(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년09월18일
(11) 등록번호 10-1554396
(24) 등록일자 2015년09월14일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04W 12/04* (2009.01)
H04W 12/08 (2009.01)
(21) 출원번호 10-2013-7001211
(22) 출원일자(국제) 2011년06월16일
심사청구일자 2013년01월16일
(85) 번역문제출일자 2013년01월16일
(65) 공개번호 10-2013-0029103
(43) 공개일자 2013년03월21일
(86) 국제출원번호 PCT/US2011/040777
(87) 국제공개번호 WO 2011/159952
국제공개일자 2011년12월22일
(30) 우선권주장
13/161,336 2011년06월15일 미국(US)
61/355,423 2010년06월16일 미국(US)
(56) 선행기술조사문헌
KR1020070003484 A*
KR1020070042243 A*
US20090024751 A1*
WO2009141919 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
에스콧 애드리안 에드워드
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
팔라니고운데르 아난드
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인코리아나

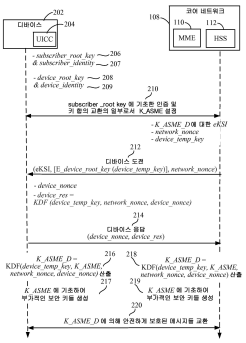
전체 청구항 수 : 총 50 항 심사관 : 이상윤

(54) 발명의 명칭 **통신 시스템들에서 가입자 인증과 디바이스 인증을 바인딩하는 방법 및 장치**

(57) 요 약

디바이스 (예를 들면, 클라이언트 디바이스 또는 액세스 단말) 와 네트워크 엔티티 사이에 인증 방법이 제공된다. 착탈식 저장 디바이스는 디바이스에 결합될 수도 있으며, 가입자 인증을 위하여 사용될 수도 있는 가입자-특정 키를 저장한다. 보안성 저장 디바이스는 디바이스에 결합될 수도 있으며, 디바이스 인증을 위하여 사용되는 디바이스-특정 키를 저장한다. 가입자 인증은 디바이스와 네트워크 엔티티 사이에 수행될 수도 있다. 디바이스의 디바이스 인증은 또한 네트워크 엔티티와 수행될 수도 있다. 가입자 인증과 디바이스 인증을 바인딩하는 보안 키가 그런 다음 생성될 수도 있다. 보안 키는 디바이스와 서빙 네트워크 사이의 통신을 안전하게 보호하기 위하여 사용될 수도 있다.

대 표 도 - 도2



명 세 서

청구범위

청구항 1

디바이스에서 작동하는 방법으로서,

가입자 인증 키에 기초하여 네트워크 엔티티와의 가입자 인증을 수행하는 단계;

디바이스 인증 데이터를 획득하기 위하여 상기 네트워크 엔티티와의 상기 디바이스의 디바이스 인증을 수행하는 단계로서, 상기 디바이스 인증 데이터는 디바이스 아이덴티티 혹은 크리덴셜, 그리고 상기 디바이스에 의해 수신된 도전(challenge)에 기초하여 획득되는, 상기 디바이스 인증을 수행하는 단계;

상기 가입자 인증 키 및 상기 디바이스 인증 데이터에 기초하여 상기 가입자 인증과 상기 디바이스 인증을 바인딩하는 보안 키를 생성하는 단계; 및

상기 보안 키를 사용하여 상기 디바이스와 서빙 네트워크 사이의 통신을 안전하게 보호하는 단계를 포함하는, 디바이스에서 작동하는 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제 1 항에 있어서,

상기 가입자 인증은 상기 네트워크 엔티티의 일부인 제 1 인증 서버에 의해 수행되고, 상기 디바이스 인증은 상기 네트워크 엔티티의 일부인 제 2 인증 서버에 의해 수행되는, 방법.

청구항 5

제 1 항에 있어서,

상기 디바이스 인증은,

상기 네트워크 엔티티로부터 상기 디바이스의 공개 키를 이용하여 암호화된 데이터를 수신하고;

대응하는 개인 키를 사용하여 상기 암호화된 데이터를 해독하고;

그 후에 상기 디바이스가 상기 데이터에 대한 지식을 가지고 있다는 것을 상기 네트워크 엔티티에 입증함으로써 수행되는, 방법.

청구항 6

제 1 항에 있어서,

상기 디바이스로부터 상기 네트워크 엔티티로 어태치 요청을 전송하는 단계를 더 포함하며, 상기 어태치 요청은 상기 디바이스가 디바이스 인증의 능력이 있다는 표시를 포함하는, 방법.

청구항 7

제 1 항에 있어서,

상기 디바이스 인증은 상기 가입자 인증 동안 생성된 적어도 하나의 키에 의해 안전하게 보호되는, 방법.

청구항 8

제 1 항에 있어서,

상기 가입자 인증 및 상기 디바이스 인증은 가입자 인증 및 디바이스 인증이 결합된 메시지 교환들에서 동시에 수행되는, 방법.

청구항 9

제 1 항에 있어서,

상기 가입자 인증은 초기의 그리고 상기 디바이스 인증과는 별도의 보안 교환에서 수행되는, 방법.

청구항 10

제 1 항에 있어서,

상기 보안 키는 적어도 상기 가입자 인증으로부터 획득된 제 1 키 및 상기 디바이스 인증으로부터 획득된 제 2 키의 함수로서 생성되는, 방법.

청구항 11

삭제

청구항 12

제 1 항에 있어서,

상기 디바이스는, 상기 네트워크 엔티티에 대한 액세스 단말로서 나타나고 하나 이상의 액세스 단말들에 대한 네트워크 디바이스로서 나타나는 릴레이 노드인, 방법.

청구항 13

제 1 항에 있어서,

상기 보안 키는 상기 디바이스 및 상기 네트워크 엔티티에 의해 별도로 생성되는, 방법.

청구항 14

제 1 항에 있어서,

서비스 합의의 일부로서 가입자-특정 키를 제공하는 단계로서, 상기 가입자-특정 키는 상기 가입자 인증을 위해 사용되는, 상기 가입자-특정 키를 제공하는 단계; 및

제조 동안에 상기 디바이스 내에 디바이스-특정 키를 제공하는 단계로서, 상기 디바이스-특정 키는 상기 디바이스 인증을 위해 사용되는, 상기 디바이스-특정 키를 제공하는 단계를 더 포함하는, 방법.

청구항 15

디바이스로서,

통신 인터페이스; 및

상기 통신 인터페이스에 결합된 프로세싱 회로를 포함하며,

상기 프로세싱 회로는,

가입자 인증 키에 기초하여 네트워크 엔티티와의 가입자 인증을 수행하고;

디바이스 인증 데이터를 획득하기 위하여 상기 네트워크 엔티티와의 상기 디바이스의 디바이스 인증을 수행하되, 상기 디바이스 인증 데이터는 디바이스 아이덴티티 혹은 크리덴셜, 그리고 상기 디바이스에 의해 수신된 도전(challenge)에 기초하여 획득되고;

상기 가입자 인증 키 및 상기 디바이스 인증 데이터에 기초하여 상기 가입자 인증과 상기 디바이스 인증을 바인딩하는 보안 키를 생성하고;

상기 보안 키를 사용하여 상기 디바이스와 서빙 네트워크 사이의 통신을 안전하게 보호하도록 구성된,

디바이스.

청구항 16

삭제

청구항 17

제 15 항에 있어서,

상기 디바이스 인증은 상기 디바이스와 상기 네트워크 엔티티 사이의 도전-응답 교환에 기초하는, 디바이스.

청구항 18

제 15 항에 있어서,

상기 디바이스 인증은,

상기 네트워크 엔티티로부터 상기 디바이스의 공개 키를 이용하여 암호화된 데이터를 수신하고;

대응하는 개인 키를 사용하여 상기 암호화된 데이터를 해독하고;

그 후에 상기 디바이스가 상기 데이터에 대한 지식을 가지고 있다는 것을 상기 네트워크 엔티티에 입증함으로써 수행되는, 디바이스.

청구항 19

제 15 항에 있어서,

상기 디바이스로부터 상기 네트워크 엔티티로 어태치 요청을 전송하는 것을 더 포함하며, 상기 어태치 요청은 상기 디바이스가 디바이스 인증의 능력이 있다는 표시를 포함하는, 디바이스.

청구항 20

제 15 항에 있어서,

상기 디바이스 인증은 상기 가입자 인증 동안 생성된 적어도 하나의 키에 의해 안전하게 보호되는, 디바이스.

청구항 21

제 15 항에 있어서,

상기 가입자 인증 및 상기 디바이스 인증은 가입자 인증 및 디바이스 인증이 결합된, 결합된 메시지 교환들에서 동시에 수행되는, 디바이스.

청구항 22

제 15 항에 있어서,

상기 가입자 인증은 초기의 그리고 상기 디바이스 인증과는 별도의 보안 교환에서 수행되는, 디바이스.

청구항 23

제 15 항에 있어서,

상기 보안 키는 획득된 상기 가입자 인증으로부터 적어도 제 1 키 및 상기 디바이스 인증으로부터 획득된 제 2 키의 함수로서 생성되는, 디바이스.

청구항 24

제 15 항에 있어서,

상기 디바이스는, 상기 네트워크 엔티티에 대한 액세스 단말로서 나타나고 하나 이상의 액세스 단말들에 대한 네트워크 디바이스로서 나타나는 릴레이 노드인, 디바이스.

청구항 25

제 15 항에 있어서,

상기 프로세싱 회로에 결합되고 상기 가입자 인증을 위해 사용되는 가입자-특정 키를 저장하는 착탈식 저장 디바이스; 및

상기 프로세싱 회로에 결합되고 상기 디바이스 인증을 위해 사용된 디바이스-특정 키를 저장하는 보안성 저장 디바이스를 더 포함하는, 디바이스.

청구항 26

디바이스로서,

가입자 인증 키에 기초하여 네트워크 엔티티와의 가입자 인증을 수행하기 위한 수단;

디바이스 인증 데이터를 획득하기 위하여 상기 네트워크 엔티티와의 상기 디바이스의 디바이스 인증을 수행하기 위한 수단으로서, 상기 디바이스 인증 데이터는 디바이스 아이덴티티 혹은 크리덴셜, 그리고 상기 디바이스에 의해 수신된 도전(challenge)에 기초하여 획득되는, 상기 디바이스 인증을 수행하기 위한 수단;

상기 가입자 인증 키 및 상기 디바이스 인증 데이터에 기초하여 상기 가입자 인증과 상기 디바이스 인증을 바인딩하는 보안 키를 생성하기 위한 수단;

상기 보안 키를 사용하여 상기 디바이스와 서빙 네트워크 사이의 통신을 안전하게 보호하기 위한 수단을 포함하는, 디바이스.

청구항 27

제 26 항에 있어서,

상기 가입자 인증을 위하여 사용되는 가입자-특정 키를 저장하기 위한 수단; 및

상기 디바이스 인증을 위하여 사용되는 디바이스-특정 키를 저장하기 위한 수단을 더 포함하는, 디바이스.

청구항 28

디바이스 상에서 동작하는 명령들을 포함한 컴퓨터 판독가능한 저장 매체로서,

상기 명령들은, 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

가입자 인증 키에 기초하여 네트워크 엔티티와의 가입자 인증을 수행하고;

디바이스 인증 데이터를 획득하기 위하여 상기 네트워크 엔티티와의 상기 디바이스의 디바이스 인증을 수행하되, 상기 디바이스 인증 데이터는 디바이스 아이덴티티 혹은 크리덴셜, 그리고 상기 디바이스에 의해 수신된 도전(challenge)에 기초하여 획득되고;

상기 가입자 인증 키 및 상기 디바이스 인증 데이터에 기초하여 상기 가입자 인증과 상기 디바이스 인증을 바인딩하는 보안 키를 생성하고;

상기 보안 키를 사용하여 상기 디바이스와 서빙 네트워크 사이의 통신을 안전하게 보호하도록 하는, 컴퓨터 판독가능한 저장 매체.

청구항 29

네트워크 엔티티에서 동작하는 방법으로서,

가입자 인증 키에 기초하여 디바이스와의 가입자 인증을 수행하는 단계;

디바이스 인증 데이터를 획득하기 위하여 상기 디바이스의 디바이스 인증을 수행하는 단계로서, 상기 디바이스 인증 데이터는 디바이스 아이덴티티 혹은 크리덴셜, 그리고 상기 디바이스로 송신된 도전(challenge)에 기초하여 획득되는, 상기 디바이스 인증을 수행하는 단계;

상기 가입자 인증 키 및 상기 디바이스 인증 데이터에 기초하여 상기 가입자 인증과 상기 디바이스 인증을 바인

딩하는 보안 키를 생성하는 단계; 및

상기 보안 키를 사용하여 상기 네트워크 엔티티와 상기 디바이스 사이의 통신을 안전하게 보호하는 단계를 포함하는, 네트워크 엔티티에서 동작하는 방법.

청구항 30

삭제

청구항 31

삭제

청구항 32

제 29 항에 있어서,

상기 디바이스 인증은,

상기 디바이스로부터 인증서를 수신하는 단계;

상기 디바이스와 연관된 상기 인증서가 취소되지 않았다는 것을 확인하는 단계를 포함하는, 방법.

청구항 33

제 29 항에 있어서,

상기 디바이스로부터 어태치 요청을 수신하는 단계를 더 포함하며, 상기 어태치 요청은 상기 디바이스가 디바이스 인증의 능력이 있다는 표시를 포함하는, 방법.

청구항 34

제 29 항에 있어서,

상기 디바이스 인증은 상기 가입자 인증 동안 생성된 적어도 하나의 키에 의해 안전하게 보호되는, 방법.

청구항 35

제 29 항에 있어서,

상기 가입자 인증 및 상기 디바이스 인증은 가입자 인증 및 디바이스 인증이 결합된, 결합된 메시지 교환들에서 동시에 수행되는, 방법.

청구항 36

제 29 항에 있어서,

상기 가입자 인증은 초기의 그리고 상기 디바이스 인증과는 별도의 보안 교환에서 수행되는, 방법.

청구항 37

제 29 항에 있어서,

상기 보안 키는 적어도 상기 가입자 인증으로부터 획득된 제 1 키 및 상기 디바이스 인증으로부터 획득된 제 2 키의 함수로서 생성되는, 방법.

청구항 38

제 29 항에 있어서,

상기 보안 키는 상기 디바이스 및 상기 네트워크 엔티티에 의해 별도로 생성되는, 방법.

청구항 39

제 29 항에 있어서,

서비스 합의의 일부로서 가입자-특정 키를 획득하는 단계로서, 상기 가입자-특정 키는 상기 가입자 인증을 위하여 사용되는, 상기 가입자-특정 키를 획득하는 단계; 및

상기 디바이스에 대한 디바이스-특정 키를 획득하는 단계로서, 상기 디바이스-특정 키는 상기 디바이스 인증을 위하여 사용되는, 상기 디바이스-특정 키를 획득하는 단계를 더 포함하는, 방법.

청구항 40

네트워크 엔티티로서,

통신 인터페이스; 및

상기 통신 인터페이스에 결합된 프로세싱 회로를 포함하며,

상기 프로세싱 회로는,

가입자 인증 키에 기초하여 디바이스와의 가입자 인증을 수행하고;

디바이스 인증 데이터를 획득하기 위하여 상기 디바이스와의 디바이스 인증을 수행하되, 상기 디바이스 인증 데이터는 디바이스 아이덴티티 혹은 크리덴셜, 그리고 상기 디바이스로 송신된 도전(challenge)에 기초하여 획득되고;

상기 가입자 인증 키 및 상기 디바이스 인증 데이터에 기초하여 상기 가입자 인증과 상기 디바이스 인증을 바인딩하는 보안 키를 생성하고;

상기 보안 키를 사용하여 상기 네트워크 엔티티와 상기 디바이스 사이의 통신을 안전하게 보호하도록 구성된, 네트워크 엔티티.

청구항 41

삭제

청구항 42

삭제

청구항 43

제 40 항에 있어서,

상기 프로세싱 회로는, 추가로,

상기 디바이스로부터 어태치 요청을 수신하도록 구성되며, 상기 어태치 요청은 상기 디바이스가 디바이스 인증의 능력이 있다는 표시를 포함하는, 네트워크 엔티티.

청구항 44

제 40 항에 있어서,

상기 디바이스 인증은 상기 가입자 인증 동안 생성된 적어도 하나의 키에 의해 안전하게 보호되는, 네트워크 엔티티.

청구항 45

제 40 항에 있어서,

상기 가입자 인증 및 상기 디바이스 인증은 가입자 인증 및 디바이스 인증이 결합된, 결합된 메시지 교환들에서 동시에 수행되는, 네트워크 엔티티.

청구항 46

제 40 항에 있어서,

상기 가입자 인증은 초기의 그리고 상기 디바이스 인증과는 별도의 보안 교환에서 수행되는, 네트워크 엔티티.

청구항 47

제 40 항에 있어서,

상기 보안 키는 적어도 상기 가입자 인증으로부터 획득된 제 1 키 및 상기 디바이스 인증으로부터 획득된 제 2 키의 함수로서 생성되는, 네트워크 엔티티.

청구항 48

제 40 항에 있어서,

서비스 합의의 일부로서 가입자-특정 키를 획득하는 것으로서, 상기 가입자-특정 키는 상기 가입자 인증을 위하여 사용되는, 상기 가입자-특정 키를 획득하는 것; 및

상기 디바이스에 대한 디바이스-특정 키를 획득하는 것으로서, 상기 디바이스-특정 키는 상기 디바이스 인증을 위하여 사용되는, 상기 디바이스-특정 키를 획득하는 것을 더 포함하는, 네트워크 엔티티.

청구항 49

네트워크 엔티티로서,

가입자 인증 키에 기초하여 디바이스와의 가입자 인증을 수행하기 위한 수단;

디바이스 인증 데이터를 획득하기 위하여 상기 디바이스와의 디바이스 인증을 수행하기 위한 수단으로서, 상기 디바이스 인증 데이터는 디바이스 아이덴티티 혹은 크리덴셜, 그리고 상기 디바이스로 송신된 도전(challenge)에 기초하여 획득되는, 상기 디바이스 인증을 수행하기 위한 수단;

상기 가입자 인증 키 및 상기 디바이스 인증 데이터에 기초하여 상기 가입자 인증과 상기 디바이스 인증을 바인딩하는 보안 키를 생성하기 위한 수단; 및

상기 보안 키를 사용하여 상기 네트워크 엔티티와 상기 디바이스 사이의 통신을 안전하게 보호하기 위한 수단을 포함하는, 네트워크 엔티티.

