(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년09월01일
(11) 등록번호 10-2439686
(24) 등록일자 2022년08월30일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2021.01) *H04L 9/40* (2022.01)
H04W 12/06 (2021.01)
(52) CPC특허분류
H04W 12/08 (2021.01)
H04L 63/0823 (2013.01)
(21) 출원번호 10-2018-7003573
(22) 출원일자(국제) 2016년07월07일
심사청구일자 2021년06월21일
(85) 번역문제출일자 2018년02월05일
(65) 공개번호 10-2018-0039061
(43) 공개일자 2018년04월17일
(86) 국제출원번호 PCT/US2016/041402
(87) 국제공개번호 WO 2017/027134
국제공개일자 2017년02월16일
(30) 우선권주장
62/202,664 2015년08월07일 미국(US)
15/082,919 2016년03월28일 미국(US)
(56) 선행기술조사문헌
KR1020110067125 A*
US20120324225 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
이 수범
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
호른 개빈 버나드
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인코리아나

전체 청구항 수 : 총 37 항 심사관 : 이준석

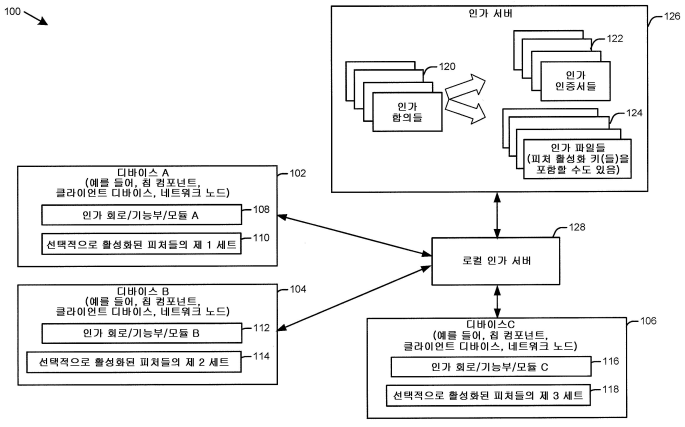
(54) 발명의 명칭 **디바이스의 피처들의 세트의 사용을 위한 인가를 검증**

(57) 요 약

디바이스는 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 그 권한의 증거 (제 1 증거) 를 획득한다. 인가 서버는 그 사설 키로 제 1 증거에 서명한다. 디바이스는 네트워크 서비스를 사용하기 위한 요청을 네트워크 노드로 전송한다. 디바이스는 제 1 증거를 네트워크 노드로 전송한다. 네트워크 노드는 인가

(뒷면에 계속)

대 표 도



서버의 공용 키를 사용하여 제 1 증거를 검증한다. 네트워크 노드는 네트워크 서비스를 사용하기 위한 요청을 허가한다. 디바이스는 네트워크 서비스를 제공하기 위한 네트워크 노드에 대한 권한의 증거 (제 2 증거)에 대한 요청을 전송한다. 디바이스는 다른 인가 서버에 의해 서명된, 제 2 증거를 획득하고, 네트워크 서비스를 사용하기 전에 제 2 증거를 검증한다. 제 1 증거 및 제 2 증거 각각은 선택적으로 활성화된 피처들의 리스트를 포함하고, 여기서 선택적으로 활성화된 피처들은 네트워크 서비스를 사용 또는 제공하기 위해 필요하다.

(52) CPC특허분류
H04L 63/0892 (2013.01)
H04L 63/12 (2013.01)
H04W 12/06 (2021.01)

(72) 발명자
스미 존
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
판카즈 라제쉬
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
라우즈 토마스
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775

명 세 서

청구범위

청구항 1

디바이스에서, 네트워크 서비스를 제공하기 위해 네트워크 노드에 의해 제공된 피처들의 제 1 세트의 리스팅을 네트워크 노드로부터 획득하는 단계;

상기 네트워크 서비스를 사용하기 위한 요청을 상기 네트워크 노드로 전송하는 단계;

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 권한의 증거에 대한 요청을 상기 네트워크 노드로 전송하는 단계;

인가 서버에 의해 서명된, 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 제 2 세트의 리스팅을 포함하는, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 상기 권한의 증거를 상기 네트워크 노드로부터 획득하는 단계;

상기 네트워크 노드에 대한 상기 권한의 증거를 검증하는 단계;

상기 네트워크 노드가 상기 네트워크 서비스를 제공하기 위해 피처들의 상기 제 2 세트를 사용하도록 유효하게 인가된 것을 확인하기 위해, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 제공된 피처들의 상기 제 1 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트에 포함되는 것을 확인하는 단계;

상기 디바이스에 의해, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 필요한 피처들의 제 3 세트의 리스팅을 식별하는 단계; 및

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 필요한 피처들의 상기 제 3 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트에 포함되는지 여부를 결정하는 것에 기초하여 상기 네트워크 서비스를 사용하는 단계를 포함하는, 방법.

청구항 2

제 1 항에 있어서,

상기 디바이스는 칩 컴포넌트, 클라이언트 디바이스, 네트워크 액세스 노드, 이동성 관리 엔티티, 또는 게이트웨이 디바이스인, 방법.

청구항 3

제 1 항에 있어서,

상기 디바이스는 클라이언트 디바이스 또는 칩 컴포넌트이고, 상기 네트워크 노드는 네트워크 액세스 노드인, 방법.

청구항 4

제 1 항에 있어서,

제 1 인가 서버에 의해 서명된, 상기 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위해 상기 디바이스에 대한 권한의 증거를 획득하는 단계로서, 상기 디바이스에서 선택적으로 활성화된 피처들의 상기 제 1 세트가 상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 사용된 제 1 선택적으로 활성화된 피처들을 포함하고, 상기 디바이스에 대한 상기 권한의 증거는 상기 제 1 인가 서버에서 비롯되고, 상기 제 1 인가 서버의 사설 키로 서명되며, 상기 디바이스에서 선택적으로 활성화된 피처들의 상기 제 1 세트의 리스팅을 포함하는, 상기 권한의 증거를 획득하는 단계;

상기 제 1 인가 서버의 공용 키를 사용하여 상기 디바이스에서 선택적으로 활성화된 피처들의 상기 제 1 세트의 상기 리스팅을 검증함으로써 상기 디바이스에 대한 상기 권한의 증거를 검증하는 단계;

상기 디바이스의 공용 키로 암호화된, 상기 제 1 선택적으로 활성화된 피처들과 연관된 피처 활성화 키들을 획득하는 단계;

상기 디바이스에만 알려진, 상기 디바이스의 사설 키를 사용하여, 상기 피처 활성화 키들을 해독하는 단계; 및

상기 피처 활성화 키들로 상기 제 1 선택적으로 활성화된 피처들을 활성화시키고/시키거나 활성화를 유지하는 단계를 더 포함하는, 방법.

청구항 5

제 1 항에 있어서,

상기 네트워크 노드에 대한 상기 권한의 증거는 상기 인가 서버에서 비롯되고, 상기 인가 서버의 사설 키로 서명되며,

상기 방법은,

상기 인가 서버의 공용 키를 사용하여 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트의 상기 리스팅을 검증함으로써 상기 네트워크 노드에 대한 상기 권한의 증거를 검증하는 단계를 더 포함하는, 방법.

청구항 6

제 4 항에 있어서,

상기 제 1 인가 서버는 로컬 인가 서버인, 방법.

청구항 7

삭제

청구항 8

제 1 항에 있어서,

상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 사용된 제 1 선택적으로 활성화된 피처들을 포함하는, 상기 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 상기 디바이스에 대한 권한의 증거는 제 1 인가 서버에서 비롯되고, 상기 디바이스에서, 상기 제 1 인가 서버로부터 획득되며,

상기 네트워크 노드에 대한 상기 권한의 증거는 상기 인가 서버에서 비롯되고, 상기 디바이스에서, 상기 네트워크 노드로부터 획득되는, 방법.

청구항 9

제 8 항에 있어서,

상기 제 1 인가 서버 및 상기 인가 서버는 하나의 인가 서버인, 방법.

청구항 10

제 8 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는 피처 활성화 프로세스 동안 상기 제 1 인가 서버로부터 획득되고, 이 동안 상기 디바이스는 상기 디바이스에서 선택적으로 활성화된 피처들의 상기 제 1 세트를 활성화시키기 위한 인가를 획득하는, 방법.

청구항 11

제 8 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는 인가 인증서를 나타내는 데이터인, 방법.

청구항 12

제 8 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는, 상기 디바이스가 상기 디바이스에서 선택적으로 활성화된 피처들의 상기 제 1 세트를 활성화시키도록 인가된다는 것을 나타내는 인가 합의를 나타내는 데이터인, 방법.

청구항 13

디바이스로서,

네트워크 통신 회로; 및

상기 네트워크 통신 회로에 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

네트워크 서비스를 제공하기 위해 네트워크 노드에 의해 제공된 피처들의 제 1 세트의 리스팅을 상기 네트워크 노드로부터 획득하고;

상기 네트워크 서비스를 사용하기 위한 요청을 상기 네트워크 노드로 전송하고;

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 권한의 증거에 대한 요청을 상기 네트워크 노드로 전송하고;

인가 서버에 의해 서명된, 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 제 2 세트의 리스팅을 포함하는, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 상기 권한의 증거를 상기 네트워크 노드로부터 획득하고;

상기 네트워크 노드에 대한 상기 권한의 증거를 검증하고;

상기 네트워크 노드가 상기 네트워크 서비스를 제공하기 위해 피처들의 상기 제 2 세트를 사용하도록 유효하게 인가된 것을 확인하기 위해, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 제공된 피처들의 상기 제 1 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트에 포함되는 것을 확인하고;

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 필요한 피처들의 제 3 세트의 리스팅을 식별하고; 그리고

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 필요한 피처들의 상기 제 3 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트에 포함되는지 여부를 결정하는 것에 기초하여 상기 네트워크 서비스를 사용하도록

구성되는, 디바이스.

청구항 14

제 13 항에 있어서,

상기 디바이스는 칩 컴포넌트, 클라이언트 디바이스, 네트워크 액세스 노드, 이동성 관리 엔티티, 또는 게이트웨이 디바이스인, 디바이스.

청구항 15

제 13 항에 있어서,

상기 프로세싱 회로는 또한,

제 1 인가 서버에 의해 서명된, 상기 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위해 상기 디바이스에 대한 권한의 증거를 획득하되, 상기 디바이스에서 선택적으로 활성화된 피처들의 상기 제 1 세트가 상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 사용된 제 1 선택적으로 활성화된 피처들을 포함하고, 상기 디바이스에 대한 상기 권한의 증거는 상기 제 1 인가 서버에서 비롯되고, 상기 제 1 인가 서버의 사설 키로 서명되며, 상기 디바이스의 선택적으로 활성화된 피처들의 상기 제 1 세트의 리스팅을 포함하고;

상기 제 1 인가 서버의 공용 키를 사용하여 상기 디바이스의 선택적으로 활성화된 피처들의 상기 제 1 세트의 상기 리스팅을 검증함으로써 상기 디바이스에 대한 상기 권한의 증거를 검증하고;

상기 디바이스의 공용 키로 암호화된, 상기 제 1 선택적으로 활성화된 피처들과 연관된 피처 활성화 키들을 획득하고;

상기 디바이스에만 알려진, 상기 디바이스의 사설 키를 사용하여, 상기 피처 활성화 키들을 해독하며;

상기 피처 활성화 키들로 상기 제 1 선택적으로 활성화된 피처들을 활성화시키고/시키거나 활성화를 유지하도록

구성되는, 디바이스.

청구항 16

제 13 항에 있어서,

상기 네트워크 노드에 대한 상기 권한의 증거는 상기 인가 서버에서 비롯되고, 상기 인가 서버의 사설 키로 서명되며,

상기 프로세싱 회로는 또한,

상기 인가 서버의 공용 키를 사용하여 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트의 상기 리스팅을 검증함으로써 상기 네트워크 노드에 대한 상기 권한의 증거를 검증하도록

구성되는, 디바이스.

청구항 17

제 15 항에 있어서,

상기 제 1 인가 서버는 로컬 인가 서버인, 디바이스.

청구항 18

삭제

청구항 19

제 13 항에 있어서,

상기 프로세싱 회로는 또한,

상기 디바이스에서, 제 1 인가 서버에 의해 서명된, 상기 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위해 상기 디바이스에 대한 권한의 증거를 획득하는 것으로서, 상기 디바이스에 대한 상기 권한의 증거는 상기 제 1 인가 서버에서 비롯되는, 상기 디바이스에 대한 상기 권한의 증거를 획득하며;

상기 디바이스에서, 상기 네트워크 노드로부터 상기 네트워크 노드에 대한 상기 권한의 증거를 획득하는 것으로서, 상기 네트워크 노드에 대한 상기 권한의 증거는 상기 인가 서버에서 비롯되는, 상기 네트워크 노드에 대한 상기 권한의 증거를 획득하도록

구성되는, 디바이스.

청구항 20

제 19 항에 있어서,

상기 제 1 인가 서버 및 상기 인가 서버는 하나의 인가 서버인, 디바이스.

청구항 21

제 19 항에 있어서,

상기 프로세싱 회로는 또한, 피처 활성화 프로세스 동안 상기 제 1 인가 서버로부터 상기 디바이스에 대한 상기

권한의 증거를 획득하도록 구성되고, 이 동안 상기 디바이스는 상기 디바이스에서 선택적으로 활성화된 피처들의 상기 제 1 세트를 활성화시키기 위한 인가를 획득하는, 디바이스.

청구항 22

제 19 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는 인가 인증서를 나타내는 데이터인, 디바이스.

청구항 23

제 19 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는, 상기 디바이스가 상기 디바이스에서 선택적으로 활성화된 피처들의 상기 제 1 세트를 활성화시키도록 인가된다는 것을 나타내는 인가 합의를 나타내는 데이터인, 디바이스.

청구항 24

네트워크 노드에 의해, 디바이스로 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 제공된 피처들의 제 1 세트의 리스팅을 상기 디바이스로 전송하는 단계;

상기 네트워크 서비스를 사용하기 위한 요청을 상기 디바이스로부터 획득하는 단계;

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 권한의 증거에 대한 요청을 획득하는 단계;

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 제공된 피처들의 상기 제 1 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 제 2 세트에 포함되는 것을 확인함으로써 상기 네트워크 노드는 상기 네트워크 서비스를 제공하기 위해 유효하게 인가된 것의 확인을 허용하기 위해, 제 1 인가 서버에 의해 서명된, 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 제 2 세트의 리스팅을 포함하는, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 상기 권한의 증거를 상기 디바이스로 전송하는 단계;

제 2 인가 서버에 의해 서명된, 상기 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 제 1 세트의 리스팅을 포함하는, 상기 디바이스에 대한 권한의 증거를 획득하는 단계;

상기 디바이스에 대한 상기 권한의 증거를 검증하는 단계;

상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 제 3 세트의 리스팅을 식별하는 단계; 및

상기 디바이스에 대한 상기 권한의 증거를 검증하고 상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 상기 제 3 세트가 상기 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 상기 제 1 세트에 포함되는지 여부를 결정한 결과들에 기초하여 상기 네트워크 서비스를 사용하기 위한 상기 요청에 대한 응답을 전송하는 단계를 포함하는, 방법.

청구항 25

제 24 항에 있어서,

상기 네트워크 노드는 네트워크 액세스 노드, 이동성 관리 엔티티, 또는 게이트웨이 디바이스인, 방법.

청구항 26

제 24 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는 상기 제 2 인가 서버에서 비롯되고, 상기 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 상기 제 1 세트의 상기 리스팅은 상기 제 2 인가 서버의 사설 키로 서명되고;

상기 방법은,

상기 제 2 인가 서버의 공용 키를 사용하여 상기 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 상기 제 1 세트의 상기 리스팅을 검증함으로써 상기 디바이스에 대한 상기 권한의 증거를 검증하는 단계를

더 포함하는, 방법.

청구항 27

제 24 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는 상기 제 2 인가 서버에서 비롯되고, 상기 디바이스로부터 상기 네트워크 노드에서 획득되는, 방법.

청구항 28

제 24 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는 상기 제 2 인가 서버에서 비롯되고, 홈 가입자 서버 (HSS) 로부터, 상기 디바이스의 능력 프로파일의 형태로, 상기 네트워크 노드에서 획득되는, 방법.

청구항 29

제 24 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는 인가 인증서를 나타내는 데이터인, 방법.

청구항 30

제 24 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는, 상기 디바이스가 상기 디바이스에서 활성화되도록 인가된 상기 선택적으로 활성화된 피처들의 상기 제 1 세트를 활성화시키도록 인가된다는 것을 나타내는 인가 합의를 나타내는 데이터인, 방법.

청구항 31

제 24 항에 있어서,

선택적으로 활성화된 피처들의 상기 제 3 세트를 식별하는 단계는,

상기 제 2 인가 서버에 의해 유지된, 인가된 선택적으로 활성화된 피처들의 모델-특정 및 디바이스-특정 리스트 중 적어도 하나로부터 상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 상기 제 3 세트의 상기 리스팅을 도출하는 단계를 포함하는, 방법.

