들기 위해, 이 표시는 또한 전송한 두 가지 다른 경우에서 UE(및 인증자)에게 제공될 수 있다.
- [0123] - 긴급 서비스에 대한 SIM이 없는(SIMless) 액세스(UE가 아이덴티티로 자신의 IMEI를 제공함)
- [0124] - UE는 자신의 IMSI를 제공하지만(UE는 SIM을 가짐), 인증을 받을 수 없다는 것을 알고 있다.
- [0125] SCM-비인증 긴급 세션에 대한 TWAN 인증 및 인가 절차에 대한 호 흐름(call flow)의 예가 도 2에 도시되어 있다.
- [0126] 다음 단계들이 제공될 수 있는데, 아래 설명에서 3GPP TS 29.273의 첨부(Annex) A.2-1의 호 흐름과 다른 부분은 밑줄로 표시되어 있다.
- [0127] 1. IEEE 802.11 [40]에 기반한 특정 절차를 사용하여 UE와 TWAN 사이에 접속이 이루어진다.
- [0128] 2. TWAN이 EAP 요청/아이덴티티를 UE로 전송한다.
- [0129] 3. UE가 사용자 부분(SIM이 없는 UE) 내의 IMEI(또는 인증될 수 없는 UE의 경우에는 IMSI) 및 긴급 서비스에 대해 비인증 액세스를 위한 특정 도메인을 포함하는 EAP 응답/아이덴티티 메시지를 TWAN으로 전송한다.
- [0130] 4. TWAN은 UE로부터 수신한 EAP 페이로드를 3GPP AAA 서버(긴급 서비스에 대해 비인증 액세스를 위한 특정 도메인을 서비스함)로 전달하며, 또한 DER 메시지 내에 지원되는 TWAN 접속 모드를 표시한다.
- [0131] 5. 보이드(Void)
- [0132] 6. 3GPP AAA 서버가 EAP 요청/AKA'-챌린지(Challenge)를 전송하는데, 이것은 UE에게 네트워크에 의해 지원되는 TWAN 접속 모드(예컨대, TSCM, SCM 및 MCM)를 알려주고, 이것이 인증이 필요없는 제한된 서비스에 대한 액세스임을 알려준다. DEA 메시지 내의 결과 코드(Result-Code) AVP는 DIAMETER_MULTI_ROUND_AUTH로 설정된다. TWAN-S2a-접속 표시자(Connectivity Indicator)는 DEA-Flags AVP에 설정되어 있지 않다. DEA 메시지는 또한 이것이 인증이 필요없는 제한된 서비스에 대한 액세스라는 표시를 포함한다.
- [0133] 7. TWAN은 EAP 페이로드를 UE에게 전달한다. UE는 네트워크를 인증하려고 시도하지 않을 것이다.
- [0134] 8. UE는 요청된 접속 모드를 나타내는 EAP 응답/AKA'-챌린지를 전송한다. UE가 SCM을 요청하면, UE는 또한 그 세션에 대한 요청된 파라미터, 즉, 긴급 서비스의 표시자, PDN 유형(이 경우 어떠한 APN도 제공되지 않음), PDN 유형(IPv4 또는 IPv6), 최초 접속/핸드오버 표시 및/또는 PCO를 알려준다.
- [0135] 9. TWAN은 EAP 페이로드를 3GPP AAA 서버로 전달한다.
- [0136] 10. 보이드.
- [0137] 11. 이 경우(긴급) 3GPP AAA 서버는 UE가 전송했을 수 있는 임의의 챌린지 응답을 수락하고 UE가 요청한 모드(여기서는 SCM)를 인가할 것이다. 3GPP AAA 서버는 DIAMETER_MULTI_ROUND_AUTH로 설정된 결과 코드 AVP를 갖는 DEA 메시지 내에 세션에 대해 UE가 요청한 파라미터, 즉, 긴급 서비스의 표시자, PDN 유형, 최초 접속/핸드오버 표시 및/또는 PCO를 포함한다. 또한 3GPP AAA 서버는 DEA-플래그 AVP에 TWAN-S2a 접속 표시자를 설정하여 TWAN에게 S2a 접속 수립을 진행하도록 요청한다.
- [0138] 12. TWAN은 S2a 터널 설정을 시작하기 위해 세션 요청 생성(Create Session Request)/PBU 메시지를 PDN GW로 전송한다. TWAN은 UE 아이덴티티(SIM이 없는 UE)(또는 인증받을 수 없는 UE의 경우에는 IMSI)로서 IMEI를 제공한다. [PGW에 대한 GTP-c 인터페이스를 통해 IMEI를 제공하는 것은 SIMless UE를 위한 3GPP 액세스를 통한 긴급 호 셋업의 경우에 사용된다]
- [0139] 13. PDN GW가 3GPP AAA 서버에 PDN GW 아이덴티티 및 UE의 PDN 접속에 대응하는 APN 및 영구 사용자 아이덴티티(PGW가 ePDG/TWAG로부터 IMSI를 수신되지 않은 경우 사용자 부분 내에 IMEI가 있는 NAI)를 통지한다(S6b 인가 요청). AAA 서버는 임의의 추가 검사없이 긴급 PDN 접속에 대한 요청을 인가한다. 3GPP AAA 서버는 HSS를 PGW