청구항 50

네트워크 엔티티 상에서 동작하는 명령들을 포함하는 컴퓨터 판독가능한 저장 매체로서,

상기 명령들은, 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

가입자 인증 키에 기초하여 디바이스와의 가입자 인증을 수행하고;

디바이스 인증 데이터를 획득하기 위하여 상기 디바이스의 디바이스 인증을 수행하되, 상기 디바이스 인증 데이터는 디바이스 아이덴티티 혹은 크리덴셜, 그리고 상기 디바이스로 송신된 도전(challenge)에 기초하여 획득되고;

상기 가입자 인증 키 및 상기 디바이스 인증 데이터에 기초하여 상기 가입자 인증과 상기 디바이스 인증을 바인딩하는 보안 키를 생성하고;

상기 보안 키를 사용하여 상기 네트워크 엔티티와 상기 디바이스 사이의 통신을 안전하게 보호하도록 하는, 컴퓨터 판독가능한 저장 매체.

청구항 51

제 1 항에 있어서,

상기 디바이스 인증 데이터는 디바이스 임시 키, 네트워크 난스(nonce) 및 디바이스 난스로부터 유래된 암호화된 파라미터를 포함하는, 방법.

청구항 52

제 15 항에 있어서,

상기 디바이스 인증 데이터는 디바이스 임시 키, 네트워크 난스 및 디바이스 난스로부터 유래된 암호화된 파라

미터를 포함하는, 디바이스.

청구항 53

제 26 항에 있어서,

상기 디바이스 인증 데이터는 디바이스 임시 키, 네트워크 난스 및 디바이스 난스로부터 유래된 암호화된 파라미터를 포함하는, 디바이스.

청구항 54

제 28 항에 있어서,

상기 디바이스 인증 데이터는 디바이스 임시 키, 네트워크 난스 및 디바이스 난스로부터 유래된 암호화된 파라미터를 포함하는, 컴퓨터 판독 가능한 저장 매체.

청구항 55

제 29 항에 있어서,

상기 디바이스 인증 데이터는 디바이스 임시 키, 네트워크 난스 및 디바이스 난스로부터 유래된 암호화된 파라미터를 포함하는, 네트워크 엔티티에서 동작하는 방법.

청구항 56

제 40 항에 있어서,

상기 디바이스 인증 데이터는 디바이스 임시 키, 네트워크 난스 및 디바이스 난스로부터 유래된 암호화된 파라미터를 포함하는, 네트워크 엔티티.

청구항 57

제 49 항에 있어서,

상기 디바이스 인증 데이터는 디바이스 임시 키, 네트워크 난스 및 디바이스 난스로부터 유래된 암호화된 파라미터를 포함하는, 네트워크 엔티티.

청구항 58

제 50 항에 있어서,

상기 디바이스 인증 데이터는 디바이스 임시 키, 네트워크 난스 및 디바이스 난스로부터 유래된 암호화된 파라미터를 포함하는, 컴퓨터 판독가능한 저장 매체.

발명의 설명

기 술 분 야

[0001] **35 U.S.C. §119 하에서의 우선권 주장**

[0002] 본 특허 출원은, 2010 년 6 월 16 일에 출원되고 발명의 명칭이 "Apparatus and Method for Device Authentication in 3GPP Systems" 이며 본원의 양수인에게 양도되고 여기에서 참조로서 명백히 통합된 미국 가출원 번호 제 61/355,423 호에 대해 우선권을 청구한다.

[0003] **분야**

[0004] 다양한 피쳐들은 통신 시스템들에 관한 것이며, 특히, 유선 및/또는 무선 통신 시스템에서 채용된 릴레이 노드들 및 머신 투 머신 디바이스들과 같은 디바이스들의 인증에 관한 것이다.

배 경 기 술

[0005] 현대의 무선 네트워크들은 본원에서 디바이스들이라고 통칭되는 릴레이 노드들 및/또는 액세스 단말들을 포함할 수도 있다. 그러한 디바이스가 적절하게 기능하기 위해서, 이 디바이스가 동작을 시작하기 전에 디바이스는

종종 운영 및 가입자 보안 크리덴셜들을 제공받거나/운영 및 가입자 보안 크리덴셜들로 구성된다. 그러한 가입자 보안 크리덴셜들은, 예를 들면, 무선 서비스 또는 액세스를 제공하기 전에 디바이스를 인증하기 위하여 사용될 수도 있고, 일부 경우들에서는, 그 호스트 디바이스에 착탈 불가하게 결합되는 모듈 내에 저장될 수도 있다. 가입자 보안 크리덴셜들이 인증된 디바이스로부터 제거되고 비인가된 디바이스에 배치될 수도 있는 리스크가 존재한다. 릴레이 노드의 경우에서, 이것은 비인가된 릴레이 노드가, 예를 들면, 하나의 액세스 노드와 하나 이상의 액세스 단말들 사이의 송신들을 몰래 액세스하고/하거나 네트워크 서비스들에 대한 자유로운 액세스를 획득할 수 있도록 할 수도 있다. 이 리스크 또는 취약성은 자유로운 네트워크 액세스를 획득하기 위하여 M2M 디바이스 내의 유효 가입자 크리덴셜들 (예를 들면, 착탈식 유니버셜 집적 회로 카드 (UICC) 내의 인증 및 키 합의 (Authentication Key Agreement exchange: AKA) 파라미터들) 이 다른 디바이스로 전송될 수 있는 머신 투 머신 (M2M) 디바이스들의 경우에도 존재한다. M2M 디바이스 자체에 물리적 액세스를 할 필요가 없다는 관련된 취약성이 존재한다. M2M 디바이스 인터페이스 (예를 들면, UICC 인터페이스에 대한 호스트 디바이스) 를 가로질러 이루어질 데이터로의 액세스 (예를 들면, 인증의 결과로 초래되는 보안 키들) 는 보안 키들로의 액세스를 얻고 상기 키들에 의해 안전하게 보호된 데이터를 노출하기에 충분하다.

[0006] 오퍼레이터가 어느 디바이스들이 그들의 네트워크에 액세스하도록 허용할 것인가를 제어하기를 원하는 경우에 유사한 이슈가 존재한다.

[0007] 따라서, 이러한 그리고 다른 취약점들과 리스크들을 다루기 위하여 디바이스들에 대한 부가적인 보안을 제공할 필요가 있다.

발명의 내용

과제의 해결 수단

[0008] 보안 키를 생성하기 위하여 가입자 인증과 디바이스 인증을 바인딩 (binding) 함으로써 디바이스를 안전하게 보호하는 방법 및 장치가 제공된다.

[0009] 제 1 양태에 따르면, 가입자 인증과 디바이스 인증을 바인딩하는, 디바이스 에서 동작하는 방법이 제공된다. 디바이스는 어태치 (attach) 요청을 네트워크 엔티티에 전송함으로써 시작할 수도 있고, 어태치 요청은 디바이스의 디바이스 인증 능력들의 표시를 포함한다. 가입자 인증은 디바이스에 의해 네트워크 엔티티와 수행될 수도 있다. 예를 들면, 가입자 인증은 디바이스와 네트워크 엔티티 사이의 인증 키 합의 교환에 기초할 수도 있다. 디바이스는 또한 네트워크 엔티티와의 디바이스 인증을 수행할 수도 있다. 예를 들면, 디바이스 인증은 디바이스와 네트워크 엔티티 사이의 도전-응답 교환에 기초할 수도 있다.

[0010] 그런 다음, 가입자 인증과 디바이스 인증을 바인딩하는 보안 키가 생성될 수도 있다. 보안 키는 가입자 인증으로부터 획득된 적어도 제 1 키와 디바이스 인증으로부터 획득된 제 2 키의 함수로서 생성될 수도 있다. 부가적으로, 보안 키는 또한 네트워크 난스 (nonce) 와 디바이스 난스의 함수일 수도 있다. 그런 다음, 보안 키는 디바이스와 서빙 네트워크 사이의 통신을 안전하게 보호하기 위하여 사용될 수도 있다. 보안 키는 디바이스 및 네트워크 엔티티에 의해 별도로 생성될 수도 있으며, 그래서 에어를 통해서 송신되지는 않는다는 것에 유의한다.

[0011] 일 구현에 따르면, 가입자 인증은 네트워크 엔티티의 일부인 제 1 인증 서버에 의해 수행될 수도 있고, 디바이스 인증은 네트워크 엔티티의 일부인 제 2 인증 서버에 의해 수행될 수도 있다.

[0012] 일 예에서, 디바이스 인증은 디바이스와 네트워크 엔티티 사이의 일정한 교환들을 암호화/해독하기 위하여 공유된 비밀 키를 사용하여 수행될 수도 있다. 다른 예에서, 디바이스 인증은 (a) 네트워크 엔티티로부터 디바이스의 공개 키를 이용하여 암호화된 데이터를 수신하는 단계; (b) 암호화된 데이터를 해독하기 위하여 대응하는 개인 키를 사용하는 단계; 및/또는 (c) 그 후에 디바이스가 데이터에 대한 지식을 가지고 있다는 것을 네트워크 엔티티에 입증하는 단계에 의해 수행될 수도 있다.

[0013] 일 양태에 따라서, 디바이스 인증은 가입자 인증 동안 생성된 적어도 하나의 키에 의해 안전하게 보호될 수도 있다.

[0014] 다양한 구현들에서, 가입자 인증 및 디바이스 인증은 결합된 메시지 교환들에서 동시에 수행될 수도 있거나 또는 가입자 인증은 초기의 그리고 디바이스 인증과는 별도의 보안 교환에서 수행될 수도 있다.

[0015] 일 피쳐에 따르면, 가입자-특정 키는 서비스 합의의 일부로서 디바이스상에 제공될 수도 있으며, 여기서 가입

자-특정 키는 가입자 인증을 위해 사용된다. 마찬가지로, 디바이스-특정 키는 제조 동안에 디바이스내에 제공될 수도 있으며, 여기서 디바이스-특정 키는 디바이스 인증을 위해 사용된다.

[0016] 일 구현에서, 디바이스는 네트워크 엔티티에 대한 액세스 단말로서 나타나고 하나 이상의 액세스 단말들에 대한 네트워크 디바이스로서 나타나는 릴레이 노드일 수도 있다. 다른 구현에서, 디바이스는 액세스 단말일 수도 있다.

[0017] 일 예에 따라서, 디바이스는 프로세싱 회로에 결합된 통신 인터페이스를 포함할 수도 있다. 프로세싱 회로는 (a) 네트워크 엔티티와의 가입자 인증을 수행하고; (b) 네트워크 엔티티와의 디바이스의 디바이스 인증을 수행하고; (c) 가입자 인증과 디바이스 인증을 바인딩하는 보안 키를 생성하고; 그리고/또는 (d) 디바이스와 서빙 네트워크 사이의 통신을 안전하게 보호하기 위하여 보안 키를 사용하도록 적응될 수도 있다.

[0018] 다른 예에 따라서, 디바이스상에서 동작하는 명령들을 포함하는 프로세서 판독가능 매체가 제공될 수도 있다. 프로세서에 의해 실행되면, 이 명령들은 프로세서로 하여금: (a) 네트워크 엔티티와의 가입자 인증을 수행하고; (b) 네트워크 엔티티와의 디바이스의 디바이스 인증을 수행하고; (c) 가입자 인증과 디바이스 인증을 바인딩하는 보안 키를 생성하고; 그리고/또는 (d) 디바이스와 서빙 네트워크 사이의 통신을 안전하게 보호하기 위하여 보안 키를 사용하도록 할 수도 있다.

[0019] 다른 양태에 따라서, 네트워크 엔티티에서 동작하는 방법이 제공된다. 네트워크 엔티티는 디바이스로부터 어태치 요청을 수신할 수도 있으며, 어태치 요청은 디바이스의 디바이스 인증 능력들의 표시를 포함한다. 네트워크 엔티티는 디바이스를 이용하여 가입자 인증을 수행할 수도 있다. 마찬가지로, 네트워크 엔티티는 디바이스의 디바이스 인증을 수행할 수도 있다. 그런 다음 보안 키는 가입자 인증과 디바이스 인증을 바인딩하는 네트워크 엔티티에 의해 생성될 수도 있다. 그런 다음 보안 키는 네트워크 엔티티와 디바이스 사이의 통신을 안전하게 보호하기 위하여 사용될 수도 있다. 보안 키의 오버 디 에어 송신 (over the air transmission) 을 방지하기 위하여, 보안 키는 디바이스와 네트워크 엔티티에 의해 별도로 생성될 수도 있다는 것에 유의한다.

[0020] 일 예에서, 가입자 인증은 네트워크 엔티티와 디바이스 사이의 인증 키 합의 교환에 기초할 수도 있다. 디바이스 인증은 네트워크 엔티티와 디바이스 사이의 도전-응답 교환에 기초할 수도 있다.

[0021] 일 구현에서, 디바이스 인증은: (a) 디바이스로부터 인증서를 수신하는 단계; 및 (b) 디바이스와 연관된 인증서가 취소되지 않았다는 것을 확인하는 단계를 포함할 수도 있다.

[0022] 일 구현에서, 디바이스 인증 프로세스 동안 스누핑 (snooping) 을 방지하기 위하여, 디바이스 인증은 초기 가입자 인증 동안 생성된 적어도 하나의 키에 의해 안전하게 보호될 수도 있다.

[0023] 다양한 예들에 따라서, 가입자 인증 및 디바이스 인증은 결합된 메시지 교환들에서 동시에 수행될 수도 있거나 또는 인증은 초기의 그리고 디바이스 인증과는 별도의 보안 교환에서 수행된다.

[0024] 다른 예에서, 보안 키는 적어도 가입자 인증으로부터 획득한 제 1 키 및 디바이스 인증으로부터 획득한 제 2 키의 함수로서 생성될 수도 있다.

[0025] 일 구현에서, 네트워크 엔티티는 서비스 합의의 일부로서 가입자-특정 키를 획득할 수도 있으며, 가입자-특정 키는 가입자 인증을 위해 사용된다. 마찬가지로, 네트워크 엔티티는 디바이스에 대한 디바이스-특정 키를 획득할 수도 있으며, 디바이스-특정 키는 디바이스 인증을 위해 사용된다.

[0026] 일 구현에서, 네트워크 엔티티는 프로세싱 회로에 결합된 통신 인터페이스를 포함할 수도 있다. 프로세싱 회로는 (a) 디바이스를 이용하여 가입자 인증을 수행하고; (b) 디바이스의 디바이스 인증을 수행하고; (c) 가입자 인증과 디바이스 인증을 바인딩하는 보안 키를 생성하고; 그리고/또는 (d) 네트워크 엔티티와 디바이스 사이의 통신을 안전하게 보호하기 위하여 보안 키를 사용하도록 적응될 수도 있다.

[0027] 일 구현에서, 네트워크 엔티티상에서 동작하는 명령들을 포함하는 프로세서 판독가능 매체가 제공된다. 프로세서에 의해 실행되면, 이 명령들은 프로세서로 하여금: (a) 디바이스를 이용하여 가입자 인증을 수행하고; (b) 디바이스의 디바이스 인증을 수행하고; (c) 가입자 인증과 디바이스 인증을 바인딩하는 보안 키를 생성하고; 그리고/또는 (d) 네트워크 엔티티와 디바이스 사이의 통신을 안전하게 보호하기 위하여 보안 키를 사용하도록 할 수도 있다.

도면의 간단한 설명

[0028] 도 1 은 서비스를 획득하기 위하여 무선 디바이스들의 다양한 유형들이 코어 네트워크에 의해 인증될 수도 있는 무선 통신 시스템을 도시하는 블록도이다.

도 2 는 디바이스 인증과 가입자 인증을 바인딩하는 것에 대한 일반적인 접근법을 도시한다.

(도 3a 및 도 3b 를 포함하는) 도 3 은 디바이스 인증을 부가하기 위하여 가입자 인증에 기초한 키 계층구조가 어떻게 수정될 수도 있는 지에 대한 예를 도시한다.

도 4 는 패킷-스위칭된 네트워크에서 동작하는 디바이스에서 구현될 수도 있는 예시적인 프로토콜 스택 (stack) 을 도시한다.

도 5 는 도 3 및 도 4 에서 도시된 다양한 인증 및/또는 보안 키들이 생성될 수도 있는 네트워크 시스템을 도시한 블록도이다.

도 6 은 가입자 인증과 디바이스 인증을 바인딩하기 위하여 적응될 수도 있는 무선 디바이스의 선택 컴포넌트들을 도시한 블록도이다.

도 7 은 가입자 인증과 디바이스 인증을 바인딩하는 보안 키를 생성하기 위하여 무선 디바이스에서 동작하는 방법의 예를 도시한 플로우 다이어그램이다.

도 8 은 가입자 인증과 디바이스 인증을 바인딩하기 위하여 적응될 수도 있는 네트워크 엔티티의 선택 컴포넌트들을 도시한 블록도이다.

도 9 는 가입자 인증과 디바이스 인증을 바인딩하는 보안 키를 생성하기 위하여 네트워크 엔티티에서 동작하는 방법의 예를 도시한 플로우 다이어그램이다.

도 10 은 가입자 인증과 디바이스 인증을 바인딩함으로써 보안 키를 생성하는 제 1 예시적인 방법을 도시한다.

도 11 은 가입자 인증과 디바이스 인증을 바인딩함으로써 보안 키를 생성하는 제 2 예시적인 방법을 도시한다.

도 12 는 가입자 인증과 디바이스 인증을 바인딩함으로써 보안 키를 생성하는 제 3 예시적인 방법을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0029] 아래의 설명에서, 설명된 구현들의 철저한 이해를 제공하기 위하여 특정 세부사항들이 주어진다. 그러나, 다양한 구현들이 이 특정 세부사항들 없이 실행될 수도 있다는 것이 이 기술분야에서 통상의 기술을 가진 자에 의해 이해될 것이다. 예를 들면, 불필요한 세부사항에서 구현들을 모호하게 하지 않도록 회로들은 블록도들로 도시될 수도 있다. 다른 인스턴스들에서, 설명된 구현들을 모호하게 하지 않도록 주지의 회로들, 구조들 및 기법들이 상세하게 도시될 수도 있다.

[0030] 본원에서 단어 "예시적인 (exemplary)" 은 "예, 인스턴스 또는 예시로서 사용되는" 을 의미하기 위하여 사용된다. 본원에서 "예시적인" 으로서 설명된 임의의 구현 또는 실시형태는 반드시 다른 실시형태들 또는 구현들에 대하여 선호되거나 이점을 가지는 것으로 해석되는 것은 아니다. 비슷하게, 용어 "실시형태들 (embodiments)" 은 모든 실시형태들이 논의된 피쳐, 이점 또는 동작의 모드를 포함할 것을 요구하지 않는다.