청구항 32

제 24 항에 있어서,

선택적으로 활성화된 피처들의 상기 제 3 세트를 식별하는 단계는,

상기 제 2 인가 서버에 의해 유지된, 라이선싱 가능한 선택적으로 활성화된 피처들의 모델-특정 및 디바이스-특정 리스트 중 적어도 하나로부터 상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 상기 제 3 세트의 상기 리스팅을 도출하는 단계를 포함하는, 방법.

청구항 33

제 24 항에 있어서,

상기 디바이스가 상기 디바이스에 대한 상기 권한의 증거에 포함된 상기 디바이스의 공용 키에 대응하는 사설 키를 홀딩한다는 것을 확인하는 단계를 더 포함하고,

상기 네트워크 서비스를 사용하기 위한 상기 요청에 대한 응답을 전송하는 단계는 또한, 상기 확인하는 단계의 결과에 기초하는, 방법.

청구항 34

네트워크 노드로서,

네트워크 통신 회로; 및

상기 네트워크 통신 회로에 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

디바이스로 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 제공된 피처들의 제 1 세트의 리스팅을 상기 디바이스로 전송하고;

상기 네트워크 서비스를 사용하기 위한 요청을 상기 디바이스로부터 획득하고;

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 권한의 증거에 대한 요청을 획득하고;

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 제공된 피처들의 상기 제 1 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 제 2 세트에 포함되는 것을 확인함으로써 상기 네트워크 노드는 상기 네트워크 서비스를 제공하기 위해 유효하게 인가된 것의 확인을 허용하기 위해, 제 1 인가 서버에 의해 서명된, 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 제 2 세트의 리스팅을 포함하는, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 상기 권한의 증거를 상기 디바이스로 전송하고;

제 2 인가 서버에 의해 서명된, 상기 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 제 1 세트의 리스팅을 포함하는, 상기 디바이스에 대한 권한의 증거를 획득하고;

상기 디바이스에 대한 상기 권한의 증거를 검증하고;

상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 제 3 세트의 리스팅을 식별하고; 그리고

상기 디바이스에 대한 상기 권한의 증거를 검증하고 상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 상기 제 3 세트가 상기 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 상기 제 1 세트에 포함되는지 여부를 결정한 결과들에 기초하여 상기 네트워크 서비스를 사용하기 위한 상기 요청에 대한 응답을 전송하도록

구성되는, 네트워크 노드.

청구항 35

제 34 항에 있어서,

상기 네트워크 노드는 네트워크 액세스 노드, 이동성 관리 엔티티, 또는 게이트웨이 디바이스인, 네트워크 노드.

청구항 36

제 34 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는 상기 제 2 인가 서버에서 비롯되고, 상기 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 상기 제 1 세트의 상기 리스팅은 상기 제 2 인가 서버의 사설 키로 서명되고;

상기 프로세싱 회로는 또한,

상기 제 2 인가 서버의 공용 키를 사용하여 상기 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 상기 제 1 세트의 상기 리스팅을 검증함으로써 상기 디바이스에 대한 상기 권한의 증거를 검증하도록

구성되는, 네트워크 노드.

청구항 37

제 34 항에 있어서,

상기 디바이스에 대한 상기 권한의 증거는 상기 제 2 인가 서버에서 비롯되고,

상기 프로세싱 회로는 또한,

상기 디바이스로부터, 상기 네트워크 노드에서 상기 디바이스에 대한 상기 권한의 증거를 획득하도록

구성되는, 네트워크 노드.

청구항 38

제 34 항에 있어서,

상기 선택적으로 활성화된 피처들의 상기 제 3 세트를 식별하는 경우,

상기 프로세싱 회로는 또한,

상기 제 2 인가 서버에 의해 유지된, 인가된 선택적으로 활성화된 피처들의 모델-특정 및 디바이스-특정 리스트 중 적어도 하나로부터 상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 상기 제 3 세트의 상기 리스팅을 도출하도록

구성되는, 네트워크 노드.

청구항 39

제 34 항에 있어서,

상기 선택적으로 활성화된 피처들의 상기 제 3 세트를 식별하는 경우,

상기 프로세싱 회로는 또한,

상기 제 2 인가 서버에 의해 유지된, 라이선싱 가능한 선택적으로 활성화된 피처들의 모델-특정 및 디바이스-특정 리스트 중 적어도 하나로부터 상기 네트워크 서비스를 사용하기 위해 상기 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 상기 제 3 세트의 상기 리스팅을 도출하도록

구성되는, 네트워크 노드.

청구항 40

삭제

청구항 41

삭제

청구항 42

삭제

청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

청구항 49

삭제

청구항 50

삭제

발명의 설명

기 술 분 야

[0001] **관련 출원들의 상호참조**

[0002] 본 출원은 2015년 8월 7일자로 미국 특허 상표국에 출원된 가출원 제 62/202,664 호, 및 2016년 3월 28일자로 미국 특허 상표국에 출원된 정규출원 제 15/082,919 호의 우선권 및 이익을 주장하고, 이들 전체 내용들은 참조로서 본원에 포함된다.

[0003] **기술분야**

[0004] 본 출원은 선택적으로 활성화될 수도 있는 피처들의 세트를 활성화시키고, 이에 의해 디바이스와 인가를 검증하는 엔티티 간의 서비스를 개시 또는 유지하기 위한, 디바이스에 의해 수신된 인가의 검증에 관한 것이다.

배 경 기 술

[0005] 대부분의 통신 디바이스들 (예를 들어, 칩 컴포넌트들, 클라이언트 디바이스들, 네트워크 노드들) 은 다수의 피처들을 제공한다. 이 피처들은 하드웨어 및/또는 소프트웨어에서 구현될 수도 있다.

[0006] 통신 디바이스의 일부 피처들은, 엔티티가 통신 디바이스를 획득하는 경우 활성화될 수도 있다. 다른 피처들은 활성화되지 않을 수도 있다. 예를 들어, 제조자, 서브컴포넌트 제조자, 또는 주문자 상표부착 제조자 (OEM) 가 통신 디바이스에 포함된 하나 이상의 피처들을 갖는 통신 디바이스의 상이한 모델들 (예를 들어, 버전들) 을 생산하는 것이 가능할 수도 있고, 여기서 하나 이상의 피처들은 디바이스 모델에 기초하여 활성화 또는 비활성화된다. 결과적으로, 통신 디바이스의 피처들의 서브세트 (예를 들어, 전체 보다 적은 세트) 는 최종 제품에서 가동될 수도 있다. 예를 들어, 양자 모두의 모델들이 피처를 구현하는데 사용된 모든 하드웨어 및 소프트웨어를 포함하더라도, 제조자는 제 1 모델에서 피처를 활성화시키지만 제 2 모델에서는 피처를 활성화시키지 않을 수도 있다. 부가적으로 또는 대안으로, 통신 디바이스 상에 저장된 프로세싱 회로 판독가능 명령들의 일부들은 피처가 활성화되지 못하게 하도록 실행되지 않을 수도 있다. 하드웨어 및/또는 소프트웨어를 인에이블링 및/또는 디스에이블링하는 것은 최종 제품에서 활성화되는 피처들의 수를 증가시키고/시키거나 감소시키고, 예를 들어 최종 제품의 가격에 영향을 줄 수도 있다.

[0007] 따라서, 통신 디바이스가 전개되는 경우, 통신 디바이스는 (예를 들어, 하드웨어 및/또는 소프트웨어 또는 펌웨어의 면에서) 그 동작의 부분으로서 소정 피처들을 수행할 수 있지만 소정 피처들을 사용하도록 인가되지 않을 수도 있다. 피처들을 사용하기 위한 권한에 대한 제한들은, 예를 들어 통신 디바이스에 이용 가능한 피처들 및/또는 서비스들의 사용들을 제한하는 구매 합의에 기초할 수도 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0008] 본원에 개시된 양태들은 전자 디바이스의 하나 이상의 피처들의 세트의 사용을 위한 인가를 동적으로 검증하는

방법들 및 장치를 제공한다.

[0009] 일부 양태들에서, 방법은 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 획득하는 단계를 포함할 수도 있다. 디바이스에 대한 권한의 증거는 제 1 인가 서버에 의해 서명될 수 있다. 방법은 네트워크 서비스를 사용하기 위한 요청을 네트워크 노드로 전송하는 단계를 포함할 수 있고, 여기서 선택적으로 활성화된 피처들의 제 1 세트는 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 제 1 선택적으로 활성화된 피처들을 포함한다. 디바이스는, 네트워크 서비스를 사용하기 위한 요청을 전송하는 것에 응답하여, 디바이스에 대한 권한의 증거에 대한 요청을 네트워크 노드로부터 획득할 수도 있다. 디바이스는 디바이스에 대한 권한의 증거 및 네트워크 서비스를 제공하기 위한 네트워크 노드에 대한 권한의 증거에 대한 요청을 네트워크 노드로 전송할 수도 있다. 디바이스는, 제 2 인가 서버에 의해 서명된, 네트워크 노드에서 선택적으로 활성화된 피처들의 제 2 세트를 사용하기 위한 네트워크 노드에 대한 권한의 증거를 네트워크 노드로부터 획득할 수도 있고, 여기서 선택적으로 활성화된 피처들의 제 2 세트는 네트워크 서비스를 제공하기 위해 네트워크 노드에 의해 필요한 제 2 선택적으로 활성화된 피처들을 포함한다. 방법은 또한, 네트워크 서비스를 사용하기 전에 네트워크 노드에 대한 권한의 증거를 검증하는 단계를 포함할 수도 있다.

[0010] 일부 예들에서, 디바이스는 칩 컴포넌트, 클라이언트 디바이스, 네트워크 액세스 노드, 이동성 관리 엔티티, 또는 게이트웨이 디바이스일 수 있다. 일 예에서, 디바이스는 클라이언트 디바이스 또는 칩 컴포넌트일 수 있고, 네트워크 노드는 네트워크 액세스 노드일 수 있다.

[0011] 일 양태에서, 디바이스에 대한 권한의 증거는 제 1 인가 서버에서 비롯될 수 있고, 제 1 인가 서버의 사설 키로 서명될 수 있으며, 제 1 선택적으로 활성화된 피처들의 리스팅을 포함할 수 있다. 방법은 제 1 인가 서버의 공용 키를 사용하여 제 1 선택적으로 활성화된 피처들의 리스팅을 검증함으로써 디바이스에 대한 권한의 증거를 검증하는 단계를 더 포함할 수도 있다. 방법은 또한, 디바이스의 공용 키로 암호화된, 제 1 선택적으로 활성화된 피처들과 연관된 피처 활성화 키들을 획득하는 단계, 디바이스에만 알려진 디바이스의 사설 키를 사용하여 피처 활성화 키들을 해독하는 단계, 및 피처 활성화 키들로 제 1 선택적으로 활성화된 피처들을 활성화시키고/시키거나 활성화를 유지하는 단계를 더 포함할 수도 있다.

[0012] 네트워크 노드에 대한 권한의 증거가 제 2 인가 서버에서 비롯되고, 제 2 인가 서버의 사설 키로 서명되며, 제 2 선택적으로 활성화된 피처들의 리스팅을 포함하는 예에서, 방법은 제 2 인가 서버의 공용 키를 사용하여 제 2 선택적으로 활성화된 피처들의 리스팅을 검증함으로써 네트워크 노드에 대한 권한의 증거를 검증하는 단계를 더 포함할 수도 있다.

[0013] 일 양태에서, 제 1 인가 서버는 로컬 인가 서버일 수 있다.

[0014] 다른 양태에서, 방법은 네트워크 서비스를 사용하기 위해 네트워크 노드에 의해 필요한 선택적으로 활성화된 피처들의 제 3 세트를 식별하는 단계, 및 선택적으로 활성화된 피처들의 제 3 세트가 선택적으로 활성화된 피처들의 제 2 세트에 포함되는지 여부를 결정하는 것에 기초하여 네트워크 서비스를 사용하는 단계를 더 포함할 수도 있다.

[0015] 일 구현에서, 디바이스에 대한 권한의 증거는 제 1 인가 서버에서 비롯되고, 디바이스에서 제 1 인가 서버로부터 획득되며, 네트워크 노드에 대한 권한의 증거는 제 2 인가 서버에서 비롯되고, 디바이스에서 네트워크 노드로부터 획득된다. 일 양태에서, 제 1 인가 서버 및 제 2 인가 서버는 하나의 인가 서버일 수 있다.

[0016] 일부 양태들에서, 디바이스에 대한 권한의 증거는 피처 활성화 프로세스 동안 제 1 인가 서버로부터 획득되고, 이 동안 디바이스는 제 1 선택적으로 활성화된 피처들을 활성화시키기 위한 권한을 획득한다. 일부 양태들에서, 디바이스에 대한 권한의 증거는 인가 인증서를 나타내는 데이터일 수 있다. 다른 양태들에서, 디바이스에 대한 권한의 증거는, 디바이스가 제 1 선택적으로 활성화된 피처들을 활성화시키도록 인가된다는 것을 나타내는 인가 합의를 나타내는 데이터일 수 있다.

[0017] 일 예에서, 디바이스는 네트워크 통신 회로 및 네트워크 통신 회로에 커플링된 프로세싱 회로를 포함한다. 프로세싱 회로는 전술된 방법(들)을 수행하도록 구성될 수도 있다.

[0018] 다른 양태에서, 네트워크 노드에서 동작하는 방법은 디바이스로부터, 네트워크 서비스를 사용하기 위한 요청을 획득하는 단계를 포함할 수도 있다. 방법은 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 제 1 세트에 대한 권한의 증거를 획득하는 단계를 포함할 수도 있다. 디바이스에 대한 권한의 증거는 인가 서버에 의해 서명될 수 있다. 디바이스는 또한, 디바이스에 대한 권한의 증거를 검증하는 단계를

포함할 수도 있다. 방법은, 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 제 2 세트를 식별하는 단계, 및 디바이스에 대한 권한의 증거를 검증하고 선택적으로 활성화된 피처들의 제 2 세트가 선택적으로 활성화된 피처들의 제 1 세트에 포함되는지 여부를 결정한 결과들에 기초하여 요청에 대한 응답을 전송하는 단계를 더 포함할 수도 있다. 일부 양태들에서, 네트워크 노드는 네트워크 액세스 노드, 이동성 관리 엔티티, 또는 게이트웨이 디바이스일 수 있다.

[0019] 일 예에서, 선택적으로 활성화된 피처들의 제 1 세트는 제 1 선택적으로 활성화된 피처들을 포함하고, 디바이스에 대한 권한의 증거는 인가 서버에서 비롯된다. 디바이스에 대한 권한의 증거는, 인가 서버의 사설 키로 서명된, 제 1 선택적으로 활성화된 피처들의 리스팅을 포함할 수 있다. 방법은 인가 서버의 공용 키를 사용하여 제 1 선택적으로 활성화된 피처들의 리스팅을 검증함으로써 디바이스에 대한 권한의 증거를 검증하는 단계를 더 포함할 수 있다.

[0020] 일 양태에서, 디바이스에 대한 권한의 증거는 인가 서버에서 비롯될 수 있고, 네트워크 노드에서 디바이스로부터 획득될 수 있다. 다른 양태에서, 디바이스에 대한 권한의 증거는 인가 서버에서 비롯될 수 있고, 홈 가입자 서버 (HSS) 로부터, 디바이스의 능력 프로파일의 형태로, 네트워크 노드에서 획득될 수 있다.

[0021] 일 구현에서, 디바이스에 대한 권한의 증거는 인가 인증서를 나타내는 데이터일 수 있다. 다른 구현에서, 디바이스에 대한 권한의 증거는, 디바이스가 선택적으로 활성화된 피처들의 제 1 세트를 활성화시키도록 인가된다는 것을 나타내는 인가 합의를 나타내는 데이터일 수 있다.

[0022] 일 양태에서, 선택적으로 활성화된 피처들의 제 2 세트를 식별하는 단계는 인가 서버에 의해 유지된, 인가된 선택적으로 활성화된 피처들의 모델-특정 및/또는 디바이스-특정 리스트로부터 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 선택적으로 활성화된 피처들을 도출하는 단계를 포함할 수 있다. 다른 양태에서, 선택적으로 활성화된 피처들의 제 2 세트를 식별하는 단계는 인가 서버에 의해 유지된 라이선싱 가능한 선택적으로 활성화된 피처들의 모델-특정 및/또는 디바이스-특정 리스트로부터 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 선택적으로 활성화된 피처들을 도출하는 단계를 포함할 수 있다.

[0023] 일 구현에서, 방법은, 디바이스가 디바이스에 대한 권한의 증거에 포함된 디바이스의 공용 키에 대응하는 사설 키를 홀딩한다는 것을 확인하는 단계를 포함할 수도 있고, 여기서 요청에 대한 응답을 전송하는 것은 또한, 확인하는 것의 결과에 기초한다.

[0024] 일 양태에서, 네트워크 노드는 네트워크 통신 회로 및 네트워크 통신 회로에 커플링된 프로세싱 회로를 포함할 수 있다. 프로세싱 회로는 전술된 방법(들)을 수행하도록 구성될 수도 있다.