주소로 업데이트하지 않는다.

- [0140] 14. PDN GW는 UE에 대해 할당된 IP 어드레스를 포함하여 세션 응답 생성/PBA 메시지를 TWAN에 리턴한다.
- [0141] 15. TWAN은 PDN GW로부터 수신한 제공된 접속 파라미터를 포함하고, 3GPP AAA 서버로의 DER 메시지 내의 DER-플래그 AVP에 TWAN-S2a 접속 표시자를 설정한다. 3GPP AAA 서버는 DER 메시지에 포함된 EAP 페이로드를 무시한다.
- [0142] 16. 3GPP AAA 서버는 AKA'-통지에 PDN 접속 파라미터를 포함하고 DEA 메시지를 TWAN으로 전송한다. DEA 메시지의 결과 코드 AVP는 DIAMETER_MULTI_ROUND_AUTH로 설정된다. TWAN-S2a-접속 표시자(Connectivity Indicator)는 DEA-플래그(Flags) AVP에는 설정되어 있지 않다.
- [0143] 17. TWAN은 EAP 페이로드를 UE로 전달한다.
- [0144] 18-19. UE는 TWAN이 3GPP AAA 서버로 전달하는 EAP-RSP/AKA'-통지 메시지로 응답한다.
- [0145] 20-21. 3GPP AAA 서버는 TWAN이 UE로 전달하는 EAP 성공(Success) 메시지를 전송한다. DEA 메시지의 결과 코드 AVP는 DIAMETER_SUCESS로 설정된다.
- [0146] 일부 실시예에서, 예로서 EPC에 대한 TWAN 액세스를 고려하면, 비인증 UE(예컨대, SIM 없는 UE)의 경우에(이것은 단지 예시일 뿐이다) AAA 서버는 인증 및 인가 응답 메시지에서 다음 정보를 TWAN에게 제공할 수 있다(3GPP TS 29.273 참조).