[0031] **개요**

[0032] 디바이스 (예를 들면, 클라이언트 디바이스 또는 액세스 단말) 와 네트워크 엔티티 사이에 인증 방법이 제공된다. 착탈식 저장 디바이스는 디바이스에 결합될 수도 있으며, 가입자 인증을 위해 사용될 수도 있는 가입자 특정 키를 저장한다. 보안성 저장 디바이스는 디바이스에 결합될 수도 있으며, 디바이스 인증을 위해 사용되는 디바이스 특정 키를 저장한다. 가입자 인증은 디바이스와 네트워크 엔티티 사이에서 수행될 수도 있다. 디바이스의 디바이스 인증은 또한 네트워크 엔티티와 수행될 수도 있다. 그런 다음, 가입자 인증과 디바이스 인증을 바인딩하는 보안 키가 생성될 수도 있다. 즉, (복합) 보안 키를 생성하기 위하여 가입자 인증으로부터의 키, 데이터 및/또는 정보 및 디바이스 인증으로부터의 키, 데이터 및/또는 정보는 결합될 수도 있다. 보안 키는 디바이스와 서빙 네트워크 사이의 통신을 안전하게 보호하기 위하여 사용될 수도 있다.

[0033] **예시적인 네트워크 환경**

[0034] 도 1 은 서비스를 획득하기 위하여 무선 디바이스들의 다양한 유형들이 코어 네트워크에 의해 인증될 수도 있는 무선 통신 시스템을 도시한 블록도이다. 이 무선 통신 시스템은, 예를 들면, 유니버셜 모바일 통신 시스템 (UMTS) 준수 네트워크 또는 호환 네트워크 또는 GSM 준수 네트워크 또는 GSM 호환 네트워크일 수도 있다. 본원에서 설명된 예들의 일부가 롱 텀 에볼루션 (LTE) 네트워크와 관련되지만, 본원에서 설명되는 다양한 피쳐들은 다른 네트워크들에서도 역시 구현될 수도 있다.

[0035] 시스템은 액세스 노드 (106) 와 통신하는 액세스 단말들 (103/104) 및 릴레이 노드 (102) 와 같은 하나 이상의 디바이스들 (101) 을 포함할 수도 있다. 릴레이 노드 (102) 는 무선 통신 네트워크 (106/108) 와 하나 이상의 액세스 단말들 (104) 사이의 무선 송신들을 용이하게 할 수도 있다. 무선 통신 시스템 (예를 들면, 롱 텀 에볼루션 (LTE) 네트워크, LTE-어드밴스드 네트워크 등) 은 코어 네트워크 (108) 및 하나 이상의 액세스 노드들 (106) 을 포함할 수도 있다. 액세스 노드 (106) 는 백홀 링크 (예를 들면 유선 커넥션) 를 통하여 코어 네트워크 (108) 에 결합될 수 있다. 코어 네트워크 (108) 는, 예를 들면 모바일 관리 엔티티들 (MME) (110), 홈 가입자 서버 (HSS) (112) 및/또는 다른 컴포넌트들을 포함할 수도 있다.

[0036] 일 예에서, 모바일 관리 엔티티 (MME) (110) 는 (본원에서 총칭하여 "디바이스" 라고 불리는) 디바이스 (101), 릴레이 노드 (102) 및/또는 액세스 단말들 (103/104) 에 대한 베어러 활성화/비활성화 및 홈 가입자 서버 (HSS) (112) 와의 상호작용에 의한 인증 보조에 관련될 수도 있다. MME (110) 는 또한 임시 아이덴티티들을 생성하고 및/또는 디바이스들 (예를 들면 디바이스 (101), 릴레이 노드 (102), 액세스 단말들 (103/104) 등) 에 할당할 수도 있다. 그것은 서비스 제공자의 공중 육상 이동 네트워크 (PLMN) 에 캠핑하기 위하여 (예를 들면, 이 네트워크로부터 서비스를 획득하기 위하여, 이 네트워크에 연결하기 위하여, 이 네트워크와의 통신 링크를 설정하기 위하여) 디바이스의 인증을 점검할 수도 있고, 디바이스의 로밍 제약들을 강요할 수도 있다. MME (110) 는 비 액세스 계층 (Non Access Stratum; NAS) 시그널링에 대한 암호화/무결성 보호를 위한 네트워크 내의 종단 포인트일 수도 있으며 보안 키 관리를 핸들링한다. MME (110) 는 또한 코어 네트워크 (108) 에 결합된 디바이스들에 대한 트랙 및/또는 (재전송들을 포함한) 페이징 프로시저들을 수행할 수도 있다.

[0037] 홈 가입자 서버 (HSS) (112) 는 디바이스들을 실제로 핸들링하는 네트워크 엔티티들을 지원하는 마스터 가입자 데이터베이스이다. 그것은 가입자-관련 정보 (가입자 프로파일들) 를 포함할 수도 있고, 가입의 인증 및 인가를 도울 수도 있으며, 가입자의 로케이션에 관한 정보를 제공할 수 있다. 그것은 GSM 홈 로케이션 레지스터 (HLR) 및 인증 센터 (AuC) 와 유사하다. 홈 로케이션 레지스터 (HLR) 는 코어 네트워크를 사용하도록 인가된 각각의 가입자의 세부사항들을 포함하는 데이터베이스일 수도 있다. HLR 은 가입자들을 인증함에 있어서 (즉, 사용자 단말들을 사용함에 있어서) AuC 를 보조할 수도 있다.

[0038] 릴레이 노드 (102) 는 액세스 단말 (104) 과 액세스 노드 (106) 사이에서의 신호를 증폭 및/또는 반복하도록 적응될 수도 있다. 일반적으로, 릴레이 노드 (102) 는 액세스 노드 (AN) 로서 액세스 단말 (104) 에 나타날 수 있고 액세스 단말 (AT) 로서 액세스 노드 (106) 에 나타날 수 있다. 예를 들면, 릴레이 노드 (102) 는 액세스 노드 (106) 와의 통신에 사용하는 액세스 단말 인터페이스 (105) 를 포함할 수도 있고, 또한 액세스 단말 (104) 과의 통신에 사용하는 액세스 노드 인터페이스 (107) 를 포함할 수도 있다. 즉, 액세스 단말 인터페이스 (105) 는 릴레이 노드가 액세스 노드 (106) 에 액세스 단말로서 나타나도록 만들수도 있다. 마찬가지로, 액세스 노드 인터페이스 (107) 는 릴레이 노드 (102) 가 액세스 단말 (104) 에 액세스 노드로서 나타나도록 만들 수도 있다. 일부 구현들에서, 릴레이 노드 (102) 는 액세스 단말 인터페이스 (105) 와 액세스 노드 인터페이스 (107) 사이에서 제 1 포맷으로부터 제 2 포맷으로 신호들을 변환할 수도 있다. 릴레이 노드 (102) 는 액세스 단말 (104) 이 액세스 노드 (106) 와 직접적으로 통신하기보다는 릴레이 노드 (102) 와 통신할 수 있도록 셀의 에지들 가까이에 배치될 수도 있다.

[0039] 무선 시스템들에서, 셀은 수신 및 송신 커버리지 (coverage) 의 지리학적 영역이다. 셀들은 서로 중첩될 수 있다. 전형적인 에에서, 각각의 셀과 연관된 하나의 액세스 노드가 있다. 셀의 사이즈는 주파수 대역, 파워 레벨 및 채널 조건들과 같은 팩터들에 의해 결정된다. 릴레이 노드 (102) 와 같은 릴레이 노드들은 셀 내에서 또는 셀 가까이에서 커버리지를 향상시키기 위하여, 또는 셀의 커버리지의 사이즈를 확장하기 위하여 사용될 수 있다. 부가적으로, 릴레이 노드 (102) 의 사용은 셀 내에서 신호의 스루풋 (throughput) 을 향상시킬 수 있는데 이것은 액세스 단말 (104) 이 그 셀에 대하여 액세스 노드 (106) 와 직접적으로 통신할 때 사용할 수도 있는 데이터 레이트보다 더 높은 데이터 레이트로 또는 액세스 단말 (104) 이 그 셀에 대하여 액세스 노드 (106) 와 직접적으로 통신할 때 사용할 수도 있는 송신 파워보다 더 낮은 송신 파워로 릴레이 노드 (102) 를 액세스할 수 있기 때문이다. 더 높은 데이터 레이트에서의 송신은 더 높은 스펙트럼 효율을 발생시키고 예를

들면, 더 적은 배터리 파워를 소모함으로써 액세스 단말 (104) 이 낮은 파워의 혜택들을 받도록 한다.

[0040] 일부 예들에서, 릴레이 노드 (102) 는 계층 1 릴레이 노드, 계층 2 릴레이 노드 및/또는 계층 3 릴레이 노드의 3 개의 릴레이 유형들 중 하나로서 구현될 수 있다. 계층 1 릴레이 노드는 증폭 및 약간의 지연 외에 임의의 수정 없이 송신을 재송신할 수 있는 본질적으로 중계기 (repeater) 이다. 계층 2 릴레이 노드는 그것이 수신하는 송신을 디코딩하고, 디코딩의 결과를 재인코딩하고, 그런 다음 재인코딩된 데이터를 송신할 수 있다.

계층 3 릴레이 노드는 충분한 무선 자원 제어 능력들을 가질 수 있으며 따라서 액세스 노드와 유사하게 기능할 수 있다. 릴레이 노드에 의해 사용된 무선 자원 제어 프로토콜들은 액세스 노드에 의해 사용된 프로토콜들과 동일할 수도 있고, 릴레이 노드는 액세스 노드에 의해 전형적으로 사용되는 고유 셀 아이덴티티를 가질 수도 있다. 본 개시를 위하여, 릴레이 노드 (102) 가 전기 통신 시스템 (예를 들면, 네트워크 (108)) 에서 다른 컴포넌트들에 액세스하기 위하여 적어도 하나의 액세스 노드 (106) (및 그 액세스 노드와 연관된 셀) 또는 다른 릴레이 노드의 존재에 의존한다는 사실에 의하여, 그 릴레이 노드 (102) 는 액세스 노드 (106) 와 구별된다. 즉, 릴레이 노드 (102) 는 네트워크에 대한 가입자 디바이스, 클라이언트 디바이스 또는 액세스 단말로서 나타날 수도 있고, 그러므로 그것은 네트워크 (108) 를 통하여 통신하기 위하여 액세스 노드에 연결된다.

그러나, 다른 가입자 디바이스들, 사용자 디바이스들 및/또는 액세스 단말들 (104) 에, 릴레이 노드 (102) 는 네트워크 디바이스 (예를 들면, 액세스 노드) 로서 나타날 수도 있다. 그 결과, 액세스 노드 및/또는 하나 이상의 액세스/가입자/사용자 단말들과 통신하기 위한 다른 릴레이 노드 (102) 는 하나 이상의 통신 인터페이스들을 구현할 수도 있다. 일 예에서, 그것의 액세스 노드 및/또는 하나 이상의 액세스 단말들과 통신하기 위하여 (예를 들면, 하나 이상의 무선 채널들에서) 동일한 송신기/수신기가 릴레이 노드 (102) 에 의해 사용될 수도 있다. 다른 예에서, 릴레이 노드 (102) 는 액세스 노드 및/또는 하나 이상의 액세스 단말들과 통신하기 위하여 2 개 이상의 상이한 송신기들/수신기들을 활용할 수도 있다.

[0041] 액세스 네트워크 서비스들로의 가입의 오용을 줄이기 위하여, 디바이스들은 디바이스 인증을 가입자 인증과 바인딩할 수도 있다. 디바이스 인증은, 예를 들면, 디바이스에 착탈 가능하게 결합된 유니버셜 집적 회로 카드 (UICC) (109, 111, 113 및 116) 또는 유니버셜 가입자 식별 모듈 (예를 들면, USIM) 에 저장된 (가입자 루트 키 (K) 와 같은) 크리덴셜들에 기초한 표준 3GPP AKA (인증 및 키 합의) 액세스 인증과 함께 작동될 수도 있다. 일부 실시형태들에서, 디바이스 인증은 AKA 인증을 위하여 사용된 동일한 비 액세스 계층 (NAS) 메시지들에서 수행될 수도 있다. 이러한 방식으로, 디바이스 (예를 들면, 릴레이 노드 (102), 액세스 단말들 (103/104) 등) 는 비인가 디바이스에서 다른 디바이스들이 (즉, 가입 서비스에 대한) 그것의 가입자 크리덴셜들을 사용하는 것을 방지하기 위하여 그것의 가입 (즉, 코어 네트워크 (108) 와의 서비스 가입) 에 바인딩될 수도 있다.

[0042] 가입자 크리덴셜들의 비인가된 사용의 리스크에 대한 하나의 솔루션은 디바이스 (예를 들면, 디바이스 (101), 릴레이 노드 (102) 또는 액세스 단말들 (103/104)) 와 UICC (109) 가 (예를 들면, 호스트 디바이스와 UICC 사이에 보안 채널을 이용하여) 서로를 상호 인증하는 것이지만, 그것은 그러한 상호 인증을 수행하기 위하여 정보를 UICC (109, 111, 113 및 116) 및/또는 호스트 디바이스 (예를 들면, 디바이스 (101), 릴레이 노드 (102) 또는 액세스 단말들 (103/104)) 에 사전 제공할 것을 요구할 수도 있다.

[0043] 다른 솔루션은 네트워크 액세스를 위하여 사용된 키들 (예를 들면, 디바이스와 네트워크 사이의 트래픽을 보호하기 위하여 사용된 키들) 이 디바이스 (예를 들면, 디바이스 (101), 릴레이 노드 (102) 또는 액세스 단말들 (103/104)) 상에 저장된 크리덴셜들 뿐만 아니라 UICC (109, 111, 113 및 116) 상에 저장된 크리덴셜들 양쪽 모두에 의존할 것을 요구하는 것일 수도 있다. 이것은 어떤 방법으로든 AKA 인증 키들을 디바이스 인증과 바인딩함으로써 달성될 수도 있다. 이 솔루션은 또한 (예를 들면, 오퍼레이터가 비인가 디바이스들을 그들의 네트워크에 어태치하는 것을 중지하도록 할 수도 있는) 국제 모바일 장비 아이덴티티 (IMEI) 인증의 경우에도 유용하다. 이것은, 네트워크 액세스를 위해 사용된 AKA 인증의 결과로 초래된 키(들)를 디바이스 인증을 위해 사용된 키들과 바인딩함에 의해, 디바이스로부터 네트워크 (108) 로 비롯된 메시지들의 모두가 인증된 디바이스로부터 사실상 비롯되었다는 것이 확인되기 때문이다. 바인딩된 키들 (및 바인딩된 키로부터 유래한 모든 다른 후속 키들) 이 디바이스 (예를 들면, 디바이스 (101), 릴레이 노드 (102) 또는 액세스 단말들 (103/104)) 상에 안전하게 저장된다는 가정 하에, AKA 인증으로부터의 키들을 디바이스 인증과 바인딩하는 것은 디바이스 인증을 위하여 도전/응답 기반 메카니즘을 단독으로 사용하는 것보다 더 강력한 보안성을 제공한다.

디바이스 인증을 위하여 도전/응답 메카니즘을 단독으로 사용하는 것은 인증 응답을 생성하기 위하여 디바이스가 존재하였다는 것만을 입증할 뿐 그 디바이스가 후속 시간에도 여전히 존재한다는 것은 입증하지 못한다.

[0044] 도 2 는 디바이스 인증과 가입자 인증을 바인딩하는 것에 대한 일반적인 접근법을 도시한다. 디바이스

(202) (예를 들면, 디바이스 (101), 릴레이 노드 (102) 또는 액세스 단말들 (103/104)) 에는 코어 네트워크 (108) 와의 가입을 인증하고/하거나 디바이스 (202) 로 전송된 암호화된 트래픽을 액세스하기 위하여 사용되는 보안 키들을 생성하기 위하여 사용될 수 있는 subscriber_root_key (206) 및/또는 subscriber_identity (207) 가 제공될 수도 있다. subscriber_root_key (206) 는 subscriber_identity (207) 와 고유하게 연관될 수도 있다. 일 예에서, subscriber_root_key (206) 및/또는 subscriber_identity (207) 는 UICC (204) 에 저장될 수도 있고/있거나 가입자 인증은 UICC (204) 에 의해 프로세싱될 수도 있다. 마찬가지로, 디바이스 (202) 는 코어 네트워크 (108) 와 디바이스를 인증하기 위하여 사용될 수 있는 device_root_key (208) 및/또는 device_identity (209) 를 제공받을 수 (또는 저장할 수) 도 있다. device_root_key (208) 는 device_identity (209) 와 고유하게 연관될 수도 있다.

[0045] 일 예에서, device_dentity (209) 는 디바이스 (202) (예를 들면, 디바이스 (101), 릴레이 노드 (102) 또는 액세스 단말들 (103/104)) 의 국제 모바일 장비 아이덴티티 (IMEI) 일 수도 있으나, 디바이스와 연관된 아이덴티티의 다른 형태들 (예를 들면, EUI-48 또는 EUI-64 와 같은 IEEE 하드웨어 어드레스) 도 또한 사용될 수도 있다.

[0046] 일부 구현들에서, device_root_key (208) 는 오직 디바이스 (202) 에 의해서만 코어 네트워크 (108) 와 공유되는 비밀 키일 수도 있으나 에어를 통해서 송신되지는 않는다. device_dentity (209) 는 디바이스 인증에 사용될 정확한 device_root_key 를 그것이 획득할 수 있도록 디바이스 (202) 에 의해 코어 네트워크 (108) 로 송신될 수도 있다. 대안적으로, device_root_key (208) 는 공개/개인 키 쌍의 공개 키일 수도 있으며, 여기서 인증서들은 디바이스 인증을 위하여 사용된다. 예를 들면, 디바이스는 네트워크로부터 일부 데이터를 수신할 수도 있으며, 여기서 데이터는 공개 키로 암호화된다. 디바이스는 그런 다음 암호화된 데이터를 해독하기 위하여 그것의 개인 키를 사용할 수도 있고, 이어서 그것이 데이터의 지식을 가지고 있다는 것을 네트워크에 입증할 수도 있다. 인증서 (예를 들면, device_credentials) 는 코어 네트워크 (108) 에 의해 확인될 수도 있다. 디바이스 (202) 의 연관된 개인 키는 디바이스 (202) 에 안전하게 저장될 수도 있다. device_credentials 는 디바이스 인증서 또는 그에 대한 포인터 중 어느 하나를 나타낼 수도 있다. 이 device_credentials 는 관련된 네트워크 엔티티가 device_challenge 를 형성하고 디바이스 (202) 의 권한 취소 상태 (revocation status) 를 점검 (예를 들면, 디바이스와 연관된 개인 키 또는 공유 키와 같은 크리덴셜들이 타협되었는지를 점검) 하도록 허용할 수도 있다. (3GPP 기술 사양 33.320 에 정의된 신뢰 환경 (Trusted Environment) 또는 TrE 와 같은) 디바이스의 보안성 부분이 인증서와 연관된 device_root_key 및/또는 개인 키와 같은 감응 디바이스 키들을 저장한다고 추가로 가정한다. 더욱이, TrE 는 이 키들을 사용하는 모든 암호화 동작들을 수행한다고 가정한다.