[0025] 일 양태에서, 서버에서 동작하는 방법은, 디바이스의 선택적으로 활성화된 피처들의 제 1 리스트를 획득하는 단계, 및 제 1 리스트에 기초하여 서버에 저장된, 디바이스의 선택적으로 활성화된 피처들의 제 2 리스트를 업데이트하여 제 2 리스트에서의 적어도 하나의 선택적으로 활성화된 피처의 인가 스테이터스에 대한 변화를 반영하는 단계를 포함할 수도 있고, 여기서 제 2 리스트는 디바이스의 가입 프로파일과 연관된다.

[0026] 일 예에서, 서버는 홈 가입자 서버 (HSS) 일 수 있다.

[0027] 일 구현에서, 방법은, 디바이스의 능력에 관련한 질의에 응답하여, 디바이스의 선택적으로 활성화된 피처들의 제 2 리스트를 포함하는 능력 프로파일을 전송하는 단계를 더 포함할 수 있다.

[0028] 일 양태에서, 선택적으로 활성화된 피처들의 제 1 리스트는 인가 서버에서 비롯되고 인가 서버의 사설 키로 서명되며, 방법은 인가 서버의 공용 키를 사용하여 선택적으로 활성화된 피처들의 제 1 리스트를 검증하는 단계를 더 포함할 수도 있다.

[0029] 일 양태에서, 인가 서버는 로컬 인가 서버일 수 있다.

[0030] 일 양태에서, 선택적으로 활성화된 피처들의 제 1 리스트는 인가 서버에 의해 서명된 인가 인증서를 나타내는 데이터일 수 있다. 다른 양태에서, 선택적으로 활성화된 피처들의 제 1 리스트는, 디바이스가 선택적으로 활성화된 피처들을 활성화시키도록 인가된다는 것을 나타내는 인가 합의를 나타내는 데이터일 수 있다.

[0031] 일 양태에서, 서버 (예를 들어, HSS) 는 네트워크를 통해 통신하기 위한 네트워크 통신 회로 및 네트워크 통신 회로에 커플링된 프로세싱 회로를 포함할 수 있다. 프로세싱 회로는 전술된 방법(들)을 수행하도록 구성될 수도 있다.

도면의 간단한 설명

[0032] 도 1 은 본원에 설명된 양태들에 따른 하나 이상의 디바이스들의 세트 상의 하나 이상의 선택적으로 활성화된 피처들을 동적으로 인가 및 활성화시킬 수도 있는 예시적인 시스템의 블록도이다.

도 2 는 본원에 설명된 양태들에 따른 예시적인 동작 환경을 예시한다.

도 3 은 본원에 설명된 양태들에 따른 시스템의 아키텍처 레퍼런스 모델이다.

도 4 는 본원에 설명된 양태들에 따른 하나 이상의 디바이스들의 제조자 또는 OEM 과 제 1 엔티티 간의 예시적인 인가 합의에 포함될 수도 있는 파라미터들 및 데이터의 예시적인 리스트를 예시한다.

도 5 는 본원에 설명된 양태들에 따른 제조자 또는 OEM 과 다른 엔티티 간의 예시적인 인가 합의에 포함될 수도 있는 파라미터들 및 데이터의 예시적인 리스트를 예시한다.

도 6 은 본원에 설명된 양태들에 따른 네트워크 오퍼레이터와 다른 엔티티 간의 예시적인 인가 합의에 포함될 수도 있는 파라미터들 및 데이터의 예시적인 리스트를 예시한다.

도 7 은 본원에 설명된 양태들에 따른 인가 인증서들, 인가 파일들, 피처 활성화 키들, 및 소프트에어를 디바이스들로 전송하는 것에 관련된 액션들을 예시하는 흐름도이다.

도 8 은 본원에 설명된 양태들에 따른 피처 활성화 요청을 수반하는 방법을 예시하는 흐름도이다.

도 9 는 본원에 설명된 양태들에 따른 선택적으로 활성화된 피처들의 활성화의 일 예를 예시하는 흐름도이다.

도 10 은 본원에 설명된 양태들에 따른 인가 합의들의 동적 확인 및 시행을 지원하도록 구성된 인가 서버를 예시하는 블록도이다.

도 11 은 본원에 설명된 양태들에 따른 인가 합의들의 동적 확인 및 시행을 지원하도록 구성된 로컬 인가 서버를 예시하는 블록도이다.

도 12 는 본원에 설명된 양태들에 따른 인가 합의들의 동적 확인 및 시행에 관련된 호 흐름도이다.

도 13 은 본원에 설명된 양태들에 따른, 디바이스의 가입 프로파일에 기초하여, 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 검증하는 것과 연관되어 발생할 수도 있는 시스템 레벨 호 흐름을 예시하는 예시적인 호 흐름도이다.

도 14 는 본원에 설명된 양태들에 따라 디바이스에 저장된 인가 인증서에서 식별된 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 검증하는 것과 연관될 수도 있는 다른 시스템 레벨 호 흐름을 예시하는 예시적인 호 흐름도이다.

도 15 는 본원에 설명된 양태들에 따라, 인가 합의들의 동적 확인 및 시행을 지원하도록 구성된 예시적인 디바이스를 예시하는 블록도이고, 여기서 시행은 인가 합의들의 조항들에 따라 선택적으로 활성화된 피처들의 활성화/비활성화 및 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거의 동적 검증을 포함한다.

도 16 은 본원에 설명된 양태들에 따른 디바이스에서 동작하는 예시적인 방법의 플로우차트이다.

도 17 은 본원에 설명된 양태들에 따른 디바이스에서 동작하는 예시적인 방법의 플로우차트이다.

도 18 은 본원에 설명된 양태들에 따른 네트워크 노드에서 동작하는 예시적인 방법의 플로우차트이다.

도 19 는 본원에 설명된 양태들에 따른 네트워크 노드에서 동작하는 다른 예시적인 방법의 플로우차트이다.

도 20 은 본원에 설명된 양태들에 따른 인가 합의들의 확인 및 시행을 지원하도록 구성된 예시적인 홈 가입자 서버 (HSS) 를 예시하는 블록도이다.

도 21 은 본원에 설명된 양태들에 따라 디바이스의 하나 이상의 피처들의 세트의 사용을 위한 인가를 검증하는 것에 관련되는, HSS 에서 동작하는 예시적인 방법을 예시한다.

발명을 실시하기 위한 구체적인 내용

[0033] 다음의 상세한 설명에서, 본 개시물에서 설명된 특정 양태들 및 피처들이 예시의 방식에 의해 도시되는 첨부 도

면들에 대한 참조가 이루어진다. 본 개시물에 설명된 양태들 및 피처들은 당업자가 본 개시물의 양태들을 실시하는 것을 가능하게 하도록 충분히 상세하게 제공되도록 의도된다. 다른 양태들 및 피처들이 이용될 수도 있고, 본 개시물의 범위로부터 벗어나지 않고 개시되는 변화들이 이루어질 수도 있다. 다음의 상세한 설명은 제한 의미로 취해지지 않아야 하고 본원에 설명 및 예시된 양태들 및 피처들의 범위는 첨부된 청구항들에만 정의된다.

[0034] 용어 "예시적인"은 본원에서 "예, 경우, 또는 예시로서 역할을 하는" 것을 의미하도록 사용된다. 본원에서 "예시적인"으로서 설명된 임의의 양태 또는 구현은 반드시 다른 양태들 및 구현들에 비해 바람직하거나 또는 유리한 것으로서 해석될 필요는 없다.

[0035] 본원에 사용된 바와 같은 용어 "양태들" 은 모든 양태들이 논의된 양태, 또는 임의의 논의된 양태, 이점, 및/또는 동작의 모드를 포함하는 것을 요구하지 않는다.

[0036] 용어 "획득하다" 는 본원에서, 도출, 생성, 연산, 요청, 수신, 포착, 수락, 입수, 취함, 수집, 얻는 것, ~ 전달하거나 수신하는 것, 주어지는 것, 액세스를 얻는 것, ~ 를 소유하는 것 등을 의미하도록 사용된다. 본원에 사용된 바와 같은 용어 "획득하다" 는 국부적으로 획득하는 것, 및/또는 비-로컬 또는 원격 엔티티로부터 획득하는 것을 망라한다.

[0037] 용어 "프로비전" 은 전송, 포워딩, 제공, 공급, 목적지로 전달되게 하는 것을 의미하도록 사용된다. 용어 "전송하다" 는 본원에서, 프로비전, 포워드, 제공, 공급, 목적지로 전달되게 하는 것을 의미하도록 사용된다.

[0038] 본원에 사용된 바와 같이, 용어 "제조자" 는 제품을 구축하고 엔티티의 자신의 명칭 하에서 제품을 소비자들 또는 OEM들에게 판매하는 엔티티를 지칭할 수도 있다. OEM 은 다른 엔티티로부터 제품들을 구매하고 OEM 의 명칭 하에서 판매를 위해 제품들을 리브랜딩하는 엔티티일 수도 있다. OEM 은 부가적으로 또는 대안으로, 동일한 또는 상이한 제조자들로부터, 상이한 유형들의 제품들 (예를 들어, 서버들 및 데이터 저장 제품들) 을 구매하고, 제품들을 함께 번들링하며 결과의 번들링된 제품을 OEM 의 명칭 하에서 판매하는 엔티티일 수도 있다.

[0039] 용어 "디바이스" 는 임의의 통신 디바이스, 예컨대 칩 컴포넌트, 클라이언트 디바이스, 및/또는 네트워크 노드를 지칭하도록 본원에서 사용될 수도 있다. "칩 컴포넌트" 는, 예를 들어 프로세싱 회로, 모뎀, 칩 세트를 포함할 수도 있다. "클라이언트 디바이스" 는, 예를 들어 무선 디바이스, 이동 디바이스, 가입자 디바이스, 이동 전화기, 이동 통신 디바이스, 이동 컴퓨팅 디바이스, 디지털 태블릿, 스마트 폰, 사용자 장비 (UE), 사용자 디바이스, 사용자 단말기, 단말기, 스테이션 (STA) 을 포함할 수도 있다. "네트워크 노드" 는 서빙 네트워크 또는 홈 네트워크의 기능성 노드인 임의의 디바이스 또는 머신을 포함할 수도 있다. 네트워크 노드의 예들은, 기지국, 네트워크 액세스 노드 (예를 들어, 이볼브드 노드 B (eNodeB, eNB)), 이동성 관리 엔티티 (MME), 게이트웨이 디바이스 (예를 들어, 서빙 게이트웨이 (S-GW), 패킷 데이터 네트워크 게이트웨이 (P-GW)), 홈 가입자 서버 (HSS), 인가, 인증, 및 어카운팅 (AAA) 서버 (총괄하여, HSS/AAA 서버로서 지칭됨), 무선 라우터, 액세스 포인트 (AP), 및/또는 네트워크 기능을 수행하는 임의의 노드를 포함하지만, 이에 제한되지는 않는다. 클라이언트 디바이스 및/또는 네트워크 노드는 칩 컴포넌트를 포함할 수도 있다.

[0040] 용어 "네트워크 액세스 노드" 는 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스) 와 코어 네트워크 간의 무선 디바이스 접속성을 포함하는 임의의 디바이스를 지칭하도록 본원에서 사용될 수도 있다. 네트워크 액세스 노드의 예들은 eNB, 기지국, AP 를 포함할 수도 있다. 네트워크 액세스 노드는 네트워크 노드의 일 예인 것으로 이해될 수도 있다.

[0041] 셀룰러 통신 시스템의 코어 네트워크 외부의 네트워크들, 예컨대 패킷 데이터 네트워크 (PDN)(예를 들어, 인터넷) 및 IP 멀티미디어 서비스 (IMS) 네트워크는 PDN 을 참조하여 본원에서 예시될 수도 있지만, 어떤 것도 코어 네트워크 외부의 네트워크들을 PDN들 또는 IMS 네트워크들에 제한하도록 의도되지 않는다. 또한, 본원에 제시된 양태들 및 피처들은 예시적이다. 어떤 것도, 셀룰러 통신 시스템에서 사용하기 위해 본원에 제시된 임의의 양태 또는 피처를 제한하도록 의도되지 않는다.

[0042] 본원에 사용된 바와 같이, "선택적으로 활성화된 피처" 에 대한 참조를 포함하는, "피처" 에 대한 참조는 양태, 회로, 서비스, 또는 하드웨어, 소프트웨어, 펌웨어, 또는 하드웨어, 소프트웨어, 및 펌웨어 중 2 이상의 임의의 조합으로 구현될 수도 있는 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 의 기능을 참조할 수도 있다.

[0043] 용어 "선택적으로 활성화된" 은 그 활성화의 상태에서 변경되는 특징, 또는 능력을 설명할 수도 있다 (예를 들

어, 이것은 활성화 및 비-활성화될 수도 있다). 일부 양태들에서, 용어 "선택적으로 활성화된" 은 구체적으로 (예를 들어, 커맨드/요구에 따라) 인에이블/디스에이블, 턴-온/턴-오프, 및/또는 시작/종료될 특징, 또는 능력을 설명할 수도 있다. 따라서, 선택적으로 활성화된 피처들은, 예를 들어 구체적으로 (예를 들어, 커맨드/요구에 따라) 활성화 및/또는 비-활성화될 수 있는 피처들이다.

[0044] 본원에서 사용된 바와 같이, "네트워크 서비스" 에 대한 참조는 네트워크에 의해 제공되거나 또는 네트워크를 통해 이용 가능한 기능, 능력, 애플리케이션, 또는 그 일부에 대한 참조일 수도 있다. 디바이스 (예를 들어, 클라이언트 디바이스, 칩 컴포넌트, 네트워크 노드) 는 네트워크 서비스를 구현하도록 선택적으로 활성화된 피처들의 세트를 포함할 수도 있다.

[0045] 본원에서 사용된 바와 같이, 용어 "인가 정보" 는 "디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거" 또는 "네트워크 노드에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 네트워크 노드에 대한 권한의 증거" 를 의미하도록 이해된다. 인가 정보는 인가 합의, 인가 인증서, 또는 인가 합의 및 인가 인증서에 의해 표현될 수도 있고, 이들을 포함할 수도 있고, 또는 이들을 식별할 수도 있다. 대안으로 또는 부가적으로, 인가 정보는 인가 서버 (또는 로컬 인가 서버) 에 저장된 인가 합의로부터, 인가 서버 (또는 로컬 인가 서버) 에 의해 도출된 선택적으로 활성화된 피처들의 세트의 리스트를 포함하거나 이를 식별할 수도 있다.

[0046] 본원에서 사용된 바와 같이, "피처 활성화 키", "피처 활성화 키들", 또는 "피처 활성화 키(들)" 에 대한 참조는 소정의 피처를 가능하게 하는데 사용된 데이터 (예를 들어, 비트들의 스트링 또는 시퀀스) 에 대한 참조일 수도 있다. 피처 활성화 키는 암호화 함수 (cryptographic function) 에 관련되고/되거나 이로 도출될 수도 있다.

[0047] 용어 "최신 (up-to-date)" 은 현재 시간으로 유효하게 확장되는 것 (예를 들어, 라이선스) 을 가리키거나 설명하는데 사용될 수도 있다. 따라서, 예를 들어 최신 라이선스는 현재 시간까지 유효한 라이선스일 수도 있다.

[0048] 본원에서 사용된 바와 같이, 용어 "일치한다" 는 "~와 동일한" 것을 의미할 수도 있고, 또는 일부 본질적인 또는 기본적인 면에서 "~에 대응하는" 을 의미할 수도 있다.

[0049] 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 가 네트워크 서비스를 사용하고자 하는 경우, 디바이스는, 네트워크 서비스를 제공하는 네트워크 노드에 그 자체를 인증하는 것에 추가하여, 또한, 디바이스가 선택적으로 활성화된 피처들의 세트를 활성화시키도록 인가된다는 증거를 네트워크 노드로 전송할 필요가 있을 수도 있다. 선택적으로 활성화된 피처들의 세트, 또는 그 서브세트는 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요할 수도 있다. 결과적으로, 선택적으로 활성화된 피처들의 세트를 활성화시키기 위한 디바이스의 권한을 입증하기 위해, 디바이스는 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 전송할 수도 있다. 이 권한의 증거는 인가 서버로부터 디바이스에 의해 획득될 수도 있다. 디바이스는 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 네트워크 서비스를 제공하는 네트워크 노드로 전송할 수도 있다. 일 양태에서, 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거는 디바이스에 활성화되도록 인가되는 선택적으로 활성화된 피처들의 세트에서 피처들을 식별하는 리스트를 포함할 수도 있다. 일 양태에서, 선택적으로 활성화된 피처들의 세트는 인가 합의로부터 도출될 수도 있다. 인가 합의는 인가 서버에 저장될 수도 있다. 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거는 네트워크 노드에 의해 검증될 수도 있다. 일 양태에서, 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 검증하는 것은, 네트워크 노드가, 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 선택적으로 활성화된 피처들이, 예를 들어 디바이스가 네트워크 서비스를 사용하기 전에 디바이스 상에서 사용을 위해 인가된다는 것을 보장하는 것을 허용한다. 예를 들어, 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 검증하는 것은, 네트워크 노드가, 선택적으로 활성화된 피처들의 세트에서 나열된 선택적으로 활성화된 피처들이 디바이스가 네트워크 서비스를 사용하기 전에, 인가 합의에 반영될 수도 있는, 라이선스의 조항들 하에서 지불된다는 것을 보장하는 것을 허용한다.