정보 요소 명	다이아미터 AVP의 매핑	Cat.	설명
사용자 식별자	User-Name	M	사용자 Id는 (본 발명의 일부로서) 사용자 부분의 IMEI와 함께 NAI로서 코딩된다. 비인증 비상 세션의 경우 빠른 RE 인증/가명이 사용되지 않는다. UE가 IMSI를 제공했지만, 이 IMSI가 인증되지 않은 경우, 이 IMSI는 사용자 식별자로서 제공된다.
EPA 페이로드	EPA payload	O	EPA 페이로드는 EPA 성공을 포함한다.
인증 요청 타입	Auth-Request-Type	M	이는 AUTHORIZE_AUTHENTICATE를 포함할 것이다. IETF RFC 4072 [5]를 참조하라.
결과 코드	Result-Code/Experimental Result Code	M	
세션 활성 시간	Session-Timeout	O	이 AVP는 Result-Code AVP가 DIAMETER_SUCCESS로 설정되면 존재할 수 있으며, 만약 존재한다면, 세션이 활성으로 유지하는 데 허용되는 최대의 초(second) 시간을 포함한다. 그러한 경우에 3GPP AAA 서버가 특성의 Session-Timeout을 사용할 수 있다는 사실을 제외하고는, 이 AVP는 비인증 UE를 지원하도록 특정되어 있지 않다.
어카운팅 중간 간격	Accounting Interim-Interval	O	비인증 비상 세션의 경우, 이 정보는 제공되지 않는다.
패어와이즈 마스터 키	EAP-Master-Session-Key	C	이 IE는 Result-Code AVP가 DIAMETER_SUCCESS로 설정되면 존재할 것이다.
디플트 APN	Context-Identifier	C	이 정보는 TWAN이 로컬 비상 구성 데이터를 사용하므로 AAA 서버에 의해 전송되지 않는다.
APN-이 교체	APN-Of-Replacement	C	이 정보는 TWAN이 로컬 비상 구성 데이터를 사용하므로 AAA 서버에 의해 전송되지 않는다.
APN 및 PGW 데이터	APN-Of-Configuration	C	이 정보는 UE가 오직 비상 서비스를 위한 비상 PDN 접속을 수립하도록만 허용되므로 제공되지 않을 것이다.
서빙 GW 어드레스	MIP6-Agent-Info	O	적용될 수 없음.
이동성 기능	MIP6-Feature-Vector	C	이 정보는 UE가 오직 비상 서비스를 위한 비상 PDN 접속을 수립하도록만 허용되므로 제공되지 않을 것이다.
영구 사용자 식별자	Mobile-Node-Identifier	C	임의의 선행하는 숫자가 없다면 사용자 식별자와 동일함. 이 정보는 AAA 서버가 사용자에 대해 HSS에 문의하지 않으므로
3GPP AAA 서버 URI	Redirect-Host	C	비인증 비상 PDN 접속을 위해 전송되지 않는다 (그리고 이에 따라 이 정보는 사용자가 이미 상이한 AAA 서버에 의해 서빙되고 있다면 HSS에 의해 통지될 수 없다).
UE 충전 데이터	3GPP-Charging-Characteristics	O	이 정보는 TWAN이 로컬 비상 구성 데이터를 사용하므로 AAA 서버에 의해 전송되지 않는다.
UE AMBR	AMBR	C	이 정보는 TWAN이 로컬 비상 구성 데이터를 사용하므로 AAA 서버에 의해 전송되지 않는다.
전설 관계 표시자	AN-Trusted	C	정규 STa 세션의 경우와 동일.
지원되는 특징들 (3GPP TS 29.229 [24] 참조)	Supported-Features	O	존재한다면, 이 정보 요소는 다이아미터 세션의 수명 동안 원래의 호스트에 지원되는 특징들의 리스트를 포함할 것이다.
FA-RK	MIP-FA-RK	C	이 AVP는 WLAN 액세스의 경우에 사용되지 않는다.
FA-RK-SPI	MIP-FA-RK-SPI	C	이 AVP는 WLAN 액세스의 경우에 사용되지 않는다.
트레이스 정보	Trace-Info	C	이 정보 요소는 비인증 비상 세션에 대해서는 지원되지 않는다.
MSISDN	Subscription-ID	C	적용될 수 없음.
DEA 플래그들	DEA-Flags	O	이 정보 요소는 비트 마스크를 포함한다. 본 발명의 일부로서, 3GPP AAA 서버는 IMSI가 인증되었는지를 나타낼 수 있다 (STa를 통한 "Unauthenticated IMSI" 플래그). TWAN은 이 정보를 사용하여 S2a/GTP-c를 통한 "Unauthenticated IMSI" 정보를 팜플레이팅하며, 이 정보는 다음과 같이 현재 정의되고 있다. Unauthenticated IMSI: 이 플래그는 메시지 내에 존재하는 IMSI가 인증되어 있지 않고 비상 첨부 UE용인 경우 S4/S11 및 S5/S8 인터페이스 상에서 1로 설정될 것이다.
선택된 TWAN 접속 모드	TWAN-Connection-Mode	C	이 정보는 정규 TWAN 세션(가령, EAP-AKA' 인증과 연관된 TWAN 세션)의 경우에서와 동일하다.
요청된 접속 파라미터들	TWAN-Connectivity-Parameters	C	이 정보는 정규 TWAN 세션(가령, EAP-AKA' 인증과 연관된 TWAN 세션)의 경우에서와 동일하다.
WLCP 키	WLCP-Key	C	이 정보는 Result-Code AVP가 DIAMETER_SUCCESS로 설정되고 선택된 TWAN 접속 모드가 MCM인 경우 반드시 존재한다. 비인증 비상 세션의 경우 WLCP 암호화를 사용하게 되면 인증 및 비인증 비상 세션들의 모두에 대해 동일한 WLCP SW를 갖는 것이 가능하다. 즉, 본 발명은 3GPP가 비인증 비상 세션에 대한 WLCP 암호화를 사용하도록 결정하지 않을 경우에 작동가능하다.