[0047] 처음에, 가입자 인증은 디바이스 (202) 와 네트워크 (108) 사이에서 일어날 수도 있다. 예를 들면, 디바이스 (202) 와 네트워크 (108) 사이의 인증 및 키 합의 (AKA) 교환 (210) 은 키 K_ASME 의 설정의 결과를 초래할 수도 있다. 디바이스 (202) 와 연관된 가입자를 인증하기 위하여 그러한 AKA 교환 (210) 은, 예를 들면, subscriber_root key (206) 및/또는 subscriber_identity (207) 에 기초할 수도 있다. 예를 들면, 그러한 가입 정보 또는 크리덴셜들은 호스트 디바이스 (202) 에 착탈 가능하게 결합된 UICC (204) 내에 안전하게 저장될 수도 있다.

[0048] 네트워크 (108) 는 또한 디바이스 (202) 상에 디바이스 인증을 수행할 수도 있다. 코어 네트워크 (108) 가 정확한 대응하는 device_root_key (208) 를 검색 또는 획득할 수 있도록 device_dentity (209) 는 디바이스 (202) 에 의해 코어 네트워크 (108) 에 제공될 수도 있다. 네트워크 (108) 는 device_challenge (212) 를 발생시킬 수도 있고 그것을 (관련된 NAS 메시지의 일부로서) 디바이스 (202) 에 전송한다. 이에 대응하여, 디바이스 (202) 는 (예를 들면, device_challenge 및 device_root_key (208) 또는 그것의 도함수에 기초하여) device_response (214) 를 계산하고 그것을 네트워크 (108) 에 리턴한다. 디바이스 (202) 는 device_challenge 및 device_response 내의 데이터를 사용하여 복합 보안 키 K_ASME_D (216) 를 산출할 수도 있다. 디바이스 (202) 의 경우에서, 복합 보안 키 K_ASME_D (216) 는 device_response (214) 가 전송되기 전에 또는 후에 생성될 수도 있다는 것에 유의한다. 일 예에서, 키 K_ASME_D 가 K_ASME 키와 같이 AKA 인증의 결과로 초래되는 키 뿐만 아니라 device_dentity (209) 에 바인딩된다는 것을 제외하고, 복합 보안 키 K_ASME_D 는 3GPP 기술 사양 33.401 에서 정의된 진화형 유니버셜 지상파 무선접속 네트워크 E-UTRAN (E-UTRAN) 에서 정의된 보안 키 K_ASME 와 등가의 키일 수도 있다. 네트워크 (108) 가 유효한 device_response 를 수신하면, 네트워크 (108) 는 또한 복합 보안 키 K_ASME_D (218) 를 산출한다.

[0049] device_challenge (212), device_response (214) 및 복합 보안 키 K_ASME_D 의 산출은 아래와 같을 수도 있다.

device_challenge (212) 는:

[0050] $$device_challenge = \text{eKSI}, [E_device_root_key\,(\text{device_temp_key})], network_nonce,$$

[0051] 와 같이 산출될 수도 있으며, 여기서 eKSI 는 K_ASME_D 와 연관되는 진화형/확장된 키 세트 식별자이고, [,.] 는 옵션적 파라미터를 나타내고, E_k (data) 는 키 k 로 암호화된 data 를 의미하고, network_nonce 는 네트워크에 의해 선택된 적합한 사이즈 랜덤 수 (예를 들면, 128-비트) 이다. 암호화 알고리즘은 (device_root_key 가 디바이스 인증서와 연관된 공개 키인 경우에) 비대칭적이거나 또는 (device_root_key 가 공유 키인 경우에) 대칭적일 수 있다. device_temp_key 는 디바이스 인증의 일부로서 획득 또는 생성된 키일 수도 있다. 일 예에서, device_temp_key 는 네트워크 (108) 에 의해 (예를 들면, 랜덤으로) 선택될 수도 있고, 암호화된 형태로 디바이스 (202) 에 전송되고, 적절한 길이 (예를 들면, 256 또는 128 비트값) 를 가진다.

[0052] 디바이스 (202) 와 네트워크 (108) 양쪽 모두는 최적화를 목적으로 네트워크 액세스들 사이에 device_temp_key 를 유지할 수도 있다. 이런 경우가 아니라면, device challenge (212) 내의 제 2 파라미터 ([E_device_root_key (device_temp_key)]) 는 옵션적이지 않다.

[0053] device_response (214) 는:

[0054] $$device_response = device_nonce, device_res,$$

[0055] 와 같이 산출될 수도 있으며, 여기서 device_nonce 는 디바이스에 의해 선택된 적합한 사이즈 랜덤 수 (예를 들면, 128-비트) 이고,

[0056] $$device_res = KDF\,(device_temp_key, network_nonce, device_nonce)$$

[0057] 와 같이 산출될 수도 있으며, 여기서 KDF 는 응답 device_res 를 생성하기에 적합한 암호화 함수이다.

[0058] 이전에 (예컨대, AKA 교환 (210) 의 일부로서) 인증 키 K_ASME 를 획득했다면, 복합 보안 키 K_ASME_D 의 산출 (216 및 218) (즉, 디바이스 인증과 가입자 인증의 바인딩) 은:

[0059] $$K_ASME_D = \text{KDF}\,(device_temp_key, K_ASME, network_nonce, device_nonce)$$

[0060] 와 같이 이루어질 수도 있으며, 여기서 K_ASME 는 디바이스와 네트워크 사이의 가입자 인증 동안 (AKA 인증 교환 (210) 의 결과로서) 획득된 키 또는 값일 수도 있다. 일 예에서, K_ASME 키는 디바이스 (202) 와 네트워크 (108) 사이에서 이전에 생성되고/되거나 사용된 키일 수도 있다. 대안적으로, 디바이스 인증 프로세스 (212 및 214) 가 AKA 프로시저 (210) 에 대하여 사용된 NAS 메시지들과 동일한 NAS 메시지들을 사용하여 수행되면, 키 K_ASME 는 새로이 또는 동시에 생성될 수도 있다. 마찬가지로, device_temp_key 는 디바이스 (202) 와 네트워크 (108) 사이의 디바이스 인증 동안 획득된 키 또는 값일 수도 있다.

[0061] 복합 보안 키는 그런 다음 부가적인 보안 키들을 산출하기 위한 베이시스 (basis) 및/또는 루트 (root) 로서 사용될 수도 있다 (217 및 219). 부가적인 보안 키들은, 예를 들면, NAS-레벨 및/또는 AS-레벨 통신을 안전하게 보호하도록 기능할 수도 있다.

[0062] 보안 파라미터들에 연관된 복합 보안 키 K_ASME_D 및 K_ASME_D 로부터 유래한 모든 키들은 디바이스 (202) 상에서 안전하게 유지될 수도 있으며 UICC (204) 상에는 저장되지 않는다. 복합 보안 키 K_ASME_D 는 그런 다음 디바이스 (202) 와 코어 네트워크 (108) 사이에서 교환된 (220) 메시지들을 안전하게 보호하기 위하여 사용될 수도 있다.

[0063] (도 3a 및 도 3b 를 포함하는) 도 3 은 가입자 인증에 기초한 키 계층구조가 또한 디바이스 인증을 포함하도록 어떻게 수정될 수도 있는 가에 대한 예를 도시한다. 키 계층구조는 디바이스와 네트워크 사이의 통신을 암호화/복호화하는데 사용되는 보안 파라미터들 (예를 들면, 보안 키) 을 설정하기 위하여 구현될 수도 있다. 이 예에서, 가입자 인증 및 디바이스 인증은 디바이스 (322) 와 네트워크 엔티티 (324) 사이에 수행될 수도 있다. 디바이스 (322) 는 예를 들면, 액세스 단말 (AT), 사용자 장비 (UE), 모바일 폰 및/또는 릴레이 노드일 수도 있다. 네트워크 엔티티 (324) 는 이동성 관리 엔티티 (MME) 및/또는 홈 가입자 서버 (HSS) 와 같은 하나 이상의 네트워크 디바이스들일 수도 있다.

[0064] 이 예는 가입자 인증과 디바이스 인증 양쪽 모두에 기초하여 제 2 키 계층구조 (300') 를 획득하기 위하여 가입자 인증에 기초한 제 1 키 계층구조 (300) 가 어떻게 수정되는 지를 도시한다.

[0065] 제 1 키 계층구조 (300) 에서 도시한 바와 같은 가입자 인증의 목적들을 위해, 유니버셜 집적 회로 카드 (디바이스 (322) 내의 UICC) 및 네트워크 엔티티 (324) (예를 들면, 도 1 에서의 MME (110) 및 HSS (112), 또는 다른 네트워크 엔티티) 는 암호 키 (CK) (304) 및 무결성 키 (IK) (306) 를 생성하기 위하여 마스터 키 (K) (302) 를 사용할 수도 있다. 그런 다음, 암호 키 (CK) (304) 및 무결성 키 (IK) (306) 는 (본원에서 가입자 인증 키라고도 지칭되는) 액세스 보안 관리 엔티티 키 K_ASME (308) 를 생성하기 위하여 인증 및 키 합의 (AKA) 교환의 일부로서 디바이스 (322) 및 네트워크 엔티티 (324) 에 의해 사용될 수도 있다. 디바이스 (202) 의 보안 활성화는 인증 및 키 합의 (AKA) 프로시저, 비 액세스 계층 (NAS) 보안 모드 구성 (NAS SMC) 프로시저 및 액세스 계층 (AS) 보안 모드 구성 (AS SMC) 프로시저를 통하여 달성될 수도 있다.

[0066] 이 예에서, 가입자 인증은 K_ASME (308) 의 결과를 초래하는 AKA 교환 (326) 을 포함할 수도 있다. AKA 교환 (326) 은 가입자 인증 요청 (340) 및 가입자 인증 응답 (342) 을 포함할 수도 있다. 이 예에서, K_ASME 키 (308) 를 생성하는 가입자 인증 프로세스는 또한 연관된 NAS-레벨 키들 (예를 들면, K_NAS-enc (305) 및 K_NAS-int (311)) 및/또는 AS-레벨 키들 (예를 들면, K_UP-enc (315), K_RRC-enc (317) 및 K_RRC-int (319)) 을 생성할 수도 있다. 일부 구현들에서, NAS-레벨 키들 및 AS-레벨 키들의 이 버전들이 사용되지 않으면, 이 키들의 생성은 가입자 인증 동안에 포기될 수도 있다는 것에 유의한다.

[0067] 제 2 키 계층구조 (300') 는 NAS-레벨 보안 키들 및 AS-레벨 보안 키들을 생성하기 위하여 디바이스 인증이 가입자 인증에 어떻게 바인딩될 수도 있는 지를 도시한다. 가입자 인증 (및 그것의 대응하는 K_ASME 키 (308) 생성) 과 동시에, 그 전에 또는 그 뒤에, 디바이스 인증 (328) 은 적어도 부분적으로 디바이스-특정 루트 키에 기초하여 수행될 수도 있다. 디바이스 인증 (328) 은 디바이스 인증 요청 (344) 및 디바이스 인증 응답 (346) 을 포함할 수도 있다. 일 구현에서, 디바이스 인증 (307) 은 가입자 인증과는 독립적일 수도 있다; 가입자 인증 및 디바이스 인증 양쪽 모두가 만족되어야만 복합 보안 키 K_ASME_D (309) 가 생성된다. 대안적인 구현에서, 디바이스 인증은 가입자 인증 전에 수행될 수도 있다.

[0068] 복합 보안 키 K_ASME_D (309) 는, 예를 들면, NAS (비 액세스 계층) 키들 (310 및 312) 및 AS (액세스 계층) 키들 (314, 316, 318 및 320) 의 산출을 위한 기저 키로서 사용될 수도 있다. 즉, 하나 이상의 보안 키들을 생성하기 위하여 디바이스 (322) 및 네트워크 엔티티 (324) 는 그런 다음 K_ASME_D (309) 를 사용할 수도 있다.

[0069] 패킷-스위칭된 네트워크들은 다수의 계층적 프로토콜 층들로 구조화될 수도 있으며, 여기서 하위 프로토콜 층들은 상위 층들에 서비스들을 제공하고 각각의 층은 상이한 태스크들에 대한 책임을 진다. 예를 들면, 도 4 는 패킷-스위칭된 네트워크에서 동작하는 디바이스에서 구현될 수도 있는 예시적인 프로토콜 스택을 도시한다. 이 예에서, 프로토콜 스택 (402) 은 물리 (PHY) 층 (404), 미디어 액세스 제어 (MAC) 층 (406), 무선 링크 제어 (RLC) 층 (408), 패킷 데이터 컨버전스 프로토콜 (PDCP) 층 (410), 무선 자원 제어 (RRC) 층 (412), 비 액세스 계층 (NAS) 층 (414) 및 애플리케이션 (APP) 층 (416) 을 포함한다.

[0070] NAS 층 (414) 아래의 층들은 종종 액세스 계층 (AS) 층 (418) 으로 지칭된다. RLC 층 (408) 은 하나 이상의 채널들 (420) 을 포함할 수도 있다. RRC 층 (412) 은 접속된 상태 및 아이들 상태를 포함하여 액세스 단말에 대한 다양한 모니터링 모드들을 구현할 수도 있다. 비 액세스 계층 (NAS) 층 (414) 은 통신 디바이스의 이동성 관리 콘텍스트, 패킷 데이터 콘텍스트 및/또는 그것의 IP 주소들을 유지할 수도 있다. 다른 층들은 프로토콜 스택 (402) 내에 (예를 들면, 도시된 층들의 위에, 아래에 및/또는 사이에) 존재할 수도 있으나, 도시를 위해서는 생략되었다는 것에 유의한다.

[0071] 도 4 를 참조하면, 무선/세션 베어러들 (422) 은, 예를 들면, RRC 층 (412) 및/또는 NAS 층 (414) 에서 설정될 수도 있다. 그 결과, 도 3 에 도시된 보안 키들 K_NAS-enc (310) 및 K_NAS-int (312) 를 생성하기 위하여 NAS 층 (414) 은 디바이스 (202) 및 코어 네트워크 (108) 에 의해 사용될 수도 있다. 마찬가지로, 액세스 계층 (AS) 보안 키들 K_UP-enc (316), K_RRC-enc (318) 및 K_RRC-int (320) 를 생성하기 위하여 RRC 층 (412) 은 디바이스 (202) 및 액세스 노드 (108) 에 의해 사용될 수도 있다. 보안 키들 K_UP-enc (316), K_RRC-enc (318) 및 K_RRC-int (320) 는 RRC 층 (312) 에서 생성될 수도 있지만, 시그널링 및/또는 사용자/데이터 통신을 안전하게 보호하기 위하여 이 키들은 PDCP 층 (410) 에 의해 사용될 수도 있다. 예를 들면, 사용자/데이터 플레인 (UP) 통신을 안전하게 보호하기 위하여 키 K_UP-enc (316) 는 PDCP 층 (410) 에 의해 사용될 수도 있으며, PDCP 층 (410) 에서의 시그널링 (즉, 제어) 통신을 안전하게 보호하기 위하여 키들 K_RRC-enc (318) 및

K_RRC-int (320) 가 사용될 수도 있다.

[0072] 암호화 및 무결성 알고리즘들에 대하여 사용된, 이 보안 키들의 도출 시에, AS (사용자 플레인 및 RRC) 및 NAS 양쪽 모두에서의 이들 키들은 개별 알고리즘 아이덴티티가 입력들의 하나로서 제공되는 것을 요구한다. AS 레벨에서, 사용될 알고리즘들은 무선 자원 제어 (RRC) 보안 모드 커맨드에 의해 제공된다.

[0073] 도 5 는 도 3 및 도 4 에 도시된 다양한 인증 및/또는 보안 키들이 생성될 수도 있는 네트워크 시스템을 도시한 블록도이다. 여기에서, 디바이스 (322) 는 다양한 층들 (예를 들면, APP, NAS, RRC, RLC, MAC 및 PHY) 을 포함하는 통신 스택을 구현할 수도 있다. 액세스 네트워크 (504) (예를 들면, 도 1 의 액세스 노드 (106)) 는 그것이 네트워크 (108) 와 통신할 수도 있도록 디바이스 (322) 에게 무선 접속성을 제공할 수도 있다. 홈 가입자 서버 (506) 및 디바이스 (322) 양쪽 모두는 암호 키 (CK) 및/또는 무결성 키 (IK) 를 생성 또는 획득하기 위하여 사용될 수 있는 루트 키 (K) 를 알 수도 있거나 액세스할 수도 있다. 액세스 보안 관리 엔티티 키 K_ASME 를 생성하기 위하여 디바이스 (322) 및/또는 HSS (506) 는 그런 다음 암호 키 (CK) 및/또는 무결성 키 (IK) 를 사용할 수도 있다. 복합 보안 키 K_ASME_D 를 생성하기 위하여 디바이스 인증이 또한 수행될 수도 있고 K_ASME 키와 결합되거나 K_ASME 키에 기초할 수도 있으며, 그렇게 함으로써 가입자 인증과 디바이스 인증을 하나의 키로 결합한다. K_ASME_d 키를 사용하여, 디바이스 (322) 및 이동성 관리 엔티티 (MME) (510) 는 그런 다음 키들 K_NAS-enc 및 K_NAS-int 를 생성할 수도 있다. 디바이스 (322) 및 MME (510) 는 또한 액세스 네트워크-특정 키 K_eNB/NH 를 생성할 수도 있다. 이 액세스 네트워크-특정 키 K_eNB/NH 를 사용하여, 디바이스 (322) 및 액세스 네트워크 (504) 는 키들 K_UP-enc 및 K_RRC-enc 및 K_RRC-int 를 생성할 수도 있다.

[0074] 이 키들의 도출에 대한 세부사항들은 본원에서 참조로서 통합된, (3GPP TS 33.401 로서 알려진) 3GPP STD-T63-33.401 "System Architecture Evolution (SAE): Security Architecture" Release 8 에 제공된다. 도 3 내지 도 5 는 디바이스 인증 및 가입자 인증 및 바인딩이 구현될 수도 있는 특정 환경/콘텍스트를 설명하지만, 이것은 네트워크들의 다양한 다른 유형들에서 구현될 수도 있는 이 피쳐들을 제한하려는 의도를 가지고 있지 않다는 것에 유의한다.