[0050] 예를 들어, 네트워크 액세스 노드 (예를 들어, eNB) 가 서비스를 제공하도록 인가되는 경우, 네트워크 액세스 노드의 메시지 통지 능력들 (예를 들어, 보장된 전달, 보장된 대역폭, 및/또는 서비스 품질에 관련된 다른 양태들) 은 메시지를 수신하는 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스) 가 디바이스가 서비스를

사용하기를 원하는 지를 결정할 수 있도록 공중 경유로 브로드캐스트될 수도 있다. 메시지를 수신하는 디바이스는 서비스를 사용하기 위해 필요한 선택적으로 활성화된 피처들의 세트를 이미 활성화하도록 인가될 수도 있고, 이미 활성화했을 수도 있다. 그럼에도 불구하고, 디바이스는 서비스를 제공하기 위한 네트워크 액세스 노드의 인가를 검증하기를 원할 수도 있다. 디바이스는, 네트워크 액세스 노드가 예를 들어 이용 불가능한 네트워크 서비스에 대한 추가 요금을 방지하기 위해 네트워크 서비스를 제공하도록 인가된다는 것을 검증할 기회를 가져야 한다. 일 양태에서, 서비스를 제공하기 위한 네트워크 액세스 노드의 인가를 검증하는 것은, 디바이스가 서비스를 사용하기 전에 네트워크 액세스 노드가 서비스를 제공하도록 인가된다는 것을 보장하는 것을 허용한다.

[0051] 예로서, 시스템 정보 브로드캐스트 (SIB) 및 (하나 이상의 SIB들을 운반하는데 사용된) 시스템 정보 (SI) 메시지들은 네트워크 노드에 의해 서명된 서명 또는 임의의 메시지 인증 코드를 반송하지 않는다. 디바이스가 셀에 캠프 온되고 네트워크 액세스 노드로부터 SIB 를 획득하면, 디바이스는 SIB 에서 광고된 피처들이 네트워크 노드에 의해 유효하게 제공되는지 여부를 확인할 수 없다. 네트워크에 대한 액세스를 얻기 위해, 디바이스는, 네트워크가 SIB 에서 광고되는 피처들을 제공하도록 인가된다는 것을, 확인하기 위한 어떤 능력 없이, 기본적으로 신뢰한다.

[0052] 본원에 개시된 양태들은, 제 1 디바이스 또는 노드가 제 1 인가 정보를 제 2 디바이스 또는 노드로 전송하는 것을 동적으로 허용하고 제 2 디바이스 또는 노드에 의해 제공된 서비스를 사용하도록 시작하기 전에 제 2 디바이스 또는 노드로부터 제 2 인가 정보를 획득하도록 인가 정보를 검증하는 방법들 및 장치를 제공할 수 있다. 본원에 개시된 양태들은 디바이스가, 네트워크 노드가 유효한 네트워크 노드인지 여부 및 네트워크 노드가 소정의 피처들을 활성화시키도록 인가되는지 여부를 확인하는 것을 허용할 수 있다. 일 양태에서, 검증, 확인, 또는 검증 및 확인은 암호화 동작을 포함할 수도 있다.

[0053] **개관**

[0054] 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 는 디바이스의 하나 이상의 선택적으로 활성화된 피처들을 활성화, 비활성화, 및/또는 보고하는 인가 회로/기능부/모듈을 포함할 수도 있다. 인가 회로/기능부/모듈은 부가적으로, 디바이스가 소정의 피처를 활성화시키고/시키거나 사용/제공할 권한을 갖는다는 것을 확인할 수도 있다. 일부 양태들에서, 확인은 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거 (예를 들어, 디바이스의 인가 정보) 의 검증에 의한 것일 수도 있다.

[0055] 일 양태에서, 예로써 클라이언트 디바이스를 사용하면, 클라이언트 디바이스는 네트워크 서비스가 네트워크 노드 (예를 들어, 네트워크 액세스 노드, eNB, MME) 로부터 이용 가능하다는 것을 결정할 수도 있다. 클라이언트 디바이스는 (클라이언트 디바이스에 이용 가능한 복수의 피처들 중에서부터) 어느 피처(들)을 클라이언트 디바이스가 서비스를 사용하기 위해 필요로 하는지를 결정할 수도 있다. 클라이언트 디바이스는 클라이언트 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 클라이언트 디바이스에 대한 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 및 네트워크 서비스를 사용하기 위해 필요한 피처들을 활성화시키는데 필요한 피처 활성화 키(들)을 획득하도록 인가 서버와의 피처 활성화 프로세스에 참여할 수도 있다. 클라이언트 디바이스는 네트워크 서비스를 사용하기 위해 요청하도록 네트워크 노드로 요청을 전송할 수도 있다. 클라이언트 디바이스는 클라이언트 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 클라이언트 디바이스에 대한 권한의 증거 (예를 들어, 디바이스의 인가 정보) 를 네트워크 노드로 전송할 수도 있다. 응답하여, 클라이언트 디바이스는 네트워크 서비스를 사용하기 위한 요청을 허가하는 응답을 네트워크 노드로부터 획득할 수도 있다. 응답은 클라이언트 디바이스에 의해 네트워크 노드로 전송된 인가 정보를 검증하는 네트워크 노드에 입각할 수도 있다. 또한, 네트워크 노드가 MME 인 경우에서, 네트워크 노드는, 인가 정보에 포함될 수 있는, 클라이언트 디바이스에서 활성화되도록 인가된 피처들의 리스트를 사용하여, 클라이언트 디바이스에 대한 클라이언트 디바이스 콘텍스트 (예를 들어, UE 콘텍스트) 를 구성할 수도 있다.

[0056] 클라이언트 디바이스는, 네트워크 서비스를 사용하기 전에, 서비스를 제공할 네트워크 노드의 권한을 검증하기를 원할 수도 있다. 클라이언트 디바이스는 따라서, 네트워크 노드로부터, 네트워크 노드에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 네트워크 노드에 대한 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 를 획득할 수도 있다. 클라이언트 디바이스는 네트워크 서비스를 사용하기 전에 네트워크 노드에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 네트워크 노드에 대한 권한의 증거를 확인할 수도 있다.

[0057] **예시적인 시스템 및 시스템 설명**

[0058] 도 1 은 본원에 설명된 양태들에 따라 하나 이상의 디바이스들 (예를 들어, 칩 컴포넌트들, 클라이언트 디바이스들, 네트워크 노드들) 의 세트 상에서 하나 이상의 선택적으로 활성화된 피처들을 동적으로 인가 및 활성화시킬 수도 있는 예시적인 시스템 (100) 의 블록도이다. 디바이스 A (102), 디바이스 B (104), 및 디바이스 C (106) 를 갖는 하나 이상의 디바이스들의 세트가 도 1 에 예시된다. 디바이스 A (102), 디바이스 B (104), 및 디바이스 C (106) 는 각각 인가 회로/기능부/모듈 (108, 112, 116) 을 포함할 수도 있다. 인가 회로/기능부/모듈 (108, 112, 116) 은 시스템에서 유용할 수도 있고, 여기서 예를 들어 서비스들 (예를 들어, 네트워크 서비스들) 은 실시간으로, 예를 들어 라이선스들의 조항들에 따라 개별적으로 활성화/비활성화 (예를 들어, 인에이블/디스에이블) 될 수 있는 디바이스 피처들 (예를 들어, 선택적으로 활성화된 피처들) 을 전체적으로 또는 부분적으로 사용하여 구현될 수 있다. 인가 회로/기능부/모듈 (108, 112, 116) 은 선택적으로 활성화된 피처를 포함하는 디바이스 A (102), 디바이스 B (104), 또는 디바이스 C (106) 와 같은 임의의 디바이스에 포함될 수도 있고, 여기서 선택적으로 활성화된 피처를 활성화시키기 위한 인가는, 예를 들어 인가 합의 (120) 에 기초할 수 있다. 인가 합의 (120) 는 따라서, 선택적으로 활성화된 피처를 활성화시킬 권리의 증거에 대한 소스일 수도 있다.

[0059] 디바이스 A (102) 는 인가 회로/기능부/모듈 A (108) 및 선택적으로 활성화된 피처들의 제 1 세트 (110) 를 포함한다. 디바이스 B (104) 는 인가 회로/기능부/모듈 B (112) 및 선택적으로 활성화된 피처들의 제 2 세트 (114) 를 포함한다. 디바이스 C (106) 는 인가 회로/기능부/모듈 C (116) 및 선택적으로 활성화된 피처들의 제 3 세트 (118) 를 포함한다. 참조의 용이함을 위해, 그리고 어떤 제한 의도 없이, 인가 회로/기능부/모듈 A (108), 인가 회로/기능부/모듈 B (112), 및 인가 회로/기능부/모듈 C (116) 는 본원에서 "인가 기능부 (108, 112, 116)" 로서 개별적으로 및/또는 총괄하여 지칭될 수도 있다. 부가적으로, 참조의 용이함을 위해, 그리고 어떤 제한 의도 없이, 디바이스 A (102), 디바이스 B (104), 및 디바이스 C (106) 는 본원에서 "디바이스 (102, 104, 106)" 로서 개별적으로 및/또는 총괄하여 지칭될 수도 있다.

[0060] 소정 디바이스 (예컨대, 디바이스 A (102), 디바이스 B (104), 및/또는 디바이스 C (106)) 에서 선택적으로 활성화된 피처들의 세트 (예컨대, 선택적으로 활성화된 피처들의 제 1 세트 (110), 선택적으로 활성화된 피처들의 제 2 세트 (114), 및/또는 선택적으로 활성화된 피처들의 제 3 세트 (118)) 에서 하나 이상의 선택적으로 활성화된 피처들을 활성화시키기 위한 인가는 소정 디바이스에서 하나 이상의 피처들의 활성화에 대한 선행 조건일 수도 있다.

[0061] 본원에 설명된 일부 양태들에서, 디바이스 (102, 104, 106) 의 인가 기능부 (108, 112, 116) 는, 디바이스 (102, 104, 106) 가 선택적으로 활성화된 피처를 활성화시키기 전에, 디바이스 (102, 104, 106) 가 인가 서버 (126) 에 의해 선택적으로 활성화된 피처를 활성화시키고, 증거 (예를 들어, 인가 정보) 를 획득 및 확인하도록 인가되었다는 증거를 획득 및 확인할 수도 있다. 일부 구현들에서, 제 1 디바이스에서 인가 기능부 (108, 112, 116) 는 또한, 그 증거를 제 2 디바이스로 전송할 수도 있고, 여기서 제 2 디바이스는 서비스 (예를 들어, 네트워크 서비스) 를 제 1 디바이스에 제공할 수도 있다.

[0062] 네트워크 서비스들의 예들은, 예를 들어 듀얼 접속성 서비스, 다중 가입 서비스, 디바이스-대-디바이스 (D2D) 모드 서비스, 멀티미디어 브로드캐스트/멀티캐스트 서비스 (MBMS), 및/또는 비허가 동작 서비스를 포함할 수도 있다. 듀얼 접속성 서비스는, 예를 들어 무선 액세스 기술 (RAT) (예를 들어, 4G) 내에 그리고 RAT 들에 걸쳐 (예를 들어, 4G 및 5G 및/또는 무선 로컬 영역 네트워크 (WLAN) 에 걸쳐) 접속성을 제공할 수도 있다.

[0063] 다중 가입 서비스는, 예를 들어 다중 가입들을 동시에 (예를 들어, 오퍼레이터 서비스 가입 및 스트리밍 비디오 가입 및/또는 온라인 소매 판매 제공자 가입을 동시에) 서빙하도록 단일의 무선 링크를 사용하여 디바이스에 서비스들을 제공할 수도 있다.

[0064] D2D 모드 서비스는, 예를 들어 서비스들, 친구들, 및 제공자들의 근위 발견을 제공하는 서비스를 제공할 수도 있다. D2D 서비스는, 예를 들어 전통적인 액세스 서비스에 추가하여 제공될 수도 있다.

[0065] MBMS 서비스는 디바이스가 유니캐스트 서비스들에 액세스하는 것에 추가하여 멀티캐스트 서비스들을 수신하는 것을 용이하게 하는 서비스일 수도 있다.

[0066] 비허가 동작 서비스는, 예를 들어 디바이스가 LTE 또는 5G 또는 하나 이상의 다른 RAT들을 사용하여 비허가 대역에서 동작하거나 비허가 보조 액세스를 사용하는 것을 허용하는 서비스일 수도 있다. 위에서 열거된 예시적인 서비스들, 뿐만 아니라 다른 서비스들을 사용하기 위해 활성화될 필요가 있을 수도 있는 피처들 (예를 들

어, 선택적으로 활성화된 피처들) 의 완전한 리스트는 본 출원의 범위 이상이다. 그럼에도 불구하고, 선택적으로 활성화될 수도 있는 피처들의 일부 예들은 캐리어 집성; (예를 들어, 듀얼 접속성, 및/또는 비허가 동작 서비스들의 경우에서) 소정의 물리적 채널들; 선택적으로 활성화된 하드웨어; 및/또는 소정의 선택적으로 활성화된 피처가 활성화되지 못하게 하도록 실행되지 않은 채로 남아 있었던 디바이스 상에 저장된 프로세싱 회로 판독가능 명령들의 선택적으로 실행된 일부들을 포함할 수도 있다.

[0067] 제 2 디바이스에 증거 (예를 들어, 인가 정보) 를 제공하는 것은, 제 2 디바이스가 서비스를 제공하기 전의 선행 조건일 수도 있다. 따라서, 예를 들어 선택적으로 활성화된 피처들의 제 1 세트 (110) 가 인가되고 디바이스 A (102) 에서 활성화된 후에도, 다른 디바이스 (예를 들어, 디바이스 C (106))(예를 들어, 네트워크 액세스 노드) 는 디바이스 A (102) 의 권한의 증거를 전송하도록 디바이스 A (102) 에 요청하여, 디바이스 A (102) 에서 선택적으로 활성화된 피처들의 제 1 세트 (110) 를 사용할 수도 있고, 여기서 권한의 증거는 인가 서버 (126) 에 의해 서명될 수 있다. 더 또한, 일부 구현들에서, 디바이스 A (102) 가 디바이스 C (106) 에 의해 제공된 서비스 (예를 들어, 네트워크 서비스) 를 (여기서, 선택적으로 활성화된 피처들의 제 3 세트는 디바이스 A (102) 에 서비스를 제공하기 위해 디바이스 C (106) 에 의해 필요한 제 3 선택적으로 활성화된 피처들을 포함) 사용 (예를 들어, 활성화, 활용) 하기 전에, 그리고 선택적으로 활성화된 피처들의 제 3 세트 (118) 가 디바이스 C (106)(예를 들어, 네트워크 액세스 노드) 에서 인가 및 활성화된 후에도, 디바이스 A (102)(예를 들어, 클라이언트 디바이스) 는 디바이스 C (106) 의 권한의 증거를 전송하도록 디바이스 C (106) 에 요청하여 디바이스 C (106) 에서 선택적으로 활성화된 피처들의 제 3 세트 (118) 를 사용할 수도 있고, 여기서 권한의 증거는 인가 서버 (126)(또는 다른 인가 서버) 에 의해 서명될 수 있다.

[0068] 디바이스 A (102) 는 디바이스 C (106) 에서 제공된 서비스를 사용하기 전에, 증거에 대한 요청을 디바이스 C (106) 로 전송할 수도 있다. 디바이스 A (102) 는 디바이스 C (106) 에서 제공된 서비스를 사용하기 전에, 디바이스 C (106) 로부터 획득된 증거를 획득 및 확인할 수도 있다.

[0069] 인가 정보 (예를 들어, 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거) 는 인가 합의 (120) 에 기초할 수도 있다. 인가 정보는, 예를 들어 인가 합의 (120) 및/또는 인가 인증서 (122) 의 형태로 제공될 수도 있다. 인가 합의 (120) 는 인가 서버 (126) 에 저장될 수도 있다. 인가 서버 (126) 는 인가 합의 (120) 에 기초하여 인가 인증서 (122) 및 (피처 활성화 키들을 포함할 수도 있는) 인가 파일 (124) 을 도출할 수도 있다. 인가 인증서 (122) 는, 예를 들어 디바이스 (102, 104, 106) 공용 키, 디바이스 (102, 104, 106) 에 인가된 선택적으로 활성화된 피처들 (예를 들어, 선택적으로 활성화된 피처들의 세트), 및 선택적으로 활성화된 피처들이 인가되는 디바이스 (102, 104, 106) 의 식별자 (예를 들어, 디바이스 공용 키의 해시 또는 일부 다른 디바이스 고유 식별자) 를 포함할 수도 있다. 인가 인증서 (122) 는 또한, 예를 들어 인가 인증서 (122) 의 만료 시간을 포함할 수도 있고, 부가적으로 또는 대안으로 디바이스 (102, 104, 106) 에 인가된 선택적으로 활성화된 피처들에 관련된 파라미터들을 포함할 수도 있다. 인가 인증서는 인가 서버 (126) 의 사설 키를 사용하여 인가 서버 (126) 에 의해 서명될 수도 있다.