[0147]

[0148]

본 발명의 다양한 측면은 이하의 측면을 포함한다(이것으로 한정되는 것은 아니다). 일 측면은 사용자 장비(UE)로서, 비인증 사용자 장비에 대해서 3GPP EPC로의 WLAN 액세스를 통한 긴급 서비스를 지원하기 위해서 구성된다.

[0149]

다양한 실시예가 제공될 수 있으며, 이하의 실시예를 포함하고(이것으로 한정되는 것은 아니다), 이들은 다양한 조합에 따라서 단독으로 혹은 조합해서 취해질 수 있다.

[0150]

일 실시예에서, 사용자 장비는,

[0151]

- 액세스 인증을 위해 사용자 아이덴티티를 제공하라는 요청에 응답하여, 긴급 서비스를 위한 비인증 액세스를 나타내는 영역 부분을 갖는 특정 네트워크 액세스 아이덴티티(NAI) 기반 사용자 아이덴티티를 제공하도록 구성된다.

[0152]

일 실시예에서, 사용자 장비는,

- [0153] - UE가 IMSI를 갖지 않는 경우,
- [0154] - UE가 IMSI를 가지지만 IMSI가 인증받을 수 없다는 것을 아는 경우
- [0155] 중 하나에서 특정 사용자 아이덴티티를 제공하도록 구성된다.
- [0156] 일 실시예에서, 사용자 장비는,
- [0157] UE가 IMSI를 갖지 않으면, IMEI에 기초한 사용자 이름 부분(username part)을 갖는 특정 NAI 기반 사용자 아이덴티티를 제공하도록 구성된다.
- [0158] 일 실시예에서, 사용자 장비는,
- [0159] - 인증없이 긴급 서비스에 액세스하기 위한 특정 EAP 기반 절차를 수행하도록 구성되되, 특정 EAP 기반 절차는 정규 EAP 기반 절차와 관련하여,
- [0160] - 네트워크 인증을 시도하지 않는 것,
- [0161] - 암호화 키(CK) 및 무결성 키(IK)를 사용하지 않고 마스터 키(MK)를 도출하는 것
- [0162] 중 적어도 하나를 포함한다.
- [0163] 또 다른 측면은, EPC로의 신뢰 WLAN 액세스를 위한 TWAN 엔티티 또는 EPC로의 비신뢰 WLAN 액세스를 위한 ePDG와 같은 인증기로서, 비인증 사용자 장비에 대해서 3GPP EPC(Evolved Packet Core)에 대한 WLAN 액세스를 통한 긴급 서비스를 지원하도록 구성된다.
- [0164] 다양한 실시예가 제공될 수 있으며, 이하의 실시예를 포함하고(이것으로 한정되는 것은 아니다), 이들은 다양한 조합에 따라서 단독으로 혹은 조합해서 취해질 수 있다.
- [0165] 일 실시예에서, 인증기는
- [0166] - 긴급 서비스를 위한 비인증 액세스를 나타내는 네트워크 액세스 아이덴티티(NAI) 기반 사용자 아이덴티티의 영역 부분에 기초하여, 사용자 장비(UE)로부터의 메시지를, 긴급 서비스에 대한 비인증 액세스에 전용인 도메인을 서비스하는 특정 3GPP AAA 서버로 라우팅하도록 구성된다.
- [0167] 일 실시예에서, 인증기는
- [0168] - 액세스가 제한된 서비스에 대한 것임을 나타내는 3GPP AAA 서버로부터의 표시를 처리하는 것,
- [0169] - 사용자 아이덴티티가 인증되지 않았음을 나타내는 3GPP AAA 서버로부터의 표시를 처리하고 이 정보를 PDN GW에 중계하는 것
- [0170] 중 적어도 하나를 수행하도록 구성된다.
- [0171] 또 다른 측면은 비인증 사용자 장비에 대해서 3GPP EPC로의 WLAN 액세스를 통한 긴급 서비스를 지원하도록 구성된 3GPP AAA 서버이다.
- [0172] 다양한 실시예가 제공될 수 있으며, 이하의 실시예를 포함하고(이것으로 한정되는 것은 아니다), 이들은 다양한 조합에 따라서 단독으로 혹은 조합해서 취해질 수 있다.
- [0173] 일 실시예에서, 3GPP AAA 서버는
- [0174] - 긴급 서비스에 대해 비인증 액세스에 전용인 도메인을 서비스하고,
- [0175] - 비인증 사용자 장비(UE)에 대한 액세스를 승인하고,
- [0176] - UE에 대한 긴급 서비스를 위한 네트워크 액세스를 허용하는 특정 인가 데이터를 제공하도록 구성된다.
- [0177] 일 실시예에서, 3GPP AAA 서버는
- [0178] - 인증없이 긴급 서비스에 액세스하기 위한 특정 EAP 기반 절차를 수행하도록 구성되되,
- [0179] 특정 EAP 기반 절차는 정규 EAP 기반 절차와 관련하여,
- [0180] - UE에 대한 인증 백터를 HSS로부터 인출하지 않는 것,
- [0181] - 액세스가 인증이 필요없는 제한된 서비스에 대한 것임을 나타내는 표시를 제공하는 것,