[0075] **예시적인 무선 디바이스**

[0076] 도 6 은 가입자 인증 및 디바이스 인증을 바인딩하도록 적응될 수도 있는 무선 디바이스 (600) 의 선택 컴포넌트들을 도시한 블록도이다. 무선 디바이스 (600) 는 일반적으로 하나 이상의 무선 통신 인터페이스(들) (604) 에 결합된 프로세싱 회로 (602) 를 포함한다. 예를 들면, 무선 디바이스 (600) 는 릴레이 노드 및/또는 액세스 단말일 수도 있다.

[0077] 프로세싱 회로 (602) 는 데이터를 획득하고, 프로세스하고/하거나 전송하고, 데이터 액세스 및 저장을 제어하고, 커맨드들을 발행하고, 그리고 다른 원하는 동작들을 제어하도록 배열될 수도 있다. 프로세싱 회로 (602) 는 적어도 하나의 실시형태에서 적절한 매체들에 의해 제공되는 원하는 프로그래밍을 구현하도록 구성된 회로를 포함할 수도 있다. 예를 들면, 프로세싱 회로 (602) 는 프로세서, 제어기, 예를 들면, 복수의 프로세서들 및/또는 소프트웨어 및/또는 펌웨어 명령들을 포함하는 실행가능한 명령들을 실행하도록 구성된 다른 구조 중 하나 이상, 및/또는 하드웨어 회로로서 구현될 수도 있다. 프로세싱 회로 (602) 의 실시형태들은 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적회로 (ASIC), 필드 프로그래머블 게이트 어레이 (FPGA) 또는 다른 프로그래머블 로직 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에서 설명된 기능들을 수행하도록 디자인된 임의의 조합을 포함할 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있으나, 대안에서, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기 또는 상태 머신일 수도 있다. 프로세서는 또한 DSP 와 마이크로프로세서의 조합과 같은 컴퓨팅 컴포넌트들의 조합, 다수의 마이크로프로세서들, DSP 코어와 협력하는 하나 이상의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로서 구현될 수도 있다. 프로세싱 회로 (602) 의 이 예들은 예시를 위한 것이며 본 개시의 범위 내의 다른 적합한 구성들이 또한 고려된다.

[0078] 무선 통신 인터페이스 (604) 는 무선 디바이스 (600) 의 무선 통신을 용이하게 하도록 구성될 수도 있다. 예를 들면, 통신 인터페이스 (604) 는 액세스 단말들, 액세스 노드들, 다른 릴레이 노드들 등과 같은 다른 무선 디바이스들에 대하여 정보를 양방향으로 통신하도록 구성될 수도 있다. 통신 인터페이스 (604) 는 안테나 (미도시) 에 결합될 수도 있고 무선 통신을 위하여 적어도 하나의 송신기 및/또는 적어도 하나의 수신기 (예를

들면, 하나 이상의 송신기/수신기 체인들) 를 포함하는 무선 송수신기 회로를 포함할 수도 있다.

[0079] 프로세싱 회로 (602) 는 가입자 및 디바이스 인증 바인딩 모듈 (610) 을 포함할 수도 있다. 가입자 및 디바이스 인증 바인딩 모듈 (610) 은 가입자 보안 크리덴셜들 (예를 들면, 유니버셜 집적 회로 카드 (608) 에 저장된 가입자-특정 키 (607) 및/또는 가입자 아이덴티티 (609)) 을 이용하여 가입자 인증 프로시저들을 수행하도록 적응되고, (신뢰 환경 (606) 내에서) 디바이스-특정 크리덴셜들 (예를 들면, 디바이스-특정 키 (605) 및/또는 디바이스 아이덴티티 (611)) 을 이용하여 디바이스 인증 프로시저들을 수행하도록 적응되고 가입자 인증 및 디바이스 인증을 함께 바인딩하는 회로 및/또는 프로그래밍을 포함할 수 있다. 그러한 "바인딩" 은 가입자 인증 및 디바이스 인증 양쪽 모두로부터의 일부 결과들을 결합하는 것과 연관될 수도 있다. 예를 들면, 제 3 (복합) 보안 키를 획득하기 위하여, 가입자 인증으로부터 획득한 제 1 보안 키는 디바이스 인증으로부터 획득한 제 2 보안 키와 결합될 수도 있다.

[0080] 일부 실시형태들에서, 무선 디바이스 (600) 는 신뢰 환경 (TrE) (606) 을 포함할 수도 있다. 신뢰 환경 (606) 은 TS 33.320 에서의 3GPP 사양 세부사항에서 신뢰 환경에 대한 사양들을 충족시키도록 적응될 수도 있다. 신뢰 환경 (606) 에는 적어도 일부 보안 크리덴셜들 (예를 들면, 디바이스-특정 키 (605) 및/또는 디바이스 아이덴티티 (611)) 이 사전 제공 (또는 안전하게 내장) 될 수도 있다. 예를 들면, 신뢰 환경 (606) 은 디바이스 인증과 관련된 보안 크리덴셜들을 가질 수도 있다.

[0081] 일부 실시형태들에서, 무선 디바이스 (600) 는 유니버셜 집적 회로 카드 (UICC) (608) 내에 안전하게 보호된 프로세싱을 포함할 수도 있다. UICC (608) 는 무선 디바이스 (600) 에 착탈 가능하게 결합될 수도 있다. UICC (608) 에는 초기 인증 및 키 합의 (AKA) 크리덴셜들과 같은, 가입자 보안 크리덴셜들 (예를 들면, 가입자-특정 키 (607) 및/또는 가입자 아이덴티티 (609)) 이 사전 제공될 수도 있다. 대안적으로, 안전하게 보호된 프로세싱이 유니버셜 가입자 아이덴티티 모듈 (USIM) 내에서 수행될 수도 있다.

[0082] 무선 디바이스 (600) 의 하나 이상의 피쳐들에 따라서, 프로세싱 회로 (602) 는 도 2 내지 도 5, 도 7, 도 10, 도 11 및 도 12 에 도시된 연관된 프로세스들, 기능들, 단계들 및/또는 루틴들의 임의의 하나 또는 모두를 수행하도록 적응될 수도 있다. 본원에서 사용된 바와 같이, 프로세싱 회로 (602) 에 관한 용어 "적응된 (adapted)" 은 프로세싱 회로 (602) 가 본원에서 개시된 다양한 피쳐들에 따라서 특정 프로세스, 기능, 단계 및/또는 루틴을 수행하도록 구성, 채용, 구현, 및/또는 프로그램된 것을 나타낼 수도 있다.

[0083] 도 7 은 가입자 인증과 디바이스 인증을 바인딩하는 보안 키를 생성하기 위하여 무선 디바이스에서 동작하는 방법의 예를 도시한 플로우 다이어그램이다. 무선 디바이스에 디바이스-특정 키가 사전 제공될 수도 있다 (702). 예를 들면, 그러한 디바이스-특정 키는 칩에 내장되거나 무선 디바이스의 제조 동안 구성될 수도 있다. 무선 디바이스는 또한 디바이스-특정 키와 연관된 디바이스 식별자를 포함할 수도 있다. 부가적으로, 무선 디바이스에 가입자-특정 키가 사전 제공될 수도 있다 (704). 예를 들면, 그러한 가입자-특정 키는 가입자에게 할당된 루트 키일 수도 있고, 무선 디바이스에 결합된 고정된 또는 착탈식 모듈 (예를 들면, UICC 또는 USIM) 내에 저장될 수도 있다. 무선 디바이스는 또한 가입자-특정 키와 연관된 가입 아이덴티티를 포함할 수도 있다. 무선 디바이스는 (예를 들면, 가입자-특정 키를 사용하여) 네트워크 엔티티와의 가입자 인증을 수행할 수도 있다 (706). 이것은, 예를 들면, 네트워크 엔티티와의 인증 및 키 합의 교환을 포함할 수도 있다. 무선 디바이스는 또한 (예를 들면, 디바이스-특정 키를 사용하여) 네트워크 엔티티와의 디바이스 인증을 수행할 수도 있다 (708). 가입자 인증 및 디바이스 인증은 동일하거나 상이한 시간들에서 동일한 네트워크 엔티티 또는 상이한 네트워크 엔티티들과 수행될 수도 있다. 보안 키 (예를 들면, K_ASME_D 등) 는 그런 다음 무선 디바이스에 의해 생성될 수도 있으며, 그러한 보안 키는 가입자 인증과 디바이스 인증을 바인딩한다 (710). 예를 들면, 일 예에서, 보안 키를 생성하기 위하여 디바이스 인증으로부터의 데이터 (예를 들면, 결과로 초래되는 하나 이상의 키들, 인증서들, 식별자들 등) 및 가입자 인증으로부터의 데이터 (예를 들면, 결과로 초래되는 하나 이상의 키들, 인증서들, 식별자들 등) 가 결합될 수도 있다. 예를 들면, 도 1 에서, 보안 키 K_ASME_D 를 생성하기 위하여 가입자 인증 (210) 으로부터의 K_ASME 키와 도 1 에서의 디바이스 인증으로부터의 device_temp_key 가 결합될 수도 있다. 보안 키는 그런 다음 무선 디바이스와 네트워크 엔티티 사이의 무선 통신을 안전하게 보호하기 위하여 사용될 수도 있다 (712). 예를 들면, 보안 키는 무선 디바이스와 네트워크 사이의 통신 (예를 들면, 데이터 및 시그널링) 을 암호화/해독하도록 기능할 수도 있는 다른 키들 및/또는 인증서들 (예를 들면, NAS-레벨 및/또는 AS-레벨 보안 키들) 을 생성하기 위하여 사용될 수도 있다.

[0084] **예시적인 네트워크 엔티티**

[0085] 도 8 은 가입자 인증과 디바이스 인증을 바인딩하기 위하여 적응될 수도 있는 네트워크 엔티티 (800) 의 선택 컴포넌트들을 도시한 블록도이다. 네트워크 엔티티 (800) 는 통신 인터페이스 (804) 에 결합된 프로세싱 회로 (802) 를 포함할 수도 있다. 프로세싱 회로 (802) 는 데이터를 획득하고, 프로세스하고/하거나 전송하고, 데이터 액세스 및 저장을 제어하고, 커맨드들을 발행하고, 그리고 다른 원하는 동작들을 제어하도록 배열된다. 프로세싱 회로 (802) 는 적어도 하나의 실시형태에서 적절한 매체들에 의해 제공되는 원하는 프로그래밍을 구현하도록 구성된 회로를 포함할 수도 있다. 예를 들면, 프로세싱 회로 (802) 는 프로세서, 제어기, 복수의 프로세서들 및/또는 예를 들면, 소프트웨어 및/또는 펌웨어 명령들을 포함하는 실행가능한 명령들을 실행하도록 구성된 다른 구조 중 하나 이상, 및/또는 하드웨어 회로로서 구현될 수도 있다. 프로세싱 회로 (802) 의 실시형태들은 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적회로 (ASIC), 필드 프로그래머블 게이트 어레이 (FPGA) 또는 다른 프로그래머블 로직 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에서 설명된 기능들을 수행하도록 디자인된 임의의 조합을 포함할 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있으나, 대안에서, 프로세서는 종래의 프로세서, 제어기, 마이크로제어기 또는 상태 머신일 수도 있다. 프로세서는 또한 DSP 와 마이크로프로세서의 조합과 같은 컴퓨팅 컴포넌트들의 조합, 다수의 마이크로프로세서들, DSP 코어와 협력하는 하나 이상의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로서 구현될 수도 있다. 프로세싱 회로 (802) 의 이 예들은 예시를 위한 것이며 본 개시의 범위 내의 다른 적합한 구성들이 또한 고려된다.

[0086] 프로세싱 회로 (802) 는 가입자 및 디바이스 인증 바인딩 모듈 (806) 을 포함한다. 가입자 및 디바이스 인증 바인딩 모듈 (806) 은 가입자 보안 크리덴셜들 (예를 들면, 가입자-특정 키 및/또는 가입자 식별자) 에 기초하여 가입을 인증하기 위한 가입자 인증 프로시저들을 수행하고, 디바이스-특정 크리덴셜들 (예를 들면, 디바이스-특정 키 및/또는 디바이스 식별자) 에 기초하여 디바이스를 인증하기 위한 디바이스 인증 프로시저들을 수행하고, 그리고 보안 키를 생성하기 위하여 디바이스 인증 및 가입자 인증으로부터 데이터 (예를 들면, 키들, 값들, 인증서들 등) 를 바인딩하도록 적응된 회로 및/또는 프로그래밍을 포함할 수 있다.

[0087] 통신 인터페이스 (804) 는 네트워크 엔티티 (800) 가 릴레이 노드들 및 액세스 단말들과 같은 다른 디바이스들과 직접적으로 또는 간접적으로 (예를 들면, 하나 이상의 다른 네트워크 엔티티들을 통하여) 통신하는 것을 용이하게 하도록 구성된다.

[0088] 네트워크 엔티티 (800) 의 하나 이상의 피처들에 따라서, 프로세싱 회로 (802) 는 모바일 관리 엔티티 (MME) (110) 및 홈 가입자 서버 (HSS) (112) 와 같은 다양한 네트워크 엔티티들과 관련된 프로세스들, 기능들, 단계들 및/또는 루틴들 중 임의의 것 또는 모두를 수행하도록 적응될 수도 있다. 더욱이, 네트워크 엔티티 (800) 는 단일 엔티티 또는 네트워크의 2 개 이상의 엔티티들의 조합을 포함할 수도 있다. 제한적이지 않은 예로서, 네트워크 엔티티 (800) 는 그 중에서도 모바일 관리 엔티티 (MME), 홈 가입자 서버 (HSS), 디바이스 인증 서버를 포함할 수도 있다. 본원에서 사용되는 바와 같이, 프로세싱 회로 (802) 에 관한 용어 "적응된 (adapted)" 은 본원에서 설명된 다양한 피처들에 따라서 특정 프로세스, 기능, 단계 및/또는 루틴을 수행하도록 구성된, 채용된, 구현된 또는 프로그램된 중의 하나 이상인 프로세싱 회로 (802) 를 나타낼 수도 있다.

[0089] 도 9 는 가입자 인증과 디바이스 인증을 바인딩하는 보안 키를 생성하기 위하여 네트워크 엔티티에서 동작하는 방법의 예를 도시하는 플로우 다이어그램이다. 네트워크 엔티티는 무선 디바이스에 대한 디바이스-특정 키를 획득할 수도 있다 (902). 예를 들면, 그러한 디바이스-특정 키는 칩 내에 내장되거나 무선 디바이스의 제조 동안에 구성될 수도 있으며, 이 정보는 네트워크 엔티티가 액세스할 수 있는 데이터베이스 내에 저장될 수도 있다. 디바이스 식별자는 디바이스-특정 키와 연관될 수도 있으며 디바이스 및 그것의 키를 식별하기 위하여 사용될 수도 있다. 부가적으로, 네트워크 엔티티는 무선 디바이스에 대한 가입과 연관된 가입자-특정 키를 획득할 수도 있다 (904). 예를 들면, 그러한 가입자-특정 키는 가입자에게 할당된 루트 키일 수도 있고, 무선 디바이스에 결합된 고정된 또는 착탈식 모듈 (예를 들면, UICC 또는 USIM) 내에 저장될 수도 있다. 네트워크 엔티티는 (예를 들면, 가입자-특정 키를 사용하여) 무선 디바이스와의 가입자 인증을 수행할 수도 있다 (906). 이것은, 예를 들면, 네트워크 엔티티와의 인증 및 키 합의 교환을 포함한다. 네트워크 엔티티는 또한 (예를 들면, 디바이스-특정 키를 사용하여) 무선 디바이스와의 디바이스 인증을 수행할 수도 있다 (908). 가입자 인증 및 디바이스 인증은 동일하거나 상이한 시간들에서 수행될 수도 있다. (복합) 보안 키 (예를 들면, K_ASME_D 등) 는 그런 다음 네트워크 엔티티에 의해 생성되며, 그러한 보안 키는 가입자 인증과 디바이스 인증을 바인딩한다 (910). 예를 들면, 일 예에서, 보안 키를 생성하기 위하여 디바이스 인증으로부터의 데이터 (예를 들면, 결과로 초래되는 하나 이상의 키들, 인증서들, 식별자들 등) 와 가입자 인증으로부터의 데이터 (예를 들면, K_ASME 등) 가 결합될 수도 있다. 보안 키는 그런 다음 네트워크 엔티티와 무선

디바이스 사이의 무선 통신을 안전하게 보호하기 위하여 사용될 수도 있다 (912). 예를 들면, 보안 키는 무선 디바이스와 네트워크 사이의 통신을 암호화/해독하도록 기능할 수도 있는 다른 키들을 생성하기 위하여 사용될 수도 있다.

[0090] **가입자-디바이스 인증의 제 1 예시적인 방법**

[0091] 도 10 은 가입자 인증과 디바이스 인증을 바인딩함으로써 보안 키를 생성하는 제 1 예시적인 방법을 도시한다. 이 예에서, 디바이스 (1002) 는, 예를 들면, 릴레이 노드 또는 액세스 단말일 수도 있다. 디바이스 (1102) 가 (예를 들면, MME (1002) 및 HSS (1006) 를 포함하는) 무선 네트워크에 어태치되도록 시도할 수도 있는 어태치 스테이지 동안에, 디바이스 아이덴티티 또는 다른 관련된 디바이스 정보를 오버 디 에어 (over the air) 로 드러내는 것은 (예를 들면, 디바이스 (1002) 에 대한) 보안상의 관심사일 수도 있다. 그 결과, 이 방법에서, 디바이스상의 수동적인 공격들을 방지하기 위하여 네트워크에 의해 안전하게 요청될 때까지 디바이스 (1002) 는 그것의 디바이스 크리덴셜들 (예를 들면, 국제 모바일 장비 아이덴티티 (IMEI) 와 같은 디바이스-특정 식별자 등) 을 오버 디 에어로 제시하지 않는다.