[0070] 따라서, 인가 인증서 (122) 는 인가 서버 (126) 의 서명을 반송하고; 이 서명은 인가 서버 (126) 의 공용 키를 사용하여 확인될 수 있다. 서명을 도출하기 위해, 예를 들어 인가 서버 (126) 는 디바이스 (102, 104, 106) 공용 키, 디바이스 (102, 104, 106) 에 인가된 선택적으로 활성화된 피처들, 및 디바이스 (102, 104, 106) 의 식별자를 해시 함수에 적용할 수도 있고; 인가 서버 (126) 는 그 후, 도출된 해시 값 및 인가 서버 (126) 의 사설 키를 서명 함수에 입력할 수도 있다. 확인 함수는 서명 함수의 반대일 수도 있다; 엔티티 (예를 들어, 네트워크 노드) 는 인가 서버 (126) 의 공용 키 및 서명을 확인 함수에 입력함으로써 서명을 확인할 수도 있다.

이 방식에서, 인가 인증서 (122) 가 인가 서버 (126) 에 의해 서명되는 경우, 인가 인증서 (122) 는 확인되고 디바이스 (102, 104, 106) 에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스 (102, 104, 106) 에 대한 권한의 증거로서 사용될 수도 있다. 따라서, 인가 인증서 (122) 는 인가 정보로서 사용될 수도 있다.

[0071] 본질적으로, 디바이스들 (102, 104, 106) 에는 피처 활성화 동안 인가 서버의 인증서가 프로비저닝된다. 인가 인증서 (122) 는 또한, 인가 서버 (126) 가 인가 파일 (124) 에서 식별된 디바이스 (102, 104, 106) 에 인가 파일 (124) 을 발행했다는 것을 입증하는 것을 담당할 수도 있다.

[0072] 디바이스 (102, 104, 106) 가 인가 인증서 (122) 를 엔티티 (예를 들어, 네트워크 노드) 로 전송하는 경우, 디바이스 (102, 104, 106) 는 디바이스 (102, 104, 106) 의 사설 키로 인가 인증서 (122) 에 서명할 수도 있다는 것이 주목된다. 이것은, 디바이스 (102, 104, 106) 가 인가 인증서 (122) 에 포함되는 공용 키의 오너라는

것을 입증하기 위한 디바이스 (102, 104, 106) 의 능력을 용이하게 한다. 인가 인증서 (122) 에 포함된 공용 키를 사용하여, 엔티티 (예를 들어, 네트워크 노드) 는, 인가 인증서 (122) 를 전송했던 디바이스가 인가 인증서 (122) 에서 인가 서버 (126) 에 의해 식별된 동일한 디바이스라는 것을 확인할 수 있다.

[0073] 인가 정보는, 임의의 시간에 (예를 들어, 초기 어태치 동안, 서비스 요청, 핸드오버, 요구 시) 디바이스 (102, 104, 106) 에 의해 요청될 수도 있다.

[0074] 인가 기능부 (108, 112, 116) 는, 인가 기능부 (108, 112, 116) 가 인가 합의 (120), 또는 인가 합의 (120) 로부터 도출된 인가 인증서 (122) 를 획득 및 확인하면, 소정의 선택적으로 활성화된 피처를 활성화시킬 수도 있다 (또는 소정의 선택적으로 활성화된 피처를 활성화시키도록 인가 기능부 (108, 112, 116) 를 호스트하는 디바이스 (102, 104, 106) 를 인가/커맨드/명령할 수도 있다). 인가 합의 (120), 뿐만 아니라 인가 인증서 (122) 는 소정의 선택적으로 활성화된 피처를 활성화시키도록 디바이스 (102, 104, 106) 의 권리를 레코드할 수 있다.

[0075] 인가 기능부 (108, 112, 116) 는 피처 활성화 요청 (예를 들어, 하나 이상의 선택적으로 활성화된 피처들을 활성화시키기 위한 요청, 하나 이상의 선택적으로 활성화된 피처들을 활성화시키기 위한 인가에 대한 요청) 을 로컬 인가 서버 (128) 로 전송할 수도 있다. 피처 활성화 요청에 대한 응답은 인가 정보 (예를 들어, 디바이스에서, 피처 활성화 요청에서 식별된 하나 이상의 선택적으로 활성화된 피처들을 포함하는, 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스 (102, 104, 106) 에 대한 권한의 증거) 를 포함할 수도 있다. 응답은 또한, 인가 파일 (124) 을 포함할 수도 있다. 인가 파일 (124) 은 하나 이상의 피처 활성화 키(들)을 포함할 수도 있다. 인가 서버 (126) 는 인가 정보, 인가 파일, 및/또는 하나 이상의 피처 활성화 키들을 암호화할 수도 있다.

[0076] 인가 서버 (126) 는 인가 서버 (126) 에 속하는 공용/사설 키 쌍의 사설 키로 인가 정보를 서명할 수도 있다. 인가 정보가 인가 인증서를 포함하는 경우에서, 인가 서버 (126) 는, 예를 들어 인가 서버 (126) 에 속하는 공용/사설 키 쌍의 사설 키로 인가 인증서에 서명할 수도 있다. 디바이스 (102, 104, 106) 는 인가 서버 (126) 의 공용 키를 사용하여, 인가 인증서 (122) 가 확실하다는 것을 확인할 수도 있다. 당업자는, 인가 인증서 (122) 와 같은 아이템들을 서명하기 위한 대안의 방식들이 본원에 제시된 양태들의 범위 내에 있다는 것을 인지할 것이다.

[0077] 인가 서버 (126) 는 디바이스 (102, 104, 106) 에 속하는 공용/사설 키 쌍의 공용 키를 사용하여 하나 이상의 피처 활성화 키들을 포함할 수도 있는 인가 파일 (124) 을 암호화할 수도 있다. 일부 양태들에서, 단지 인가 기능부 (108, 112, 116) 는 디바이스 (102, 104, 106) 에 속하는 공용/사설 키 쌍의 사설 키에 대한 액세스를 갖고; 따라서 단지, 인가 기능부 (108, 112, 116) 는 하나 이상의 피처 활성화 키들을 포함할 수도 있는 인가 파일 (124) 을 해독할 수 있다. 당업자는, 피처 활성화 키들을 포함할 수도 있는 인가 파일 (124) 과 같은 아이템들에 대한 암호화의 다른 유형들이 본원에 제시된 양태들의 범위 내에 있다는 것을 인지할 것이다.

[0078] 로컬 인가 서버 (128) 는 피처 활성화 요청을 인가 서버 (126) 로 전송할 수도 있다. 일부 양태들에서, 피처 활성화 요청은, 먼저 로컬 인가 서버 (128) 로 전송되지 않고 인가 기능부 (108, 112, 116) 로부터 인가 서버 (126) 로 직접 전송될 수 있다.

[0079] 인가 서버 (126) 는, 디바이스 A (102), 디바이스 B (104), 또는 디바이스 C (106) 와 같은 디바이스와 연관된 인가 합의 (120) 를 고려/평가/프로세싱한 후에 피처 활성화 요청에 대한 응답을 전송할 수 있다. 피처 활성화 요청에 대한 응답은 피처 활성화 요청에서 식별된 하나 이상의 선택적으로 활성화된 피처들을 활성화시키도록 디바이스 (102, 104, 106) 의 권리를 확인하는데 사용될 수도 있는 인가 정보를 포함할 수도 있다.

[0080] 응답은 또한, 인가 파일 (124) 을 포함할 수도 있다. 인가 파일 (124) 은 하나 이상의 피처 활성화 키(들), 인가 파라미터들, 또는 하나 이상의 피처 활성화 키(들) 및 인가 파라미터들을 포함할 수도 있다. 인가 파라미터들은, 예를 들어 인가의 만료 날짜/철회 날짜를 포함할 수도 있다. 로컬 인가 서버 (128), 또는 일부 양태들에서 인가 서버 (126) 는 인가 인증서 (122) 및 피처 활성화 키(들) 및 인가 파라미터들을 포함하는 인가 파일 (124) 을 인가 기능부 (108, 112, 116) 로 포워딩할 수도 있다.

[0081] 위에서 나타낸 바와 같이, 디바이스 (102, 104, 106) 의 선택적으로 활성화된 피처를 활성화시키기 위해 선택적으로 활성화된 피처가 인가될 필요가 있을 수도 있다. 하나의 비-제한 예에 따르면, 엔티티 (예를 들어, 사용자, 서비스 제공자, OEM, 제조자) 는 선택적으로 활성화된 피처를 활성화시키기 위한 인가 요금 (예를 들어, 라이선싱 요금) 을 인가 합의 (120) 에서 정의된 조항들에 기초하여 라이선싱 서비스에 지불할 수도 있다.

지불이 확인되기 전에 또는 후에, 인가 합의 (120) 는 인가 서버 (126) 및/또는 로컬 인가 서버 (128) 로 업로드될 수도 있다. 인가 서버 (126) 는 라이선싱 서비스에 의해 호스트될 수도 있다. 인가 서버 (126)(예를 들어, 라이선싱 서버) 는 인가 합의 및/또는 그와 연관된 선택적으로 활성화된 피처들의 검증, 활성화, 및/또는 시행을 위해 사용될 수도 있다.

[0082] 일 양태에서, 디바이스 (102, 104) 는, 네트워크 서비스가 이용 가능하다는 것을 결정할 수도 있다. 디바이스 (102, 104) 는 디바이스에 이용 가능한 (하지만 디바이스에서 반드시 활성화되지는 않는) 그리고 네트워크 서비스를 사용하기 위해 필요한 선택적으로 활성화된 피처들을 식별할 수도 있다. 네트워크 서비스를 사용하는데 필요한 선택적으로 활성화된 피처들의 식별은, 예를 들어 디바이스 (102, 104) 에 저장된 리스팅/테이블, 로컬 인가 서버 (128) 로부터 획득된 리스팅/테이블, 인가 서버 (126) 로부터 획득된 리스팅/테이블과 같은 임의의 적합한 소스로부터 획득될 수도 있고, 또는 원격 네트워크 노드 또는 다른 소스 (예를 들어, 패킷 데이터 네트워크 상의 노드) 로부터 획득될 수도 있다. 디바이스 (102, 104) 는, 그것 (즉, 디바이스 (102, 104)) 이 네트워크 서비스를 사용하기 위해 필요한 선택적으로 활성화된 피처들을 활성화시키도록 인가되는지를 결정할 수도 있다.

[0083] 디바이스 (102, 104) 가 네트워크 서비스를 사용하기 위해 필요한 선택적으로 활성화된 피처들의 전부를 활성화시키도록 인가되지 않으면, 디바이스 (102, 104), 또는 디바이스 (102, 104) 의 인가 기능부 (108, 112) 는 선택적으로 활성화된 피처 (또는 복수의 선택적으로 활성화된 피처들) 를 활성화시키기 위한 인가를 요청할 수도 있다. 디바이스 (102, 104), 또는 디바이스 (102, 104) 의 인가 기능부 (108, 112) 는, 요청된 선택적으로 활성화된 피처를 활성화시키도록 디바이스 (102, 104) 가 인가된다는 증거를 요청할 수도 있다. 요청된 선택적으로 활성화된 피처의 활성화는, 디바이스 (102, 104) 로 하여금, 예를 들어 네트워크 액세스 노드 (예를 들어, eNB) 에 의해 제공된 서비스를 사용하거나 애플리케이션 서버 상에 제공된 서비스를 획득하게 할 수도 있다.

[0084] **예시적인 동작 환경**

[0085] 도 2 는 본원에 설명된 양태들에 따른 예시적인 동작 환경 (200) 을 예시한다. 참조의 용이함을 위해, 그리고 어떤 제한 의도 없이, 각각의 인가 회로/기능부/모듈은 본원에서 "인가 기능부" 로서 지칭될 것이다. 예시적인 동작 환경 (200) 에서, 제 1 디바이스 (202)(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 는 제 1 인가 기능부 (203) 를 포함한다. 제 2 디바이스 (204)(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 는 제 2 인가 기능부 (205) 를 포함한다. 제 1 디바이스 (202) 및 제 2 디바이스 (204) 는 네트워크 액세스 노드 (예를 들어, eNodeB) 로서 도시된, 제 3 디바이스 (206) 와 무선으로 통신할 수도 있다. 제 3 디바이스 (206)(예를 들어, 네트워크 액세스 노드) 는 제 3 인가 기능부 (207) 를 포함할 수도 있다.

[0086] 제 1 디바이스 (202) 는 제 1 네트워크 서비스를 사용하기 위해 필요한 하나 이상의 선택적으로 활성화된 피처들을 포함할 수도 있다. 제 2 디바이스 (204) 는 제 2 네트워크 서비스를 사용하기 위해 필요한 하나 이상의 선택적으로 활성화된 피처들을 포함할 수도 있다. 제 3 디바이스 (206) 는 제 1 네트워크 서비스를 사용하고/제 1 디바이스 (202) 에 제공하고, 및/또는 제 2 네트워크 서비스를 사용하고/제 2 디바이스 (204) 에 제공하는데 필요한 하나 이상의 선택적으로 활성화된 피처들을 포함할 수도 있다.

[0087] 제 3 디바이스 (206)(예를 들어, 네트워크 액세스 노드) 는 무선 액세스 네트워크 (RAN)(210) (예를 들어, 강화된 유니버셜 지상 무선 액세스 네트워크; E-UTRAN) 의 부분일 수도 있다. 셀룰러 통신 시스템 (예를 들어, 4G, LTE, LTE-A, 5G) 의 비-제한 예에서, RAN (210) 은 코어 네트워크 (212)(예를 들어, 이볼브드 패킷 코어 (EPC)) 로 제어 시그널링 및 데이터 트래픽을 통신할 수도 있다. 네트워크 오퍼레이터 (예를 들어, 모바일 네트워크 오퍼레이터 (MNO)) 는 코어 네트워크 (212) 를 동작할 수도 있다. 제어 시그널링은 S1-MME 레퍼런스 포인트를 통해 통신될 수도 있다. 데이터 트패픽은 S1-U 레퍼런스 포인트를 통해 통신될 수도 있다.

[0088] 코어 네트워크 (212) 는 이동성 관리 엔티티 (MME)(214), 홈 가입자 서버/인가, 인증, 및 어카운팅 서버 (HSS/AAA)(216), 서빙 게이트웨이 디바이스 (S-GW)(218), 및 패킷 데이터 네트워크 게이트웨이 디바이스 (P-GW)(220) 를 포함할 수도 있다. 위에서 식별된 컴포넌트들에 추가하여, 코어 네트워크 (212) 는 또한, 로컬 인가 서버 (222) 를 포함할 수도 있다. 로컬 인가 서버 (222) 는 RAN (210) 뿐만 아니라 다른 네트워크 액세스 노드들 (미도시) 에서 제 3 디바이스 (206)(예를 들어, 네트워크 액세스 노드) 와 통신할 수도 있다. 로컬 인가 서버 (222) 는 제 3 디바이스 (206)(예를 들어, 네트워크 액세스 노드) 를 통해 제 1 디바이스 (202) 및 제 2 디바이스 (204) 와 통신할 수도 있다. 코어 네트워크 (212) 내에서, 로컬 인가 서버 (222) 는 MME

(214), 및/또는 HSS/AAA (216) 와 통신할 수도 있다. 로컬 인가 서버 (222) 는 로컬 인가 서버 (222) 와 연관된 코어 네트워크 (212) 에 커플링된 제 1 디바이스 (202), 제 2 디바이스 (204), 및 제 3 디바이스 (206) (예를 들어, 네트워크 액세스 노드) 에 대한 인가 서버 (234) 의 프록시로서 역할을 할 수도 있다.

[0089] P-GW (220) 는 패킷 데이터 네트워크 (PDN)(232) (예를 들어, 인터넷) 상의 애플리케이션 서버들 (228, 230) 과 통신할 수도 있다. 애플리케이션 서버들 (228, 230) 은 예를 들어, 소매 판매 제공자, 인터넷 검색 엔진 제공자, 엔터테인먼트 제공자, 및 소셜 미디어 서비스 제공자와 같은 서비스 제공자들과 연관될 수도 있다. 애플리케이션 서버들 (228, 230) 은 서비스 제공자들과 연관된 애플리케이션 서비스들 및/또는 애플리케이션들을 호스트할 수도 있다.

[0090] 코어 네트워크 (212) 내의 로컬 인가 서버 (222) 는 패킷 데이터 네트워크 (232) 에서 인가 서버 (234) 와 통신할 수도 있다. 인가 서버 (234) 는 어디든 위치될 수 있다는 것으로 이해될 것이다. 다시 말해, 패킷 데이터 네트워크 (232) 상에 애플리케이션 서버들 (228, 230) 과 인가 서버 (234) 를 위치시키는 것은 선택적이다. 예를 들어, 코어 네트워크 (212) 는 로컬 인가 서버 (222) 에 추가하여 인가 서버 (234) 를 포함할 수도 있다.