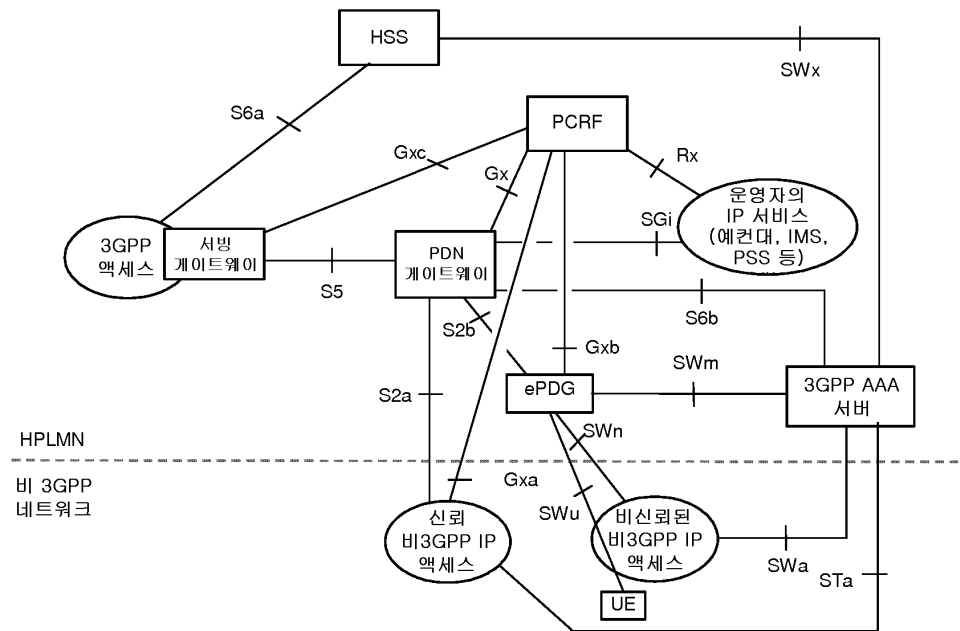
- [0182] - UE에 의해 전송된 임의의 도전 응답을 수용하는 것,
- [0183] - HSS로부터 사용자의 가입 정보를 다운로드하지 않는 것,
- [0184] - 긴급 PDN 접속에 대한 요청을 임의의 추가 확인없이 수용하는 것,
- [0185] - 암호화 키(CK) 및 무결성 키(IK)를 사용하지 않고 마스터 키(MK)를 도출하는 것,
- [0186] - 특정 EAP 기반 절차가 예를 들어 TWAN 액세스의 경우 정규 3GPP AAA 서버의 특징들 중 일부를 지원하는 경우, EAP 기반 시그널링과 인증기 사이에서 정보를 중계하거나 액세스의 모드를 협상하는 것
- [0187] 중 적어도 하나를 포함한다.
- [0188] 일 실시예에서, 3GPP AAA 서버는
- [0189] 액세스가 인증이 필요없는 제한된 서비스에 대한 것임을, 액세스 인증에 포함된 UE 및 인증기에 알리도록 구성된다.
- [0190] 일 실시예에서, 3GPP AAA 서버는
- [0191] 인증기에 알릴 때 제공하는 IMSI가 인증되지 않았다는 것을, 액세스 인증에 포함된 인증기에 알리도록 구성된다.
- [0192] 또 다른 측면은 비인증 사용자 장비에 대해서 3GPP EPC로의 WLAN 액세스를 통한 긴급 서비스를 지원하도록 구성된 3GPP AAA 프록시이다.
- [0193] 다양한 실시예가 제공될 수 있으며, 이하의 실시예를 포함한다(이것으로 한정되는 것은 아니다).
- [0194] 일 실시예에서, 3GPP AAA 프록시는
- [0195] - 사용자 장비에 대해 긴급 상황과 연관된 액세스 인증 시도를 위해 HPLMN 내의 3GPP AAA 서버와 접촉한다는 것이 불가능하다고 검출되면, 로컬 정책에 기초하여, 긴급 서비스에 대한 비인증 액세스에 전용인 도메인을 서비스하는 로컬 AAA 서버로 액세스 인증 요청을 방향 전환하도록 구성된다.
- [0196] 또 다른 측면은 비인증 사용자 장비에 대해서 3GPP EPC로의 WLAN 액세스를 통한 긴급 서비스를 지원하기 위한 방법이다.
- [0197] 다양한 실시예가 제공될 수 있으며, 이하의 실시예를 포함하고(이것으로 한정되는 것은 아니다), 이들은 다양한 조합에 따라서 단독으로 혹은 조합해서 취해질 수 있다.
- [0198] 일 실시예에서, 이 방법은,