[0092] 디바이스는 디바이스 인증을 할 수 있는 표시를 포함하는 어태치 요청 (1010) 을 네트워크에 전송함으로써 시작할 수도 있다. 어태치 요청 (1010) 을 수신하면, 이동성 관리 엔티티 (MME) (1004) 는 홈 가입자 서버 (HSS) (1006) 로부터 (예를 들면, 디바이스 (1002) 의 가입-기반 어카운트 또는 사용자와 연관된) 가입 및 인증 정보를 요청 및 수신할 수도 있다 (1012). AKA 인증을 수행하기 위하여 MME (1004) 는 그런 다음 AKA 도전을 포함하는 인증 요청 (1014) 을 전송한다. AKA 인증 요청 (1014) 을 수신하면, 디바이스 (1002) 는 AKA 응답을 포함하는 인증 응답 (1016) 을 전송한다. AKA 인증 요청 (1014) 및 응답 (1016) 은 가입자 인증을 수행하도록 기능한다. 그러한 AKA 인증 프로시저들은 디바이스 (1002) 및 MME 에 의해 생성되는 가입자 인증 키 (예를 들면, K_ASME) 의 결과를 초래할 수도 있다.

[0093] 디바이스 인증은 이 보안 활성화 프로세스 동안 다양한 스테이지들에서 수행될 수도 있다. 이 예에서, 디바이스 인증은 NAS-레벨 보안 메시지들 상에서 피기 백 (piggy-backed) 될 수도 있다. 예를 들면, MME (1004) 는 디바이스 아이덴티티에 대한 요청 (예를 들면, IMEI 소프트웨어 버전 (IMEISV) 에 대한 요청 및/또는 device_credentials 에 대한 요청) 을 포함하는 NAS 보안 모드 커맨드 (1018) 를 전송할 수도 있다. 응답하여, 디바이스 (1002) 는 보안 모드 완료 (1020) 메시지 내에, 디바이스 인증이 수행될 것이라는 디바이스 아이덴티티 또는 크리덴셜을 제공할 수도 있다. 송신 동안 오버 디 에어로 디바이스 아이덴티티 또는 크리덴셜을 노출하는 것을 회피하기 위하여, 보안 모드 완료 (1020) 내의 디바이스 아이덴티티 또는 크리덴셜은 이전에 계산된 가입자 인증 키 (예를 들면, K_ASME) 에 의해 안전하게 보호될 수도 있다는 것에 유의한다. 디바이스 아이덴티티 또는 크리덴셜을 수신하면, MME (1004) 는 진화형/확장형 키 세트 식별자 (eKSI) 및 device_challange 와 함께 아이덴티티 요청 (1022) 메시지를 전송할 수도 있다. eKSI 는 생성될 K_ASME_D 와 연관될 수도 있다. 따라서, 아이덴티티 요청 (1022) 에서 사용된 eKSI 는, 예를 들면, AKA (즉, 가입자 인증) 에 대하여 사용되었을 수도 있는 임의의 다른 eKSI 와 상이하거나 구별될 수도 있다. 아이덴티티 요청 (1022) 메시지를 수신하면, 디바이스 (1002) 는 device_challange 에 기초하여 device_response 를 생성할 수도 있으며 이것을 아이덴티티_응답 (1024) 메시지의 일부로서 전송한다. device_response 는 device_challange 및 디바이스 아이덴티티 또는 크리덴셜에 기초할 수도 있다. 디바이스 (1002) 는 그런 다음 인증 키 (예를 들면, K_ASME) 및 디바이스 인증 데이터 (예를 들면, 디바이스 응답 등) 에 기초하여 (복합) 보안 키 (K_ASME_D) (1025) 를 산출할 수도 있다. MME (1004) 는, 예를 들면, 디바이스 (1002) 의 디바이스 아이덴티티 또는 인증서를 사용하여 그리고 device_response 를 사용함으로써 device_response 를 점검한다.

디바이스 (1002) 가 MME (1004) 에 의해 성공적으로 인증되면, MME (1004) 는 또한 보안 키 (K_ASME_D) (1027) 를 생성한다. 이 시점에서, 디바이스 (1002) 및 MME (1004) 는 보안 키 (K_ASME_D) 및 그것의 연관된 식별자 (eKSI) 를 공유한다.

[0094] MME (1004) 는 그런 다음 보안 키 (K_ASME_D) 와 연관된 진화형/확장형 키 세트 식별자 (eKSI) 와 함께 보안 모드 커맨드 (1026) 를 전송할 수도 있다. 이것은 디바이스 (1002) 가 보안 키 (K_ASME_D) 에 기초하여 하나 이상의 보안 키들을 계산하는 것을 허용한다. 이 디바이스 (1002) 는 보안 모드 완료 (1028) 메시지를 MME (1004) 에 전송할 수도 있으며, 이에 의해 MME (1004) 이 어태치 완료 (1030) 메시지를 전송하는 것을 허용한다.

[0095] **가입자-디바이스 인증의 제 2 예시적인 방법**

[0096] 도 11 은 가입자 인증과 디바이스 인증을 바인딩함으로써 보안 키를 생성하는 제 2 예시적인 방법을 도시한다. 이 예에서, 오버 디 에어 송신에서 디바이스 아이덴티티 또는 인증서 (또는 다른 관련된 크리덴셜 정보) 를 드러내는 것은 보안상의 관심사가 아니다. 도 10 의 방법과는 달리, 이 경우에서, 디바이스 아이덴티티를 솔직하게 제시하는 것은 임의의 프라이버시 이슈들 또는 리스크들을 유도하지 않을 것이라는 것이 가정된다.

[0097] 디바이스는, MME 가 허용할 디바이스 식별자 또는 크리덴셜들 (예를 들면, IMEI) 을 이미 갖고 있지만 그 MME 가 사용하고자 하는 E-UTRAN 보안 콘텍스트는 갖고 있지 않다.

[0098] 디바이스 (1102) 는 그것의 디바이스 식별자 또는 크리덴셜들을 포함하는 어태치 요청 (1108) 을 MME (1104) 에 전송한다. MME (1104) 는 HSS (1106) 로부터 가입 및 인증 정보를 획득할 수도 있고 (1110), 예를 들면, (가입 인증에 대한) AKA 도전 및/또는 (디바이스 인증에 대한) 디바이스 도전을 포함하는 인증 요청 (1112) 를 전송한다. 디바이스 (1102) 는 AKA 응답 및/또는 디바이스 응답을 포함할 수도 있는 인증 응답 (1114) 을 전송함으로써 응답할 수도 있다는 것에 유의한다. AKA 응답은 적어도 부분적으로 가입자 식별자에 기초할 수도 있다. 디바이스 응답은 디바이스 식별자 및/또는 크리덴셜들 및 디바이스 도전에 기초할 수도 있다. 디바이스 (1104) 는 그런 다음 가입자 인증 정보와 디바이스 인증 정보를 결합함으로써 (복합) 보안 키 (K_ASME_D) 를 생성할 수도 있다. 마찬가지로, AKA 응답과 디바이스 응답을 성공적으로 검증하면, MME (1104) 는 또한 가입자 인증 정보와 디바이스 인증 정보를 결합함으로써 보안 키 (K_ASME_D) 를 생성할 수도 있다.

[0099] MME 는 보안 키 (K_ASME_D) 에 기초하여 보안 콘텍스트 사용을 시작하기 위하여 보안 모드 커맨드 (1116) 메시지를 전송한다. 디바이스 (1102) 는 보안 모드 완료 (1118) 메시지로 대응한다. 즉, 디바이스 (1102) 및 MME (1104) 는 보안 키 (K_ASME_D) 를 사용하여 하나 이상의 부가적인 보안 키들을 생성할 (또는 그렇지 않으면 디바이스 (110) 와 MME (1104) 사이의 통신을 안전하게 보호할) 수도 있다. MME (1104) 는 그런 다음 어태치 완료 (1120) 메시지를 디바이스 (1102) 에 전송할 수도 있다.

[0100] 여기에서의 관측은 디바이스 식별자 및/또는 크리덴셜들 (또는 이전에 획득된/생성된 디바이스 키들) 이 HSS (1106) 또는 가입 식별자를 가진 다른 네트워크내의 다른 서버에 저장되었다면, 어태치먼트를 수행하기 위하여 디바이스 (1102) 는 이 플로우를 사용할 수 있다는 것이다. 거기에서 이것을 하기 위하여, 디바이스 (1102) 는 그것의 디바이스 식별자 및/또는 크리덴셜이 HSS (1106) 또는 다른 네트워크 서버로부터 획득될 수도 있다는 것을 (예를 들면, 어태치 요청 (1108)에서) 나타낼 수도 있다. 대안적으로, MME (1104) 는 (예를 들면, 일부 형태의 device_challenge 와 함께, IMEI 와 같은 디바이스 식별자를 포함함으로써) device_challenge 는 특정 디바이스 식별자와 연관되었다는 것을 디바이스 (1102) 에게 나타낼 수도 있다. 이렇게 하여, 디바이스 (1102) 는 (인증 요청 (1112) 에서의) 디바이스 도전이 그것의 디바이스 식별자와 연관된다는 것을 알 수 있다.

[0101] **가입자-디바이스 인증의 제 3 예시적인 방법**

[0102] 도 12 는 가입자 인증과 디바이스 인증을 바인딩함으로써 보안 키를 생성하는 제 3 예시적인 방법을 도시한다. 이 예에서, 가입자 인증은 이전에 수행되었으므로 가입자 보안 콘텍스트 (1206) (예를 들면, K_ASME 키) 는 이미 제시되었다. 결합된 가입자 인증과 디바이스 인증은 기존의 보안 콘텍스트를 대체하기 위하여 네트워크에 의해 개시될 수도 있다. 이 실시형태는 오퍼레이터로부터 완벽하거나 동작할 준비가 된 크리덴셜들을 획득하기 위하여 초기 AKA-기반 보안 콘텍스트를 설정하는 것이 필요할 수도 있는 디바이스들에게 유익할 수도 있다.

[0103] 이 접근법은 MME 가 디바이스 식별자 (예를 들면, IMEI) 및/또는 device_credentials 를 이미 알고 있다는 것을 가정한다.

[0104] MME (1204) 는 device_challenge 를 포함하는 인증 요청 (1208) 을 디바이스 (1202) 에 전송한다. 응답하여, 디바이스 (1202) 는 device_response 를 포함하는 인증 응답 (1210) 을 MME (1204) 에 전송한다. device_response 는 device_challenge 및 디바이스 식별자 및/또는 인증서에 기초할 수도 있다. 이 시점에, 디바이스 (1202) 및 MME (1204) 양쪽 모두는 (예를 들면, AKA-기반 보안 콘텍스트 및 디바이스 인증 정보에 기초하여) (복합) 보안 키 (K_ASME_D) 를 산출하기 위한 충분한 정보를 가질 수도 있다.

[0105] MME (1204) 는 기존의 보안 콘텍스트 (1206) 를 (예를 들면, 가입자 인증과 디바이스 인증 양쪽 모두를 통합하

는) 새로운 보안 키 (K_ASME_D) 에 기초한 콘텍스트로 교체하기 위하여 NAS 보안 모드 커맨드 (1212) 를 디바이스 (1202) 에 전송할 수도 있다. 응답하여, 디바이스 (1202) 는 보안 키 (K_ASME_D) 에 기초한 새로운 보안 콘텍스트를 생성할 수도 있으며 응답으로 NAS 보안 모드 완료 (1214) 메시지를 전송할 수도 있다.

[0106] 본원에서 다양한 예들은 가입자 인증 및 디바이스 인증 양쪽 모두가 MME 를 통하여 수행될 수도 있다는 것을 예시하지만, 다른 네트워크 엔티티들은 MME 를 결합하여 또는 MME 를 대신하여 이 기능들의 일부를 수행할 수도 있다는 것에 유의한다.

[0107] 도 1, 도 2, 도 3, 도 4, 도 5, 도 6, 도 7, 도 8, 도 9, 도 10, 도 11 및/또는 도 12 에 도시된 컴포넌트들, 단계들, 피쳐들 및/또는 기능들 중 하나 이상은 단일 컴포넌트, 단계, 피쳐 또는 기능으로 재배치될 수도 있고/있거나 결합될 수도 있거나 또는 여러 개의 컴포넌트들, 단계들 또는 기능들로 구체화될 수도 있다. 부가적인 엘리먼트들, 컴포넌트들, 단계들 및/또는 기능들은 또한 본 개시를 벗어나지 않고 부가될 수도 있다. 도 1, 도 5, 도 6 및/또는 도 8 에 도시한 장치, 디바이스들 및/또는 컴포넌트들은 도 2, 도 3, 도 4, 도 7 및/또는 도 9 내지 도 12 에 설명된 방법들, 피쳐들 또는 단계들 중 하나 이상을 수행하도록 구성될 수도 있다. 본원에서 설명된 신규한 알고리즘들은 또한 소프트웨어로 효율적으로 구현되고/되거나 하드웨어로 구체화될 수도 있다.

[0108] 또한, 적어도 일부 구현들이 플로우차트, 플로우 다이어그램, 구조도 또는 블록도로서 도시된 프로세스로서 설명되었다는 것에 유의한다. 플로우차트가 동작들을 연속적 프로세스로서 설명할 수도 있으나, 동작들의 다수는 병행하여 또는 동시에 수행될 수 있다. 부가하여, 동작들의 순서는 재배치될 수도 있다. 프로세스는 그것의 동작들이 완료되면 종료된다. 프로세스는 방법, 기능, 프로시저, 서브루틴, 서브프로그램 등에 대응할 수도 있다. 프로세스가 기능에 대응할 때, 그것의 종료는 콜링 기능 또는 주요 기능으로의 기능의 리턴 (return) 에 대응한다.

[0109] 더구나, 실시형태들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드 또는 이들의 조합에 의해 구현될 수도 있다. 소프트웨어, 펌웨어, 미들웨어 또는 마이크로코드로 구현되면, 필요한 태스크들을 수행할 프로그램 코드 또는 코드 세그먼트들은 저장 매체 또는 다른 스토리지(들) 과 같은 기계 판독가능 매체에 저장될 수도 있다. 프로세서는 필요한 태스크들을 수행할 수도 있다. 코드 세그먼트는 프로시저, 기능, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스, 또는 명령들의 임의의 조합, 데이터 구조들, 또는 프로그램 문들 (statements) 을 나타낼 수도 있다. 코드 세그먼트는 정보, 데이터, 논의들, 파라미터들 또는 메모리 콘텐츠들을 패스 및/또는 수신함으로써 다른 코드 세그먼트 또는 하드웨어 회로에 결합될 수도 있다. 정보, 논의들, 파라미터들, 데이터 등은 메모리 공유, 메시지 패싱, 토큰 패싱, 네트워크 송신 등을 포함하는 임의의 적합한 수단을 통하여 패스되거나, 포워딩되거나 또는 송신될 수도 있다.

[0110] 용어들 "기계 판독가능 매체", "컴퓨터 판독가능 매체" 및/또는 "프로세서 판독가능 매체" 는 휴대용 또는 고정된 저장 디바이스들, 광 저장 디바이스들, 및 명령(들) 및/또는 데이터를 저장, 포함 또는 캐리할 수 있는 다양한 다른 비일시적 매체들을 포함할 수도 있으나 이에 제한되지는 않는다. 따라서, 본원에서 설명된 다양한 방법들은 "기계 판독가능 매체", "컴퓨터 판독가능 매체" 및/또는 "프로세서 판독가능 매체" 에 저장될 수도 있는 명령들 및/또는 데이터에 의해 부분적으로 또는 전체적으로 구현될 수도 있고 하나 이상의 프로세서들, 기계들 및/또는 디바이스들에 의해 수행될 수도 있다.

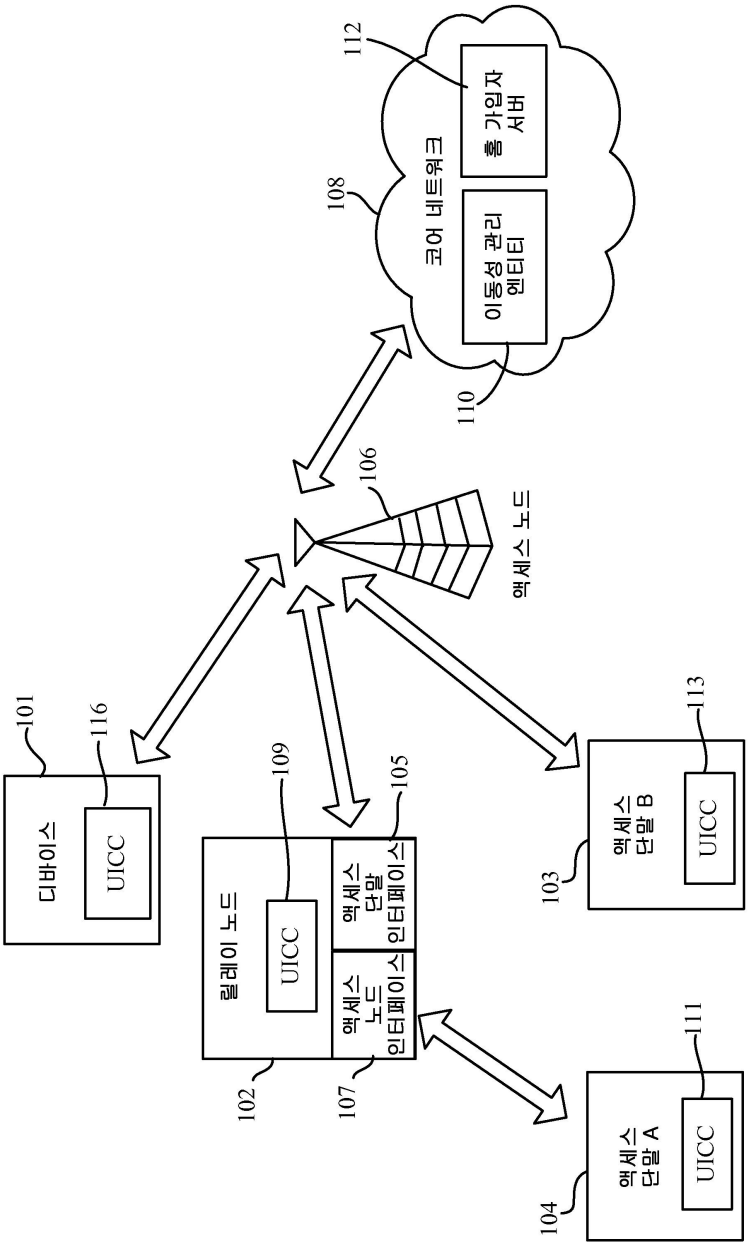
[0111] 본원에서 개시된 예들과 연계되어 설명된 방법들 또는 알고리즘들은 직접적으로 하드웨어로, 프로세서에 의해 실행가능한 소프트웨어 모듈로, 또는 양쪽의 조합으로, 프로세싱 유닛, 프로그래밍 명령들 또는 다른 방향들의 형태로 구체화될 수도 있으며, 단일 디바이스에 포함되거나 다수의 디바이스들에 걸쳐서 배분될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 착탈식 디스크, CD-ROM, 또는 기술 분야에서 알려진 비일시적인 저장 매체의 임의의 다른 형태에 상주할 수도 있다. 저장 매체는 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기입할 수 있도록 프로세서에 결합될 수도 있다. 대안적으로, 저장 매체는 프로세서에 내장될 수도 있다.