[0091] 인가 서버 (234) 는 제 1 디바이스 (202), 제 2 디바이스 (204), 제 3 디바이스 (206) 에 의해, 뿐만 아니라 임의의 수의 엔티티들, 예컨대 무선 액세스 네트워크 제공자들, 모바일 네트워크 오퍼레이터들, 또는 액세스 포인트 제공자들에 의해 액세스될 수도 있다. 각각의 엔티티는 또한, 그 자신의 로컬 인가 서버를 유지할 수도 있다. 인가 서버들 및 로컬 인가 서버들의 양태들은 이하에서 제공될 것이다.

[0092] **아키텍처 레퍼런스 모델**

[0093] 도 3 은 본원에 설명된 양태들에 따른 시스템 (300) 의 아키텍처 레퍼런스 모델이다. 도 3 은 디바이스 (302)(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드), 로컬 인가 서버 (306), 및 인가 서버 (308) 를 예시한다. 디바이스 (302) 는 적어도 하나의 선택적으로 활성화된 피처 (320) 를 포함할 수도 있다. 선택적으로 활성화된 피처 (320) 를 활성화시키기 위한 디바이스 (302) 의 권리는 인가 합의 (330)(예를 들어, 계약, 합의, 라이선스) 에 기초할 수도 있다. 일 양태에서, 선택적으로 활성화된 피처 (320) 를 활성화시키기 위한 디바이스 (302) 의 권리는 인가 합의 (330)(또는 인가 합의 (330) 로부터 도출된 인가 정보) 의 검증에 기초할 수도 있다. 일 양태에서, 선택적으로 활성화된 피처 (320) 를 활성화시키기 위한 디바이스 (302) 의 권리는 그 선택적으로 활성화된 피처 (320) 에 관련된 지불에 기초할 수도 있다. 일 양태에서, 선택적으로 활성화된 피처 (320) 에 관련된 지불의 스테이터스는 인가 합의 (330)(또는 인가 합의 (330) 로부터 도출된 인가 정보) 에 반영될 수도 있다. 일 구현에서, 인가 서버 (308) 는, 예를 들어 (예를 들어, 선택적으로 활성화된 피처 (320) 를 사용할 권리의) 검증 동안, (예를 들어, 선택적으로 활성화된 피처 (320) 의) 활성화, 및 (예를 들어, 선택적으로 활성화된 피처 (320) 에 관련된 인가 합의 (330) 의 조항들의) 시행을 포함하는, 선택적으로 활성화된 피처 (320) 와 연관되는 다양한 경우들에서 유틸리티를 발견할 수도 있다.

[0094] 디바이스 (302) 는 로컬 인가 서버 (306) 에 커플링될 수도 있다. 로컬 인가 서버 (306) 는 인가 서버 (308) 에 커플링될 수도 있다. 디바이스 (302), 로컬 인가 서버 (306), 및 인가 서버 (308) 가 이제 설명될 것이다.

[0095] 디바이스 (302) 는, 참조의 용이함을 위해, 그리고 어떤 제한 의도 없이 본원에서 "인가 기능부 (304)" 로서 지칭될 인가 회로/기능부/모듈을 포함할 수도 있다.

[0096] 인가 기능부 (304) 는 디바이스 (302) 의 프로세싱 회로 (314) 에서 및/또는 디바이스 (302) 의 보안 동작 환경 (305) 에서 보안 프로세스를 구현 (예를 들어, 보안 프로세싱을 수행) 할 수도 있다. 본원에서 사용된 바와 같이, 용어 "보안" 은 외부 및 내부 프로세스들을 포함하는 다른 프로세스들에 의한 액세스로부터 및/또는 사용자로부터 보호되거나 안전한 것을 의미할 수도 있다. 일 양태에서, 보안 동작 환경 (305), 및/또는 거기에서 구현된 보안 프로세스는 사용자에게 접근하기 힘들고/힘들거나 인가 기능부 (304) 에 의해 구현된 보안 프로세스 외의 프로세스들에 접근하기 힘들 수도 있다. 일 양태에서, 인가 기능부 (304) 가 디바이스 (302) 의 프로세싱 회로 (314) 에서 보안 프로세스를 구현하는 경우, 보안 프로세스는 사용자에게 접근하기 힘들고/힘들거나 인가 기능부 (304) 에 의해 구현된 보안 프로세스 외의 프로세스들에 접근하기 힘들 수도 있다.

[0097] 인가 기능부 (304) 는, 디바이스 (302) 가 디바이스 (302) 의 선택적으로 활성화된 피처 (320) 를 활성화시키도록 인가된다는 것을 확인하기 위한 프로세스를 구현할 수도 있다. 이 프로세스는 보안 프로세스일 수도 있다. 일 양태에서, 디바이스 (302) 가 선택적으로 활성화된 피처 (320) 를 활성화시키도록 인가된다는 것을

확인하기 위해, 인가 기능부 (304) 는 선택적으로 활성화된 피처 (320) 가 활성화되도록 인가된다는 증거 (예를 들어, 인가 정보) 를 획득할 수도 있다. 선택적으로 활성화된 피처 (320) 는 초기, 반복된, 및/또는 계속된 사용을 위해 활성화되도록 인가될 수도 있다. 확인은 획득된 증거를 검증하는 방식에 의한 것일 수도 있다.

[0098] 인가 기능부 (304) 는 또한, 디바이스 (302) 가 어태치되는 네트워크와 연관되는 네트워크 노드 (예를 들어, eNB, MME, S-GW, 등) 가 선택적으로 활성화된 피처 (320) 에 대응하는 피처를 활성화시키도록 인가된다는 것을 확인하기 위한 프로세스를 구현할 수도 있다. 이 프로세스는 보안 프로세스일 수도 있다. 네트워크 노드에서 선택적으로 활성화된 피처 (320) 에 대응하는 피처는 네트워크 노드를 통해 네트워크에 의해 제공된 서비스를 실시하는데 사용될 수도 있다. 예로서, 디바이스 (320) 는 네트워크 노드에서 제공된 네트워크 서비스를 사용하도록 네트워크 노드에서 활성화될 선택적으로 활성화된 피처 (320) 에 대응하는 피처를 필요로할 수도 있다. 추가적인 예로서, 디바이스 (302) 는, 디바이스 (302) 에서 선택적으로 활성화된 피처 (320) 를 활성화시킴으로써 달성될 수 있는 개선된 서비스를 실현하기 위해 네트워크 노드에서 활성화될 선택적으로 활성화된 피처 (320) 에 대응하는 피처를 필요로할 수도 있다. 예를 들어, 이 예시의 목적을 위해 클라이언트 디바이스일 수도 있는 디바이스 (302) 는 선택적으로 활성화된 피처 (320) 의 활성화 시에 캐리어 집성을 구현하도록 제조될 수도 있다. 캐리어 집성은 다수의 캐리어들의 사용을 허용하여 송신 대역폭을 증가시킨다. 캐리어 집성은 디바이스 (302) 의 성능을 개선시킬 수도 있다. 디바이스 (302) 는 선택적으로 활성화된 피처 (320) 를 활성화시키도록 인가될 수도 있고 캐리어 집성을 사용하기 위해 그 자체를 구성하도록 인가될 수도 있다. 그러나, 효과적이기 위해, 디바이스 (302) 에 커플링된 네트워크 액세스 노드 (예를 들어, eNB) 는 또한, 네트워크 액세스 노드가 캐리어 집성을 사용하기 위해 구성되도록 대응하는 피처를 활성화시켜야 한다. 따라서, 일부 양태들에서, 선택적으로 활성화된 피처 (320) 는 2 개의 디바이스들 (예를 들어, 칩 컴포넌트들, 클라이언트 디바이스들, 네트워크 노드들, 또는 2 이상의 이들의 임의의 조합) 에 의해 합동으로 활성화 및 사용될 수도 있다.

[0099] 일 예에서, 인가 기능부 (304) 는 인가 합의 (330) 에 정의된 (및 인가 합의 (330) 로부터 도출된 그리고 인가 기능부 (304) 에서 획득된 인가 정보에 반영된) 조항들에 따라 선택적으로 활성화된 피처 (320) 를 활성화 및/또는 비활성화시킬 수도 있다. 이 예에서, 활성화 및 사용이 수용 가능한 조항들은 인가 합의 (330) 에 의해 정의, 또는 인가 합의에 열거될 수도 있다. 이 예에서, 조항들은 선택적으로 활성화된 피처 (320) 를 사용할 권리와 교환하는 지불을 포함할 수도 있다. 일 구현에서, 디바이스 (302) 의 인가 기능부 (304) 는, 예를 들어 (예를 들어, 선택적으로 활성화된 피처 (320) 를 사용할 권리의) 검증 동안, (예를 들어, 선택적으로 활성화된 피처 (320) 의) 활성화, 및 (예를 들어, 선택적으로 활성화된 피처 (320) 에 관련된 인가 합의 (330) 의 조항들의) 시행을 포함하는 디바이스 (302) 와 연관된, 선택적으로 활성화된 피처 (320) 와 연관되는 다양한 경우들에서 유틸리티를 발견할 수도 있다. 일부 양태들에서, 선택적으로 활성화된 피처 (320) 의 활성화는 디바이스 (302) 가, 예를 들어 다른 디바이스 (예컨대, eNB) 를 통해 네트워크 (예를 들어, 인터넷) 상의 애플리케이션 서버로부터 서비스들을 획득하는 것을 허용할 수 있다.

[0100] 디바이스 (302) 는 또한, 보안 저장 회로 (310)(예를 들어, 회로/기능부/모듈) 를 포함할 수도 있다. 일 양태에서, 보안 저장 회로 (310) 는 보안 저장 회로 (310) 로부터 데이터를 판독하고 보안 저장 회로에 데이터를 기입하기 위한 (디바이스 (302) 내부 및/또는 외부의) 컴포넌트들/엔티티들의 능력에 기초하여 안전한 것으로 간주될 수도 있다. 일 양태에서, 보안 저장 회로 (310) 는 디바이스 (302) 안에 영구적으로 통합되고, 또는 이와 집적될 수도 있다. 예를 들어, 보안 저장 회로 (310) 는 디바이스 (302) 에 포함된 프로세싱 회로 (314) 와 동일한 기판 상에 조립된 비-휘발성 메모리 어레이를 포함할 수도 있다.

[0101] 보안 저장 회로 (310) 내에는, 디바이스 (302) 에 대해 도출된 사설/공용 키 쌍의 사설 키 (316) 에 대한 저장 공간이 존재할 수도 있다. 일 양태에서, 제조자 또는 OEM 은 사설/공용 키 쌍을 생성할 수도 있다. 다른 양태에서, 다른 엔티티가 사설/공용 키 쌍을 생성할 수도 있다. 사설/공용 키 쌍의 사설 키 (316) 는 제조자, OEM 에 의해, 또는 다른 엔티티에 의해 보안 저장 회로 (310) 에 저장될 수도 있다. 일 양태에서, 사설 키 (316) 는 제조자 또는 OEM 으로부터 제 3 엔티티로의 디바이스 (302) 의 소유권의 트랜스퍼 전에 보안 저장 회로 (310) 에 저장될 수도 있다. 다른 양태들에서, 사설 키 (316) 는 임의의 시간에 그리고 임의의 엔티티에 의해 보안 저장 회로 (310) 에 저장될 수도 있다. 일부 양태들에서, 사설 키 (316) 는 단지, 디바이스 (302) 에 알려져 있다. 일부 양태들에서, 사설 키 (316) 는 단지, 디바이스 (302) 의 인가 기능부 (304) 에만 알려져 있다.

[0102] 사설 키 (316) 는 피처 활성화 키들 (318) 을 포함할 수도 있는 인가 파일들 및/또는 피처 활성화 키들 (318) 을 해독하도록 디바이스 (302)(또는 인가 기능부 (304)) 에 의해 사용될 수도 있다. 피처 활성화 키들

(318) 및/또는 피처 활성화 키들 (318) 을 포함할 수도 있는 인가 파일들은, 피처 활성화 키들 (318) 을 디바이스 (302) 로 전송하기 전에 디바이스 (302) 의 공용 키를 사용하여 제 3 엔티티 (예를 들어, 인가 서버 (308)) 에 의해 서명/암호화될 수도 있다.

[0103] 일 양태에서, 피처 활성화 키 (318) 는 디바이스 (302) 의 선택적으로 활성화된 피처 (320) 를 활성화시키는데 사용될 수도 있다. 본원에 설명된 양태들에서, 피처 활성화 키들 (318) 은 암호화된 형태로 저장될 수도 있다. 일부 예들에서, 피처 활성화 키들 (318) 은 단지, (예를 들어, 디바이스 (302) 의 사설 키 (316) 를 사용하여) 인가 기능부 (304) 에 의해 해독될 수도 있다. 일부 예들에서, 피처 활성화 키들 (318) 은 보안 환경, 예컨대 보안 저장 회로 (310) 에 저장될 수도 있다.

[0104] 디바이스 (302) 는, 보안 저장 회로 (310) 로부터 별개일 수도 있는 데이터 저장 디바이스 (312)(예를 들어, 회로/기능부/모듈) 를 더 포함할 수도 있다. 일 양태에서, 보안 저장 회로 (310) 는 데이터 저장 디바이스 (312) 의 파티션일 수 있고, 그 반대일 수도 있다. 보안 저장 회로 (310) 및/또는 데이터 저장 디바이스 (312) 는, 예를 들어 하드 디스크, 하드 디스크의 파티션, 광학 디스크, 광학 디스크의 파티션, 고체 상태 메모리, 또는 고체 상태 메모리 상의 파티션을 포함할 수도 있다.

[0105] 데이터 저장 디바이스 (312) 내에, 피처들 및 인가 파라미터들의 리스트 (322) 가 저장될 수도 있다. 예를 들어, 피처들 및 인가 파라미터들의 리스트 (322) 는 디바이스 (302) 가 활성화/비활성화할 권한을 갖는 선택적으로 활성화된 피처 (320), 및 그 연관된 인가 파라미터들을 식별할 수도 있다. 피처들 및 인가 파라미터들의 리스트 (322) 는, 예를 들어 (인가 파일들을 검증하기 위해 서명이 사용될 수도 있는) 인가 서버에 의해 서명된 하나 이상의 인가 파일들로부터 컴파일링될 수도 있다. 인가 파일들은, 예를 들어 디바이스 활성화, 디바이스 핸드오버, 디바이스 업데이트 시에, 또는 디바이스 (302) 로부터의 요청에 응답하여 로컬 인가 서버 (306) 또는 인가 서버 (308) 로부터 획득될 수도 있다. 피처들 및 인가 파라미터들의 리스트 (322) 에서의 인가 파라미터들은, 예를 들어 선택적으로 활성화된 피처 (320) 가 활성화 또는 비활성화되는지 여부 및 선택적으로 활성화된 피처 (320) 를 사용하기 위한 디바이스 (302) 의 권한이 만료되거나 또는 철회되는 날짜를 나타낼 수도 있다. 본원에서 사용된 바와 같이, 선택적으로 활성화된 피처 (320) 를 사용할 디바이스 (302) 의 권한은 선택적으로 활성화된 피처 (320) 를 제공할 디바이스 (302) 의 권한을 포함한다.

[0106] 데이터 저장 디바이스 (312) 내에, 인가 인증서 (323) 가 또한 저장될 수도 있다. 일 양태에서, 인가 인증서들 (323) 은 임의의 엔티티에 의해 확인될 수도 있고 따라서 보안 스토리지에 저장될 필요가 없다. 반면에, 인가 파일(들)(324) 은 피처 활성화 키들과 같은 사설 정보를 포함한다. 따라서, 일 양태에서, 인가 파일(들)(324)은 보안 저장 회로 (310) 에 저장될 수도 있다.

[0107] 디바이스 (302) 는 또한, 디바이스 (302) 에 포함된 인가 기능부 (304), 보안 동작 환경 (305), 보안 저장 회로 (310), 데이터 저장 디바이스 (312), 프로세싱 회로 (314), 및/또는 네트워크 통신 회로 (326) 간의 통신들을 제공하도록 통신 버스 (325) 를 포함할 수도 있다. 네트워크 통신 회로 (326) 는 또한, 로컬 인가 서버 (306) 및/또는 인가 서버 (308) 와의 통신을 제공할 수도 있다.

[0108] 일부 양태들에서, 로컬 인가 서버 (306) 는 인가 서버 (308) 에 대한 로컬 프록시로서 작용할 수도 있다. 일부 양태들에서, 로컬 인가 서버 (306) 는, 로컬 인가 서버 (306) 에 의해 서명된, 디바이스 (302) 에서 선택적으로 활성화된 피처들 (320) 의 세트를 사용하기 위한 디바이스 (302) 에 대한 권한의 증거를 전송할 수도 있고, 여기서 디바이스 (302) 는 로컬 인가 서버 (306) 와 연관된 코어 네트워크에 커플링될 수도 있다. 일부 양태들에서, 로컬 인가 서버 (306) 는 인가 서버 (308) 와 독립적으로 일시적으로 동작할 수도 있다. 로컬 인가 서버 (306) 가 인가 서버 (308) 에 대한 로컬 프록시 또는 로컬 서버 그 자체로서 작용하는지 여부는, 예를 들어 인가 서버 (308) 에 저장된 인가 합의 (330) 의 조항들의 함수일 수도 있다.