- [0199] - 긴급 서비스에 대한 비인증 액세스에 전용인 도메인을 서비스하는 특정 3GPP AAA 서버가 비인증 사용자 장비(UE)에 대한 액세스를 승인하고, UE에 대한 긴급 서비스를 위한 네트워크 액세스를 허용하는 특정 인가 데이터를 제공하는 단계를 포함한다.
- [0200] 일 실시예에서, 이 방법은,
- [0201] 액세스 인증을 위해 사용자 아이덴티티를 제공하라는 요청에 응답하여, 사용자 장비(UE)가 긴급 서비스를 위한 비인증 액세스를 나타내는 영역 부분을 갖는 특정 NAI 기반 사용자 아이덴티티를 제공하는 단계,
- [0202] 신뢰 WLAN 액세스를 위한 TWAN 엔티티 또는 비신뢰 WLAN 액세스를 위한 ePDG와 같은 인증기가 UE로부터의 메시지를 영역 부분에 기초하여 특정 3GPP AAA 서버로 라우팅하는 단계를 포함한다.
- [0203] 일 실시예에서, 이 방법은,
- [0204] 사용자 장비에 대해 긴급 상황과 연관된 액세스 인증 시도를 위해 HPLMN 내의 3GPP AAA 서버와 접촉한다는 것이 불가능하다고 검출되면, 로컬 정책에 기초하여, 긴급 서비스에 대한 비인증 액세스에 전용인 도메인을 서비스하는 로컬 AAA 서버로 UE에 대한 액세스 인증 요청을 방향 전환하는 단계를 포함한다.
- [0205] 일 실시예에서, 이 방법은,
- [0206] 3GPP AAA 서버가, 액세스가 비인증 장치를 위한 긴급 서비스에 대한 액세스에 대응하고 따라서 긴급 서비스의 지원으로 제한된다는 것을, UE 및 인증기에 나타내는 단계를 포함한다.

[0207] 사용자 장비, 인증자, 3GPP AAA 서버, 3GPP AAA 프록시에 대한 상술한 다양한 실시예에 따라서, 이 방법에 대한 다양한 실시예가 제공될 수 있다.

[0208] 당업자라면 다양한 상술한 방법의 단계가 프로그래밍된 컴퓨터에 의해서 수행될 수 있다는 것을 용이하게 이해할 것이다. 본 명세서에서, 일부 실시예는 머신 혹은 컴퓨터 판독 가능한 것이며 명령어의 머신-실행 가능 혹은 컴퓨터-실행 가능 프로그램을 인코딩하는 예컨대, 디지털 데이터 저장 매체와 같은 프로그램 저장 장치를 포함하도록 했으며, 명령어는 상술한 방법의 단계 중 일부 혹은 전부를 수행하는 것이다. 프로그램 저장 장치는 예컨대, 디지털 메모리, 자기 디스크 및 자기 테이프와 같은 자기 저장 매체, 하드 드라이브, 혹은 광학적으로 판독 가능한 디지털 데이터 저장 매체가 될 수 있다. 실시예는 또한 상술한 방법의 단계를 수행하도록 프로그래밍된 컴퓨터를 포함하도록 했다.

도면

도면1



도면2