[0112] 기술 분야의 숙련된 자들은 본원에서 개시된 실시형태들과 연계하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어 또는 양쪽 모두의 조합으로서 구현될 수도 있다는 것을 더 이해할 것이다. 하드웨어 및 소프트웨어의 이 교환성을 명확히 보여주기 위하여, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 그들의 기능성의 측면에서 위에서 일반적으로 설명되어져 있다. 그러한 기능성이 하드웨어 또는 소프트웨어로 구현될 것인가 하는 여부는 특정 애플리케이션 및 전체 시스템상에 부과된 디자인 제약사항들에 좌우된다.

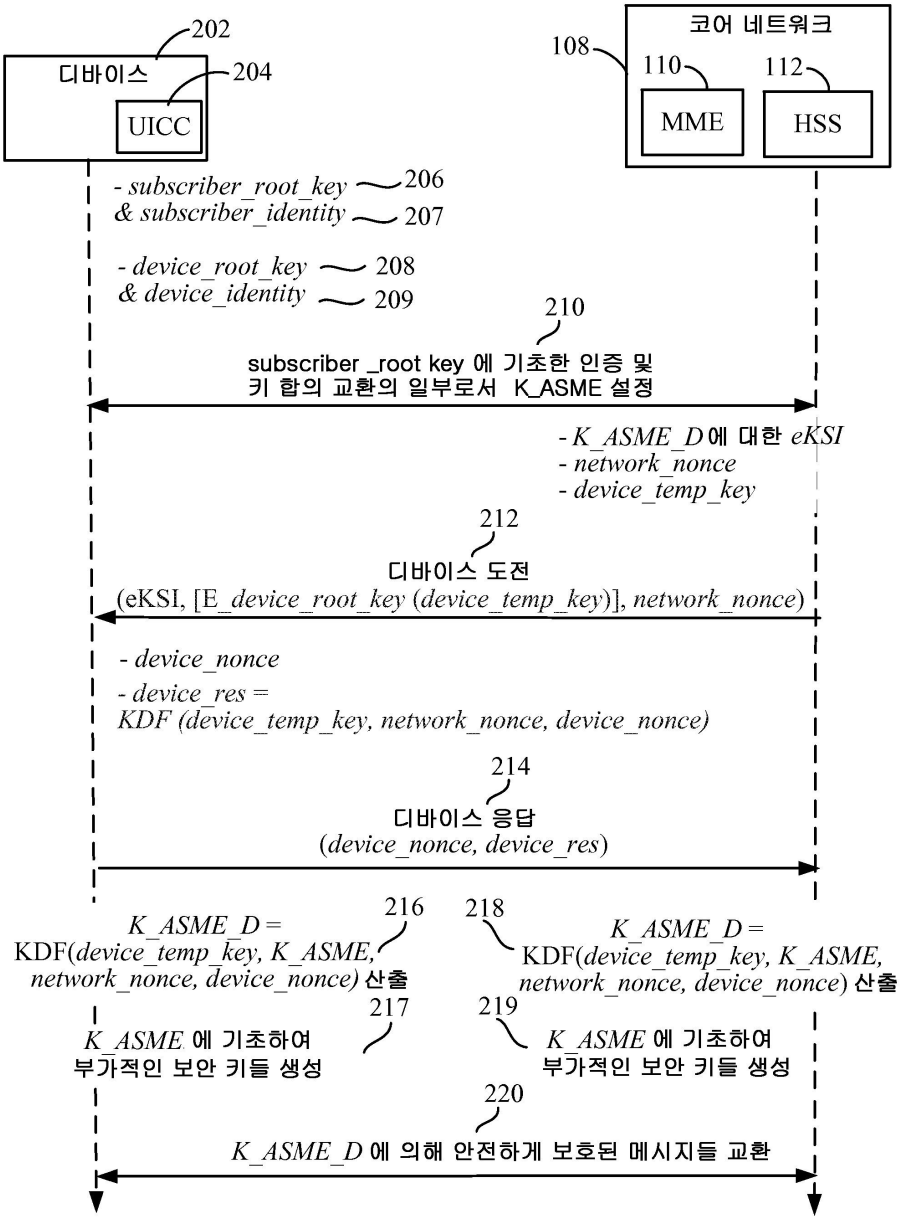
[0113] 본원에서 설명된 발명의 다양한 피쳐들은 본 발명을 벗어나지 않고 상이한 시스템들에서 구현될 수 있다. 앞에서 말한 실시형태들은 단지 예들에 지나지 않으며 본 발명을 제한하는 것으로 이해되지 않아야 한다는 것에 유의해야 한다. 실시형태들의 설명은 예시를 위한 것이며 본 개시의 범위를 제한할 의도를 가지고 있지 않다. 이와 같이, 본 교시들은 장치들의 다른 유형들에 쉽게 적용될 수 있으며 많은 대안들, 수정들 및 변형들이 기술 분야에 숙련된 자들에게 명백할 것이다.

도면

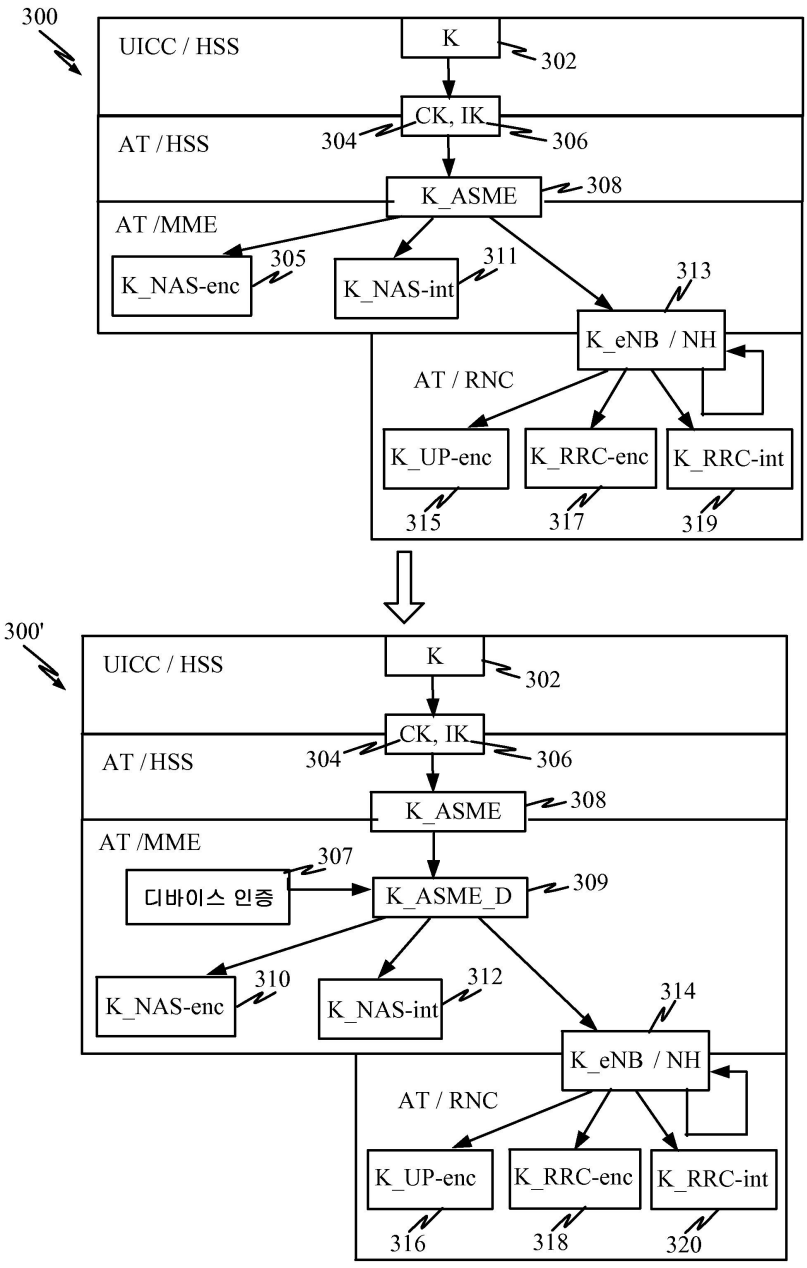
도면1



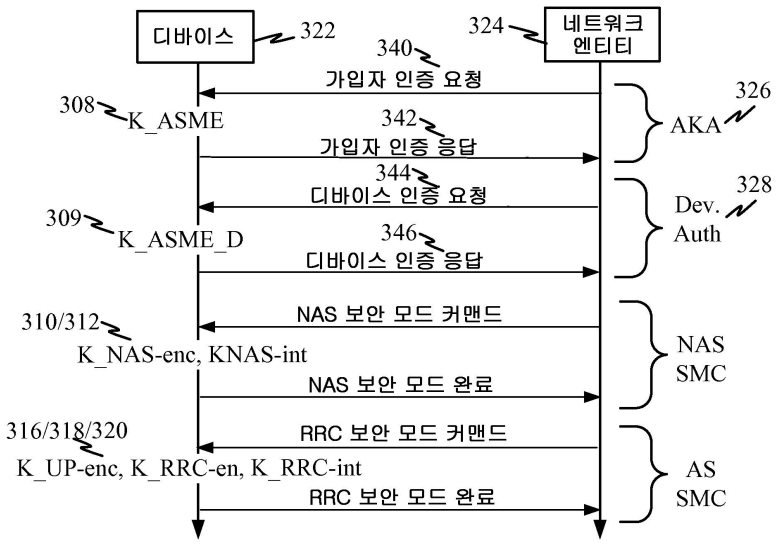
도면2


202
디바이스
204
UICC
코어 네트워크
108
110
MME
112
HSS
- subscriber_root_key 206
& subscriber_identity 207
- device_root_key 208
& device_identity 209
210
subscriber _root key 에 기초한 인증 및
키 합의 교환의 일부로서 K_ASME 설정
- K_ASME_D 에 대한 eKSI
- network_nonce
- device_temp_key
212
디바이스 도전
(eKSI, [E_device_root_key (device_temp_key)], network_nonce)
- device_nonce
- device_res =
KDF (device_temp_key, network_nonce, device_nonce)
214
디바이스 응답
(device_nonce, device_res)
216
K_ASME_D =
KDF(device_temp_key, K_ASME,
network_nonce, device_nonce) 산출
218
K_ASME_D =
KDF(device_temp_key, K_ASME,
network_nonce, device_nonce) 산출
217
K_ASME 에 기초하여
부가적인 보안 키들 생성
219
K_ASME 에 기초하여
부가적인 보안 키들 생성
220
K_ASME_D 에 의해 안전하게 보호된 메시지들 교환

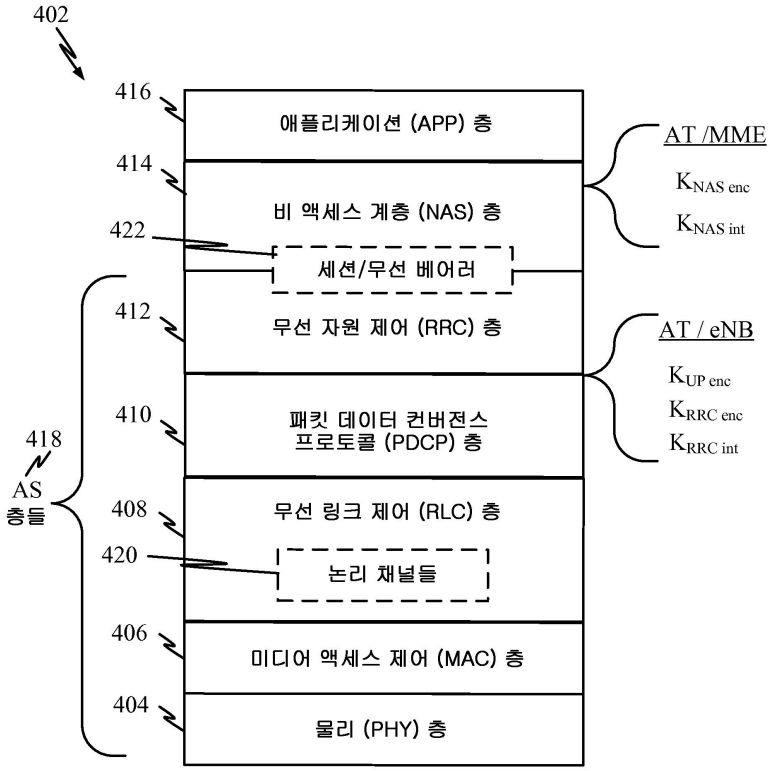
도면3a


300
UICC / HSS
K
302
CK, IK
304
306
AT / HSS
K_ASME
308
AT /MME
K_NAS-enc
305
K_NAS-int
311
313
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
315
317
319
300'
UICC / HSS
K
302
CK, IK
304
306
AT / HSS
K_ASME
308
AT /MME
307
디바이스 인증
K_ASME_D
309
K_NAS-enc
310
K_NAS-int
312
314
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
316
318
320

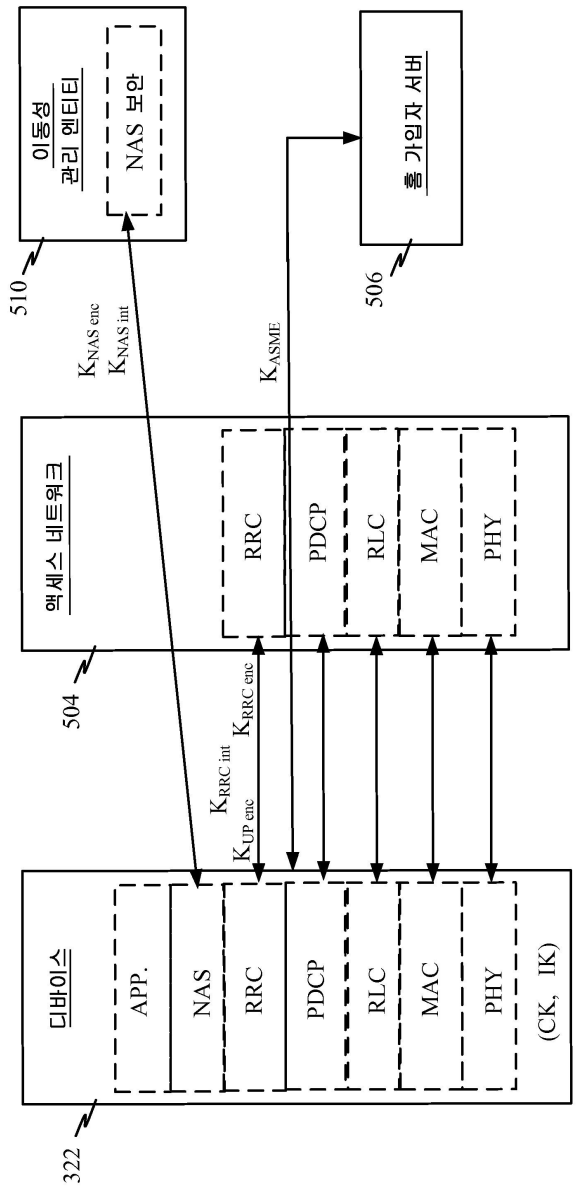
도면3b


디바이스
322
네트워크 엔티티
324
340
가입자 인증 요청
326
AKA
308
K_ASME
342
가입자 인증 응답
344
디바이스 인증 요청
328
Dev. Auth
309
K_ASME_D
346
디바이스 인증 응답
NAS 보안 모드 커맨드
310/312
K_NAS-enc, KNAS-int
NAS SMC
NAS 보안 모드 완료
316/318/320
RRC 보안 모드 커맨드
K_UP-enc, K_RRC-en, K_RRC-int
AS SMC
RRC 보안 모드 완료

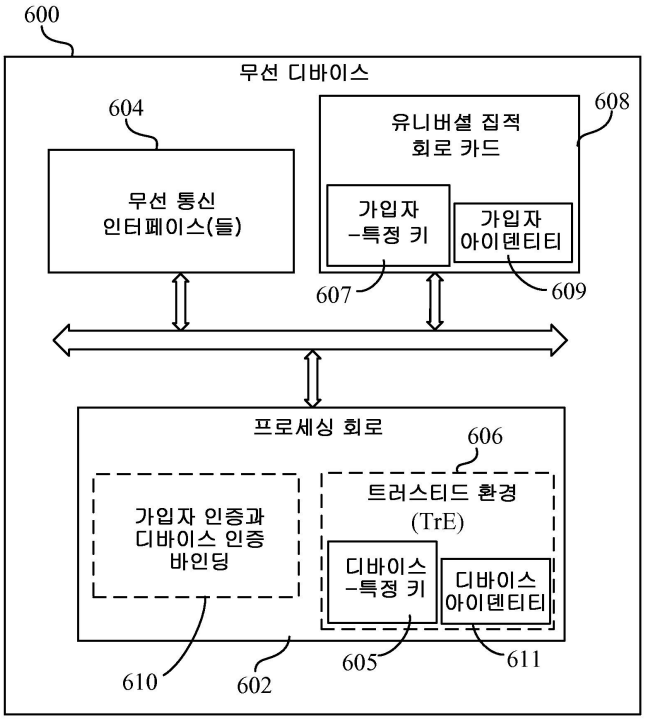
도면4


402
416
애플리케이션 (APP) 층
AT /MME
414
비 액세스 계층 (NAS) 층
$K_{NAS\ enc}$
$K_{NAS\ int}$
422
세션/무선 베어러
412
무선 자원 제어 (RRC) 층
AT / eNB
$K_{UP\ enc}$
$K_{RRC\ enc}$
$K_{RRC\ int}$
410
패킷 데이터 컨버전스 프로토콜 (PDCP) 층
418
AS 층들
408
무선 링크 제어 (RLC) 층
420
논리 채널들
406
미디어 액세스 제어 (MAC) 층
404
물리 (PHY) 층