[0109] 인가 서버 (308) 는 데이터 저장 디바이스 (328)(예를 들어, 회로/기능부/모듈) 를 포함할 수도 있다. 데이터 저장 디바이스 (328) 는 인가 합의들 (330)(예를 들어, 합의들, 계약들, 라이선스들) 의 리스팅, 리포지토리, 또는 레코드를 저장할 수도 있다. 인가 합의들 (330) 은 복수의 디바이스들의 다양한 선택적으로 활성화된 피처들에 관련할 수도 있다. 데이터 저장 디바이스 (328) 는 인가 합의들 (330) 에 의해 커버되는 디바이스들에 대한 키 스토리지 (332) 를 유지할 수도 있다. 키 스토리지 (332) 는 인가 합의들 (330) 에 의해 커버되는 디바이스들 (예컨대, 디바이스 (302)) 로 전송된 메시지들을 암호화하는데 사용될 수도 있는 사설 키들 및/또는 공용 키들을 포함할 수도 있다.

[0110] 인가 서버 (308) 의 데이터 저장 디바이스 (328) 는 또한, 디바이스 (302) 의 선택적으로 활성화된 피처

(들)(320) 을 활성화시키는데 사용될 수도 있는 피처 활성화 키(들)(334) 을 포함할 수도 있다. 일부 양태들에서, 피처 활성화 키(들)(334) 은, 디바이스 (302) 의 인가 기능부 (304) 가, 디바이스 (302) 가 선택적으로 활성화된 피처(들)(320) 중 하나 이상을 활성화시키기 위한 권한을 갖는다는 증거를 요청하는 경우, 인가 서버 (308)(또는 로컬 인가 서버 (306)) 로부터 디바이스 (302) 로 전송될 수 있다. 이러한 양태들에서, 선택적으로 활성화된 피처(들)(320) 은, 인가 서버 (308)(또는 로컬 인가 서버 (306)) 가, 디바이스 (302) 가 선택적으로 활성화된 피처(들)(320) 을 활성화시키기 위한 권한을 갖는다는 증거 (예를 들어, 인가 정보) 를 인가 기능부 (304) 로 전송한 후에, 인가 기능부 (304) 에 의해 (또는 그 권한으로) 활성화될 수도 있다.

[0111] 일 예에서, 인가 서버 (308) 의 데이터 저장 디바이스 (328) 는 디바이스 모델 넘버의 함수로서, 디바이스 (302) 에서 각각 선택적으로 활성화된 피처 (320) 에 대한 인가 파라미터들 (336) 의 리스팅, 리포지토리, 또는 레코드를 저장할 수도 있다. 일 양태에서, 동일한 모델 넘버를 갖는 개별의 디바이스들의 구별을 허용하기 위해, 예를 들어 데이터 저장 디바이스 (328) 는 디바이스 시리얼 넘버의 함수, 또는 국제 이동국 장비 아이덴티티 (IMEI) 와 같은 다른 디바이스 식별자로서 각각 선택적으로 활성화된 피처 (320) 에 대한 인가 파라미터들 (336) 을 저장할 수도 있다. 당업자에게 알려진 바와 같이, IMEI 는 제 3 세대 파트너쉽 프로젝트 (3GPP) 시스템들 (예를 들어, GSM, UMTS, LTE, LTE-A) 에 따라 하드웨어를 식별하는데 사용되는 고유 넘버이다.

[0112] 인가 서버 (308) 는 또한, 인가 서버 (308) 에 포함된 데이터 저장 디바이스 (328), 프로세싱 회로 (340), 및/또는 네트워크 통신 회로 (342) 간의 통신들을 제공하도록 통신 버스 (338) 를 포함할 수도 있다. 네트워크 통신 회로 (342) 는 또한, 로컬 인가 서버 (306) 및/또는 디바이스 (302) 와의 통신을 제공할 수도 있다.

[0113] 위에서 나타낸 바와 같이, 로컬 인가 서버 (306) 는 인가 서버 (308) 에 대한 프록시로서 역할을 할 수도 있다. 이와 같이, 로컬 인가 서버 (306) 는 인가 서버 (308) 의 것과 동일한 또는 유사한 회로들/기능부들/모듈들을 포함한다. 동일한 또는 유사한 회로들/기능부들/모듈들의 설명 및 예시는 따라서 생략될 것이다.

[0114] **인가 합의들**

[0115] 도 1 로 돌아가, 선택적으로 활성화된 피처들 (110, 114, 118) 의 세트를 사용하기 위한 디바이스 (102, 104, 106) 의 권한은 인가 합의 (120)(예를 들어, 합의, 계약, 라이선스) 에서 주어질 수도 있다. 일부 양태들에서, 인가 합의 (120) 는 라이선스로 간주될 수도 있다. 본원에서 사용된 바와 같이, 일 양태에서, 선택적으로 활성화된 피처들의 세트에 대한 참조, 또는 선택적으로 활성화된 피처(들)에 대한 참조는 하나의 선택적으로 활성화된 피처에 대한 참조인 것으로 이해될 수도 있다 (예를 들어, 세트가 하나의 선택적으로 활성화된 피처를 포함하고 또는 세트가 하나 이상의 별개의 선택적으로 활성화된 피처들을 포함하는 경우). 인가 합의 (120) 는 증거로서 사용될 수도 있고, 또는 인가 합의 (120) 는 디바이스 (102, 104, 106) 에서 선택적으로 활성화된 피처들 (110, 114, 118) 의 세트를 사용 (예를 들어, 활성화, 활성화의 유지) 하기 위한 디바이스 (102, 104, 106) 의 권한의 증거를 도출하는데 사용될 수도 있다.

[0116] 인가 합의 (120) 는 2 이상의 엔티티들 간에 확립될 수도 있다. 인가 합의 (120) 로의 엔티티들은, 예를 들어 디바이스에 대한 권리들, 디바이스의 피처, 및/또는 디바이스에 의해 사용될 서비스를 주장할 수도 있다. 예로서, 인가 합의 (120) 는 제조자, 벤더/OEM, 디바이스 구매자, 재-판매자, 라이선싱 서비스, 및/또는 제조자, 벤더/OEM, 디바이스 구매자, 재-판매자, 또는 라이선싱 서비스 중 임의의 2 이상 간에 확립될 수도 있다. 디바이스 구매자는 엔드 사용자, 재-판매자, 또는 디바이스를 대여할 엔티티일 수도 있다. 라이선싱 서비스는 라이선스들을 허가하고 라이선싱 조항들의 준수를 모니터링하는 기관일 수도 있다.

[0117] 일 예에서, 인가 합의 (120) 는, 인가 기능부 (108, 112, 116) 가 인가 합의 (120) 의 증거를 획득하고자 하는 시간에 앞서 확립될 수도 있다. 다른 예에서, 인가 합의는, 인가 기능부 (108, 112, 116) 가 인가 합의 (120) 의 증거를 획득하고자 하는 때와 동시에, 또는 실질적으로 동시에 확립될 수도 있다.

[0118] 인가 합의 (120) 는 기입으로서 지칭될 수도 있다. 본원에서 사용된 바와 같이, 기입은 이러한 인가 합의들이 물리적 인간-판독가능 형태로 존재했는지 여부에 관계없이 인가 합의들의 모든 비-일시적 머신 판독가능 표현들을 포함한다. 용어 "기입" 은 머신에 의해 판독될 수 있는 임의의 형태로 축소된 임의의 인간-판독가능 문서를 포함한다. 머신에 의해 판독될 수 있는 형태들은 전기적, 광학, 자기적, 또는 당업자에게 알려진 다른 저장 형태들을 포함할 수도 있다.

[0119] 일 예에서, 인가 합의는 다음을 포함하는 인가 인증서를 도출하는데 사용될 수도 있다:

[0120] 1. 사용을 위해 인가된 선택적으로 활성화된 피처들의 세트;

[0121] 2. 수명/만료 시간;

[0122] 3. 선택적으로 활성화된 피처들이 인에이블되는 로케이션 (예를 들어, PLMN, SSID들, 또는 셀 IDS들과 같은 지리학적 또는 네트워크 식별자들을 포함하는);

[0123] 4. 선택적으로 활성화된 피처들을 사용할 수 있는 네트워크 액세스 노드들의 최대 수;

[0124] 5. 주기적 사용 보고 요건들.

[0125] 도 4 는 본원에 설명된 양태들에 따른 하나 이상의 디바이스들의 제조자 또는 OEM 과 제 1 엔티티 (예를 들어, 디바이스의 오너, 디바이스의 판매자/재판매자, 디스카운트하여 또는 디스카운트 없이 소비자들에게 디바이스를 제공하는 서비스 제공자) 간의 예시적인 인가 합의에 포함될 수도 있는 데이터 및 파라미터들의 예시적인 리스트 (400) 를 예시한다. 리스팅은 도 4 에서 표로 만든 형태로 제시되지만, 임의의 머신 판독가능 (예를 들어, 프로세싱 회로 판독가능) 형태가 이 양태에 따라 수용 가능하다. 리스팅은 파라미터들, 예컨대 합의의 날짜 (402), 디바이스의 오너의 식별자 (404), 디바이스의 제조자 또는 OEM 의 식별자 (406), 디바이스의 식별자 (408)(예를 들어, IMEI 넘버), 인가된 피처들의 리스트 (410), 인가 합의의 지속기간 (412), 피처들의 사용상의 제한들 (414), 및 피처들의 사용에 대한 요금 (416) 을 포함한다.

[0126] 도 5 는 본원에 설명된 양태들에 따른 제조자 또는 OEM 과 다른 엔티티 (예를 들어, 인가 서버를 동작하는 엔티티) 간의 예시적인 인가 합의에 포함될 수도 있는 파라미터들 및 데이터의 예시적인 리스트 (500) 를 예시한다.
리스팅은 도 5 에서 표로 만든 형태로 제시되지만, 임의의 머신 판독가능 (예를 들어, 프로세싱 회로 판독가능) 형태가 이 양태에 따라 수용 가능하다. 리스팅은 파라미터들, 예컨대 합의의 시작 날짜 (502), 합의의 종료 날짜 (504), 디바이스의 식별자 (506)(예를 들어, IMEI 넘버), 인가된 피처들의 리스트 (508), 피처들의 사용 상의 제한들 (510), 디바이스의 공용 키의 식별자 (512), 디바이스의 제조자 또는 OEM 의 식별자 (514), 및 피처들의 사용에 대한 요금 (516) 을 포함한다.

[0127] 도 6 은 본원에 설명된 양태들에 따른 네트워크 오퍼레이터 (예를 들어, 모바일 네트워크 오퍼레이터 (MNO)) 와 다른 엔티티 (예를 들어, 인가 서버의 오너/오퍼레이터) 간의 예시적인 인가 합의에 포함될 수도 있는 데이터 및 파라미터들의 예시적인 리스팅 (600) 을 예시한다. 예시적인 리스팅 (600) 은 도 6 에서 표로 만든 형태로 제시되지만, 임의의 머신 판독가능 (예를 들어, 프로세싱 회로 판독가능) 형태가 이 양태에 따라 수용 가능하다. 예시적인 리스팅 (600) 은 파라미터들, 예컨대 인가 합의의 시작 날짜 (602), 인가 합의의 종료 날짜 (604), 디바이스의 식별자 (606)(예를 들어, IMEI 넘버), 인가된 서비스(들)의 리스트 (608), 인가된 피처들의 리스트 (610), 디바이스의 제조자 또는 OEM 의 식별자 (612), 및 피처들의 사용에 대한 요금 (614) 을 포함한다.

[0128] **프로비저닝**

[0129] 도 7 은 본원에 설명된 양태들에 따른 인가 인증서들, 인가 파일들, 피처 활성화 키들, 및 소프트에어를 디바이스들 (예를 들어, 칩 컴포넌트들, 클라이언트 디바이스들, 네트워크 노드들) 로 전송하는 것에 관련된 액션들을 예시하는 흐름도이다. 일 양태에서, 참조 부호들 (702-712) 로 식별된 액션들은 인가 서버에 의해 취해질 수도 있는 한편, 참조 부호 (714) 로 식별된 액션은 로컬 인가 서버에 의해 취해질 수도 있다. 일 양태에서, 참조 부호들 (702-714) 로 식별된 액션들은 인가 서버에 의해 취해질 수도 있다. 즉, 이러한 양태들에서, 인가 서버는 인가 인증서, 인가 파일, 피처 활성화 키(들), 및/또는 소프트웨어를 도출하고 로컬 인가 서버의 중재 없이 디바이스로 전송할 수도 있다. 일 양태에서, 참조 부호들 (702-714) 로 식별된 액션들은 로컬 인가 서버에 의해 취해질 수도 있다. 즉, 이러한 양태들에서, 로컬 인가 서버는 인가 인증서, 인가 파일, 피처 활성화 키(들), 및/또는 소프트웨어를 도출하고 인가 서버의 중재 없이 디바이스로 전송할 수도 있다.

[0130] 전술된 바와 같이, 다양한 엔티티들 (예를 들어, 디바이스의 오너, 디바이스의 판매자/재-판매자, 디스카운트하여 또는 디스카운트 없이 소비자들에게 디바이스를 제공하는 서비스 제공자, 제조자, 또는 디바이스의 OEM) 간에 인가 합의들이 시작될 수도 있다. 예를 들어, 하나의 엔티티는 미리정의된 시간 동안 (예를 들어, 분기별로) 선택적으로 활성화된 피처 또는 서비스를 사용할 권리에 대한 요금을 제 2 엔티티에 지불할 수도 있다.
일단 엔티티들이 인가 합의로 시작되면, 인가 합의는 인가 서버 상에 저장 (702)될 수도 있다. 인가 서버는 인가 합의에서의 정보에 기초하여 피처 활성화 키(들)을 도출 (704)(예를 들어, 인가 합의에 기초하여 피처 활성화 키(들)을 도출 (704)) 할 수도 있다. 인가 서버는 인가 합의에서의 정보에 기초하여 인가 인증서를 도출 (706) 할 수도 있다. 인가 서버는 또한, 인가 합의에서의 정보에 기초하여 인가 파일을 도출 (708)

할 수도 있다. 일부 양태들에서, 인가 파일은 하나 이상의 피처 활성화 키들을 포함할 수도 있다. 이들 액션들의 순서는 예시적이며 비제한적이다. 임의의 순서가 수용 가능하다.

[0131] 피처 활성화 키는 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 의 선택적으로 활성화된 피처를 활성화시키는데 사용될 수도 있다. 피처 활성화 키는 암호화될 수도 있고, 및/또는 그와 함께 피처 활성화 키(들)을 갖는 인가 파일이 암호화될 수도 있다. 일부 예들에서, 피처 활성화 키(들) 및/또는 인가 파일은 단지, 디바이스의 인가 기능부에 의해 해독될 수도 있다.

[0132] 일부 양태들에서, 선택적으로 활성화된 피처 당 하나의 피처 활성화 키는 선택적으로 활성화된 피처 활성화를 위해 사용될 수도 있다. 다른 양태들에서, 하나의 피처 활성화 키는 다수의 선택적으로 활성화된 피처들을 활성화시키는데 사용될 수도 있다. 선택적으로 활성화된 피처를 활성화시키는 것은 선택적으로 활성화된 피처의 초기 활성화 뿐만 아니라 이미 활성화된 선택적으로 활성화된 피처의 활성화를 유지하는 것을 포함할 수도 있다. 일 양태에서, 피처 활성화 키는 선택적으로 활성화된 피처를 언로크할 수도 있다. 예로서, 선택적으로 활성화된 피처가 활성화될 수도 있지만, 인가 합의의 기간들에 기초하여 사용으로부터 로크될 수도 있다 (예를 들어, 선택적으로 활성화된 피처는 인가 합의에 의해 부과된 지리학적 또는 시간-관련 파라미터 제한에 기초하여 사용으로부터 로크될 수도 있다). 활성화된 선택적으로 활성화된 피처는 적합한 피처 활성화 키의 획득 및 사용에 기초하여 언로크될 수도 있다 (예를 들어, 이미 활성화된 선택적으로 활성화된 피처를 사용하기 위한 디바이스의 능력이 인에이블될 수도 있다).

[0133] 인가 파일은 선택적으로 활성화된 피처에 관련한 데이터를 포함할 수도 있다. 선택적으로 활성화된 피처에 관련한 데이터는, 예를 들어 선택적으로 활성화된 피처를 사용하기 위한 디바이스의 권한이 만료 또는 철회될 때의 날짜를 포함할 수도 있다. 선택적으로 활성화된 피처에 관련한 다른 데이터는 또한, 인가 파일에 포함될 수도 있다.

[0134] 일 양태에서, 인가 서버는 피처 활성화 키(들)을 포함하는 인가 파일 및 인가 인증서를 로컬 인가 서버로 전송 또는 업로드 (예를 들어, 프로비전) (710) 할 수도 있다. 인가 서버는 선택적으로, 디바이스의 선택적으로 활성화된 피처들에 관련된 소프트웨어, 또는 디바이스에 관련된 임의의 피처 (하드웨어 또는 소프트웨어) 를 로컬 인가 서버로 전송 또는 업로드 (712) 할 수도 있다. 예를 들어, 업데이트된 드라이버 형태의 소프트웨어가 인가 인증서 및 인가 파일에 추가하여 전송 또는 업로드될 수도 있다.