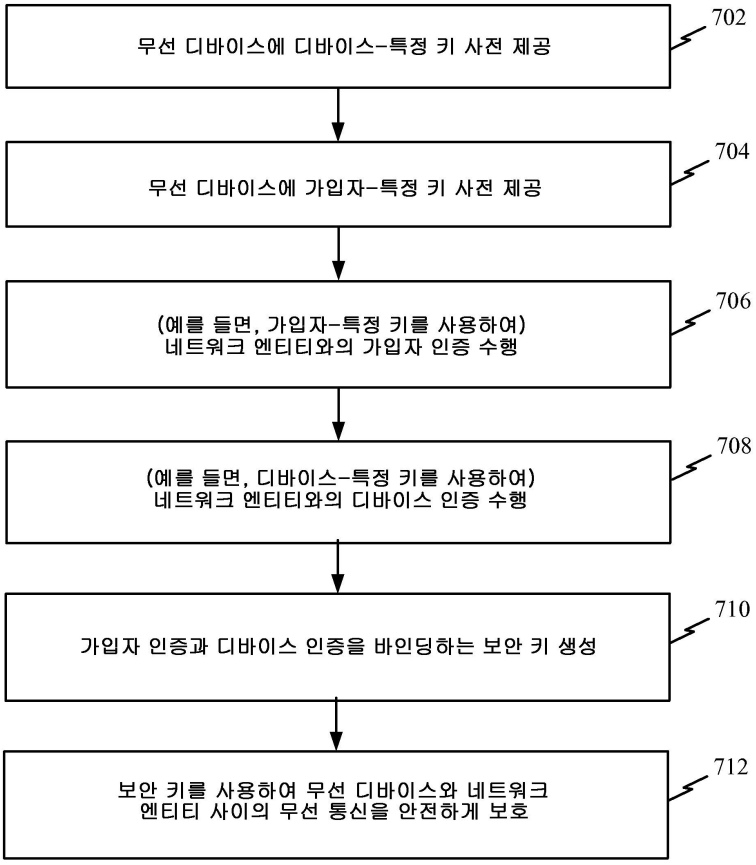
도면5


이동성
관리 엔티티
NAS 보안
510
홈 가입자 서버
506
$K_{NAS\ enc}$
$K_{NAS\ int}$
K_{ASME}
액세스 네트워크
RRC
PDCP
RLC
MAC
PHY
504
$K_{RRC\ enc}$
$K_{RRC\ int}$
$K_{UP\ enc}$
디바이스
APP.
NAS
RRC
PDCP
RLC
MAC
PHY
(CK, IK)
322

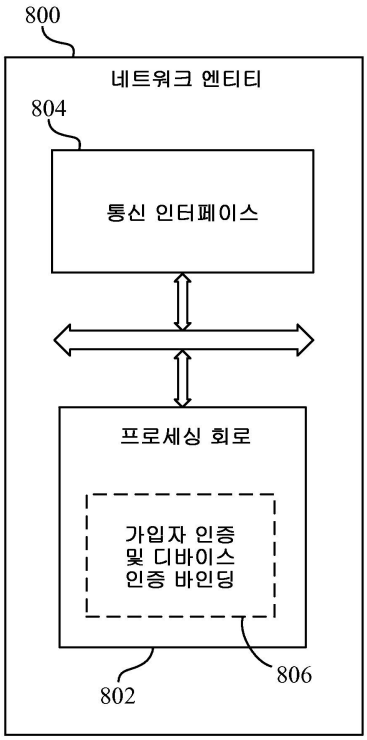
도면6


600
무선 디바이스
604
무선 통신
인터페이스(들)
608
유니버셜 집적
회로 카드
가입자
-특정 키
가입자
아이덴티티
607
609
프로세싱 회로
606
가입자 인증과
디바이스 인증
바인딩
트러스티드 환경
(TrE)
디바이스
-특정 키
디바이스
아이덴티티
610
602
605
611

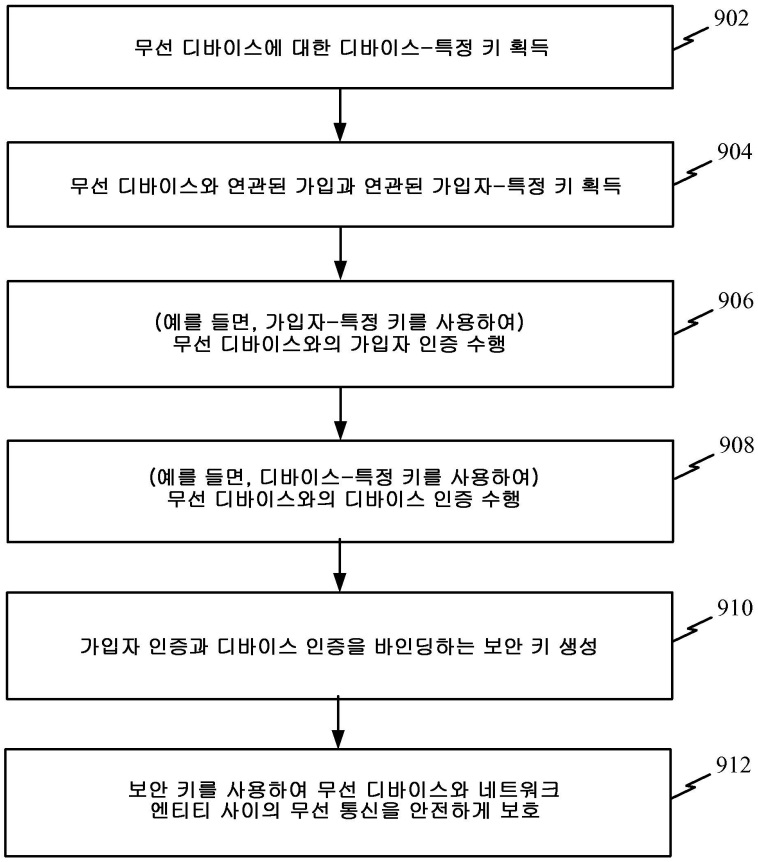
도면7


무선 디바이스에 디바이스-특정 키 사전 제공
702
무선 디바이스에 가입자-특정 키 사전 제공
704
(예를 들면, 가입자-특정 키를 사용하여)
네트워크 엔티티와의 가입자 인증 수행
706
(예를 들면, 디바이스-특정 키를 사용하여)
네트워크 엔티티와의 디바이스 인증 수행
708
가입자 인증과 디바이스 인증을 바인딩하는 보안 키 생성
710
보안 키를 사용하여 무선 디바이스와 네트워크
엔티티 사이의 무선 통신을 안전하게 보호
712

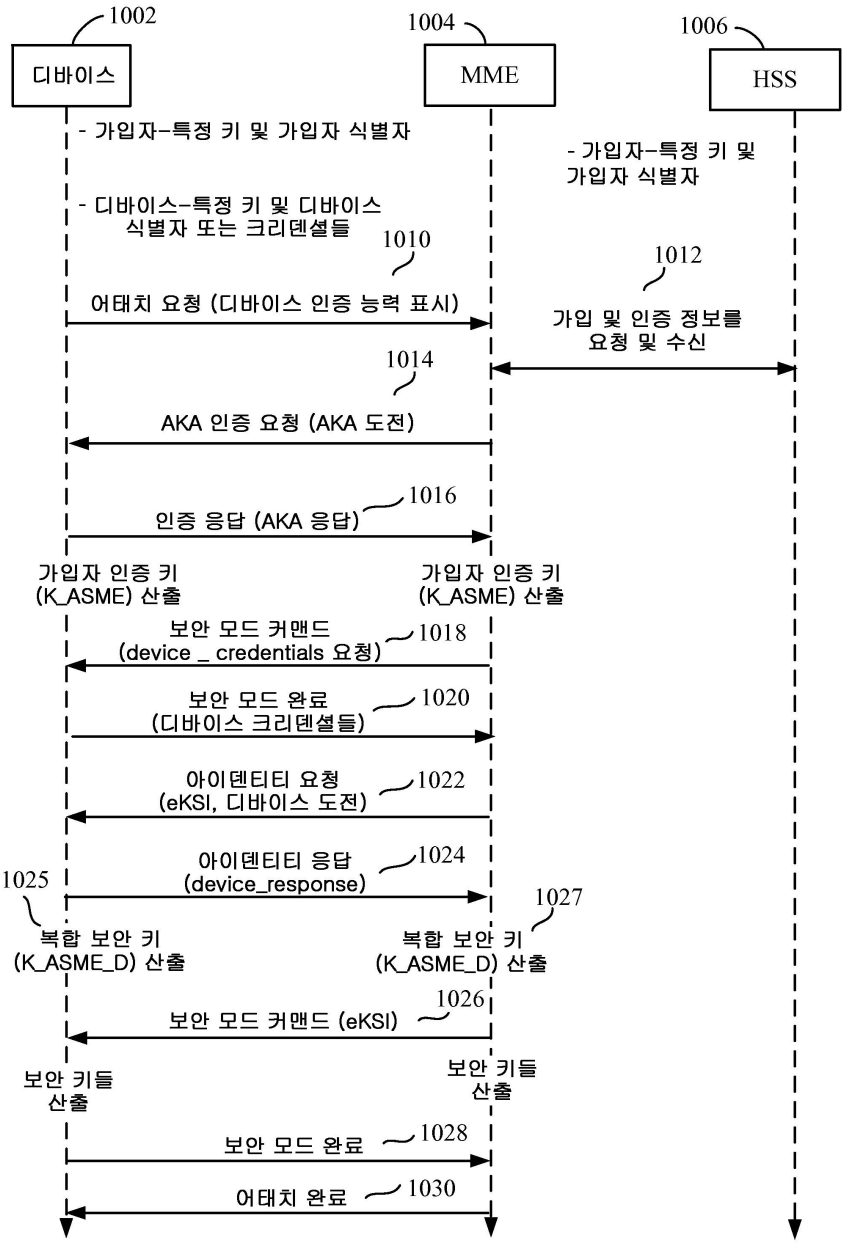
도면8


800
네트워크 엔티티
804
통신 인터페이스
프로세싱 회로
가입자 인증
및 디바이스
인증 바인딩
802
806

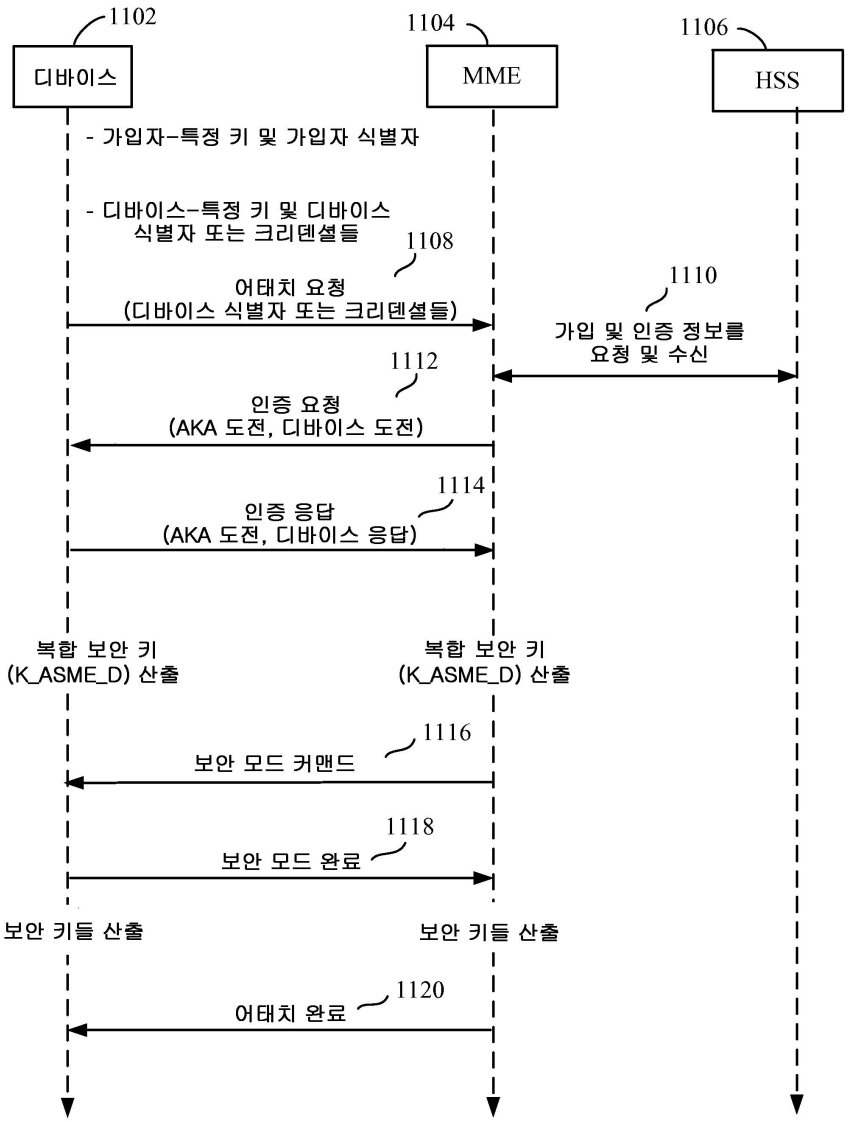
도면9


무선 디바이스에 대한 디바이스-특정 키 획득
902
무선 디바이스와 연관된 가입과 연관된 가입자-특정 키 획득
904
(예를 들면, 가입자-특정 키를 사용하여)
무선 디바이스와의 가입자 인증 수행
906
(예를 들면, 디바이스-특정 키를 사용하여)
무선 디바이스와의 디바이스 인증 수행
908
가입자 인증과 디바이스 인증을 바인딩하는 보안 키 생성
910
보안 키를 사용하여 무선 디바이스와 네트워크
엔티티 사이의 무선 통신을 안전하게 보호
912

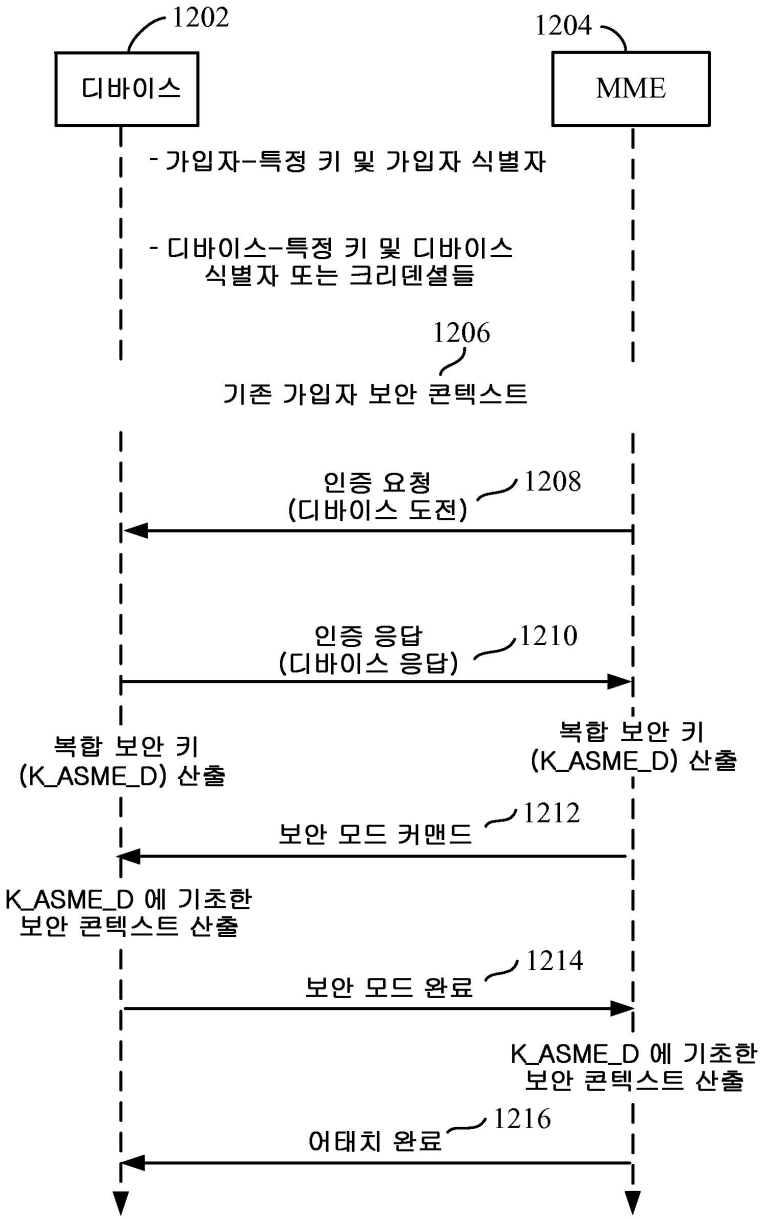
도면10


1002
디바이스
1004
MME
1006
HSS
- 가입자-특정 키 및 가입자 식별자
- 디바이스-특정 키 및 디바이스 식별자 또는 크리덴셜들
- 가입자-특정 키 및 가입자 식별자
1010
어태치 요청 (디바이스 인증 능력 표시)
1012
가입 및 인증 정보를 요청 및 수신
1014
AKA 인증 요청 (AKA 도전)
1016
인증 응답 (AKA 응답)
가입자 인증 키 (K_ASME) 산출
가입자 인증 키 (K_ASME) 산출
보안 모드 커맨드 (device _ credentials 요청)
1018
보안 모드 완료 (디바이스 크리덴셜들)
1020
아이덴티티 요청 (eKSI, 디바이스 도전)
1022
아이덴티티 응답 (device_response)
1024
1025
1027
복합 보안 키 (K_ASME_D) 산출
복합 보안 키 (K_ASME_D) 산출
보안 모드 커맨드 (eKSI)
1026
보안 키들 산출
보안 키들 산출
보안 모드 완료
1028
어태치 완료
1030

도면11


1102
디바이스
1104
MME
1106
HSS
- 가입자-특정 키 및 가입자 식별자
- 디바이스-특정 키 및 디바이스 식별자 또는 크리덴셜들
1108
어태치 요청
(디바이스 식별자 또는 크리덴셜들)
1110
가입 및 인증 정보를 요청 및 수신
1112
인증 요청
(AKA 도전, 디바이스 도전)
1114
인증 응답
(AKA 도전, 디바이스 응답)
복합 보안 키 (K_ASME_D) 산출
복합 보안 키 (K_ASME_D) 산출
1116
보안 모드 커맨드
1118
보안 모드 완료
보안 키들 산출
보안 키들 산출
1120
어태치 완료

도면12


1202
디바이스
1204
MME
- 가입자-특정 키 및 가입자 식별자
- 디바이스-특정 키 및 디바이스 식별자 또는 크리덴셜들
1206
기존 가입자 보안 콘텍스트
인증 요청
(디바이스 도전)
1208
인증 응답
(디바이스 응답)
1210
복합 보안 키
(K_ASME_D) 산출
복합 보안 키
(K_ASME_D) 산출
보안 모드 커맨드
1212
K_ASME_D 에 기초한
보안 콘텍스트 산출
보안 모드 완료
1214
K_ASME_D 에 기초한
보안 콘텍스트 산출
어태치 완료
1216