[0135] 인가 서버 및/또는 로컬 인가 서버는, 예를 들어 디바이스로부터 피처 활성화 요청을 획득하는 것에 응답하여 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 로 인가 인증서, 피처 활성화 키(들)을 포함하는 인가 파일, 및 소프트웨어 (선택적) 를 전송 (714) 할 수도 있다.

[0136] 일 예에서, 다수의 디바이스들이 인가 합의에 포함되는 경우, 로컬 인가 서버는, 최대 수 보다 많지 않은 디바이스들 (예를 들어, 쿼타) 이 인가된 선택적으로 활성화된 피처를 사용하고 있다는 것을 보장할 수도 있다. 예를 들어, 로컬 인가 서버는, 로컬 인가 서버가 제 2 디바이스에서 선택적으로 활성화된 피처를 활성화시키기 위한 인가를 발행하기 전에 선택적으로 활성화된 피처가 제 1 디바이스에서 비활성화되는 때의 표시를 수신할 수도 있다. 대안으로, 로컬 인가 서버는, 로컬 인가 서버가 제 2 디바이스에서 선택적으로 활성화된 피처를 활성화시키기 위한 인가를 발행하기 전에 제 1 디바이스에서 선택적으로 활성화된 피처를 활성화시키기 위한 인가를 철회할 수도 있다. 철회는, 예를 들어 어느 디바이스들에서 선택적으로 활성화된 피처가 활성화되어 사용되고 있는지를 결정하도록 모든 인가된 디바이스들로부터의 주기적인 보고에 기초할 수도 있다.

[0137] **피처 활성화 요청**

[0138] 도 8 은 본원에 설명된 양태들에 따른 피처 활성화 요청 (예를 들어, 하나 이상의 피처들을 활성화시키기 위한 요청, 하나 이상의 피처들을 활성화시키기 위한 인가에 대한 요청) 을 수반하는 방법을 예시하는 흐름도 (800) 이다. 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 는, 디바이스가 그렇게 하기 위한 인가를 갖는 경우 선택적으로 활성화된 피처를 활성화시킬 수도 있다. 다양한 이벤트들은 디바이스가 피처 활성화 요청을 전송하는 것을 초래할 수도 있다. 예를 들어, 선택적으로 활성화된 피처는 네트워크 서비스를 사용하는데 필요할 수도 있고, 관리자는 선택적으로 활성화된 피처를 인보크하는 방식으로 디바이스를 구성하도록 결정할 수도 있고, 가입 업데이트가 발생할 수도 있으며/있거나 동작, 행정, 및 관리 (OAM) 프로토콜이 유지 목적들을 위해 선택적으로 활성화된 피처를 활성화시키기 위해 필요할 수도 있다.

[0139] 선택적으로 활성화된 피처를 활성화시키기 위해, 디바이스는 디바이스에서 선택적으로 활성화된 피처를 사용하도록 디바이스에 대한 권한의 증거를 획득하고, 피처 활성화 키(들)을 포함하는 인가 파일을 획득할 수도 있다.

권한의 증거는, 예를 들어 인가 정보의 형태로 제공될 수도 있다. 인가 정보는 인가 합의 및/또는 인가 인증서를 포함할 수도 있다. 일 예에서, 선택적으로 활성화된 피처 및 피처 활성화 키(들)을 포함하는 인가 파일을 사용하기 위한 디바이스에 대한 권한의 증거를 획득하기 위해, 디바이스는 피처 활성화 요청 (예를 들어, 하나 이상의 선택적으로 활성화된 피처들을 활성화시키기 위한 요청) 을 로컬 인가 서버로 전송할 수도 있다.

[0140] 로컬 인가 서버는 디바이스로부터 피처 활성화 요청을 획득 (802) 할 수도 있다. 로컬 인가 서버는, 로컬 인가 서버가 요청에 대한 응답에 필요한 아이템들 (예를 들어, 디바이스에 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거, 예컨대 인가 정보, 및 피처 활성화 키(들)을 포함하는 인가 파일) 을 보유하는지를 결정 (804) 할 수도 있다. 로컬 인가 서버가 필요한 아이템들을 보유하지 않으면, 또는 로컬 인가 서버가 아이템들을 보유하지만 이 아이템들이 (예를 들어, 인가의 만료로 인해) 유효하지 않으면, 로컬 인가 서버는 인가 서버로부터, 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 및 피처 활성화 키(들)을 포함하는 인가 파일을 획득 (806) 하도록 시도할 수도 있다.

[0141] 일 양태에서, 로컬 인가 서버는 인가 서버로부터 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 및 피처 활성화 키(들)을 포함하는 인가 파일을, 피처 활성화 요청을 인가 서버로 포워딩함으로써 획득 (806) 할 수도 있다. 인가 서버는, 예를 들어 인가 합의가, 요청된 선택적으로 활성화된 피처들이 인가된다는 것을 확인하는 경우 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 및 피처 활성화 키(들)을 포함하는 인가 파일을 전송할 수도 있다. 피처 활성화 요청이 인가 서버로 전송되는 경우에서, 로컬 인가 서버는 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 와 인가 서버 간의 보안 터널을 제공하는 프록시 서버로서 작용할 수도 있다. (예를 들어, 디바이스와 라이선싱 서비스 간 및/또는 모바일 네트워크 오퍼레이터와 라이선싱 서비스 간의) 인가 합의를 확인한 후에, 인가 서버는 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 및 피처 활성화 키(들)을 포함하는 인가 파일을 로컬 인가 서버로 전송할 수도 있다.

[0142] 로컬 인가 서버가 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 및 인가 파일을 보유하면, 로컬 인가 서버는 요청된 선택적으로 활성화된 피처에 대해 쿼타에 도달되는지를 결정 (808) 할 수도 있다. 요청된 선택적으로 활성화된 피처에 대한 쿼타에 도달되면, 로컬 인가 서버는 선택적으로 활성화된 피처를 활성화시키기 위한 요청을 거부하는 응답을 디바이스로 전송 (810) 할 수도 있다. 거부에 대한 이유는 응답에 포함될 수도 있다. 요청된 선택적으로 활성화된 피처에 대한 쿼타에 도달되지 않으면, 로컬 인가 서버는, 예를 들어 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 및 피처 활성화 키(들)을 포함하는 인가 파일을 포함하는 응답을 디바이스로 전송 (812) 할 수도 있다.

[0143] 로컬 인가 서버는 인가 합의들, 인가 인증서들, 인가 파일들, 피처 활성화 키(들), 및 미래의 사용을 위한 선택적 소프트웨어를 캐시할 수도 있다. 일 양태에서, 캐싱은, 로컬 인가 서버가 인가 서버 대신에 인가 인증서를 발행하고 인가 스테이터스를 인가 서버로 보고하는 경우 적용할 수도 있다.

[0144] **선택적으로 활성화된 피처들의 활성화**

[0145] 도 9 는 본원에 설명된 양태들에 따른 선택적으로 활성화된 피처들의 활성화의 일 예를 예시하는 흐름도 (900) 이다. 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드), 또는 디바이스의 인가 기능부는 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스의 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 를 획득 (902) 할 수도 있고, 또한 피처 활성화 키들을 포함하는 인가 파일을 획득할 수도 있으며, 여기서 권한의 증거는 인가 서버에 의해 서명된다. 일 양태에서, 권한의 증거 및 인가 파일은 피처 활성화 요청 (예를 들어, 하나 이상의 선택적으로 활성화된 피처들을 활성화시키기 위한 요청) 에 응답하여 획득될 수도 있다. 인가 파일은 디바이스의 공용 키로 암호화된 피처 활성화 키들을 포함할 수도 있다. 인가 기능부는 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 를 검증 (904) 할 수도 있다. 일 양태에서, 검증은 검증 함수 및 인가 서버의 공용 키를 사용하는 것을 포함할 수도 있다. 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 가 검증되면, 디바이스는 디바이스의 사설 키를 사용하여 피처 활성화 키들을 포함하는 인가 파일을 해독 (906) 할 수도 있다. 인가 기능부는 해독된 인가 파일로부터 피처 활성화 키들을 취출할 수도 있다. 인가 기능부는 인가 파일에 포함된 인가 파라미터들을 평가 (908)(예를 들어, 인가 파라미터들, 예컨대 선택적으로 활성화된 피처를 사용하기 위한 디바이스의 권한의 만료 날짜가 만료되지 않았다는 것을 확인) 할 수도 있다. 인가 기능부는 그 후, 해독된 피처 활성화 키들을 사용하여 선택적으로 활성화된 피처들의 세트를 활성화 (910) 시킬 수도 있다.

[0146] 임의의 활성화된 선택적으로 활성화된 피처는, 비활성화 이벤트가 발생할 때까지 활성화된 채로 있을 수도 있다. 비활성 이벤트의 일 예는 활성화된 선택적으로 활성화된 피처와 연관된 인가 파라미터들에서 지정된 만료 시간의 도달일 수 있다. 다른 비활성화 이벤트들이 수용 가능하다. 인가 기능부는 취출된 피처 활성화 키를 디바이스의 보안 저장 디바이스에 저장 (912) 할 수도 있다. 인가 기능부는 또한, 취출된 인가 파라미터들을 디바이스의 데이터 저장 디바이스에 저장 (912) 할 수도 있다.

[0147] 일 예에서, 디바이스의 인가 기능부는, 적어도, 인가 서버가 디바이스의 (공용/사설 키 쌍의) 공용 키를 사용하여 인가 파일을 암호화했을 수도 있고, 디바이스가 디바이스의 보안 저장 회로에 사설 키를 저장했을 수도 있으며, 사설 키는 인가 기능부에만 알려져 있을 수도 있기 때문에, 인가 파일을 신뢰할 수 있게 그리고 보안의 우수한 보장으로 해독할 수도 있다. 디바이스는, 선택적으로 활성화된 피처(들)의 활성화가 적합하다는 것을 보장하도록 인가 기능부에 의존할 수도 있다. 부가적으로, 디바이스가 네트워크 (예를 들어, 인가 서버) 로부터 인가 인증서를 수신하는 경우, 디바이스는, 인가 인증서가 (예를 들어, 임포스터 (imposter) 에 의해 전송되지 않은) 인가 서버에 의해 전송된 정확한 인가 인증서라는 것을 확인할 수 있어야 한다. 일 예에서, 인가 인증서가 인가 서버에 의해 전송된 정확한 인가 인증서라는 것을 확인하기 위한 디바이스의 능력을 용이하게 하기 위해, 인가 서버는 (인가 서버의 사설 키로 도출된) 인가 서버의 서명을 인가 인증서에 추가할 수 있다.
인가 서버의 서명은 인가 서버의 공용 키를 사용하여 디바이스에서 확인될 수도 있다. 유사하게, 디바이스가 네트워크 (예를 들어, 인가 서버) 로부터 인가 파일을 수신하는 경우, 디바이스는, 인가 파일이 (예를 들어, 임포스터에 의해 전송되지 않은) 인가 서버에 의해 전송된 정확한 인가 파일이라는 것을 확인할 수 있어야 한다. 일 예에서, 인가 파일이 인가 서버에 의해 전송된 정확한 인가 파일이라는 것을 확인하기 위한 디바이스의 능력을 용이하게 하기 위해, 인가 서버는 인가 서버의 서명 (인가 서버의 사설 키로 도출된 서명) 을 인가 파일에 추가할 수 있다. 인가 서버의 서명은 인가 서버의 공용 키를 사용하여 디바이스에서 확인될 수도 있다.

[0148] 디바이스는 활성화된 선택적으로 활성화된 피처의 사용을 모니터링할 수도 있고, 선택적으로 활성화된 피처들의 사용에 관련된 주기적인 레포트들을 인가 서버 및/또는 로컬 인가 서버로 전송 (914)(예를 들어, 활성화 스테이터스를 보고) 할 수도 있다. 인가 서버 및/또는 로컬 인가 서버는 이러한 레포트들을 전송한 모든 디바이스들로부터 선택적으로 활성화된 피처들의 사용에 관련된 레포트들을 집성할 수도 있다. 선택적으로 활성화된 피처들의 사용 스테이터스에 대한 레포트는 스테이터스 레포트로서 본원에 지칭될 수도 있다. 주기적 스테이터스 레포트들은, 예를 들어 선택적으로 활성화된 피처들을 사용하기 위한 디바이스들의 권리들에 대한 제한들을 강요하는데 사용될 수도 있다. 예를 들어, 인가 서버 (또는 로컬 인가 서버) 는 스테이터스 레포트들로부터 획득된 데이터를 사용하여, 최대 수보다 더 많은 디바이스들이 선택적으로 활성화된 피처를 동시에 사용하고 있는지 또는 아닌지를 확인할 수도 있다. 최대 수보다 더 많은 디바이스들이 선택적으로 활성화된 피처를 동시에 사용하고 있으면 (예를 들어, 쿼타에 도달되면), 선택적으로 활성화된 피처를 활성화시키기 위한 새로운 요청들이 거부될 수도 있다. 사용, 라이선스 요금들 등에 관련한 레코드들이 도출되고 유지될 수도 있다.

[0149] **오케스트레이션 절차**

[0150] 일 양태에서, 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 에서 성공적인 피처 활성화 시에, 인가 서버는 데이터를 디바이스와 연관된 HSS/AAA 서버로 송신하여 디바이스의 업데이트된 피처들/업데이트된 능력을 HSS/AAA 서버에 알릴 수도 있다.

[0151] HSS/AAA 서버는 디바이스의 가입 프로파일을 업데이트할 수도 있고, 업데이트된 디바이스 피처들이 네트워크 오퍼레이터 (예를 들어, MNO) 에 의해 확인된 후에 정보를 네트워크 노드들 (예를 들어, eNodeB, MME, P-GW, 등) 로 전송할 수도 있다. 일부 양태들에서, 이것은 디바이스의 능력 및 인가 스테이터스에 기초하여 가입 프로파일을 업데이트하기 위한 네트워크 오퍼레이터의 역할일 수 있다.

[0152] 디바이스의 가입 프로파일을 업데이트하는 것은, 일단 하나 이상의 피처들을 활성화시키기 위한 요청이 수락되고/되거나 피처들이 활성화되면, 네트워크 노드 (예를 들어, eNB, MME, S-GW, P-GW) 가 증거의 다른 형태를 획득하기 위해 네트워크 노드에 대한 필요성 없이 피처를 사용할 디바이스의 인가를 검증하는 것을 허용할 수도 있다. 예를 들어, 네트워크 노드가 가입 프로파일에 기초하여 피처를 사용하기 위한 디바이스의 인가를 검증하는 것을 허용하도록 가입 프로파일을 업데이트하는 것은 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 디바이스로부터 획득하도록 네트워크 노드의 필요성을 배제할 수도 있다.

[0153] 일 양태에서, 디바이스가 네트워크 액세스 노드 (예를 들어, eNodeB) 인 경우, 네트워크 액세스 노드에서 활성화되는 피처들/서비스들의 소정 세트의 이용 가능성에 관련한 정보는 디바이스로 전송될 수도 있다. 일부 구현들에서, 네트워크 액세스 노드에서 활성화되는 피처들/서비스들의 소정 세트는 공중파 브로드캐스트 (예를 들어, 시스템 정보 블록 (SIB) 유형 1 브로드캐스트) 를 통해 디바이스들 (예를 들어, 칩 컴포넌트들, 클라이언트 디바이스들) 에 알려질 수도 있다. 일부 구현들에서, 디바이스는 네트워크 액세스 노드에 질의하도록 프로토콜을 사용할 수도 있고, 이에 의해 네트워크 액세스 노드에서 활성화될 수도 있는 피처들/서비스들의 소정 세트의 이용 가능성을 결정할 수도 있다. 이러한 질의 프로토콜의 일 예는 액세스 네트워크 질의 프로토콜 (ANQP) 일 수도 있다. 다른 질의 프로토콜들이 수용 가능하다. 이들 예시적인 방식들에서, 디바이스는, 디바이스가 상호 인증 후에 피처들/서비스들을 사용하기를 원하는지 디바이스가 결정할 수 있도록 네트워크 액세스 노드로부터 이용 가능한 피처들/서비스들을 알게 될 수도 있다.

[0154] **예시적인 인가 서버**

[0155] 도 10 은 본원에 설명된 양태들에 따른 인가 합의들의 동적 확인 및 시행을 지원하도록 구성된 인가 서버 (1000) 를 예시하는 블록도이다. 일 예에서, 인가 서버 (1000) 는 네트워크 통신 회로 (1002), 프로세싱 회로 (1004), 및 (메모리 회로 (1006) 로서 본원에 지칭된) 메모리 회로/저장 디바이스를 포함할 수도 있다. 네트워크 통신 회로 (1002), 프로세싱 회로 (1004), 및 메모리 회로 (1006) 는 데이터 및 명령들의 교환을 위해 통신 버스 (1008) 에 커플링될 수도 있다.

[0156] 네트워크 통신 회로 (1002) 는 네트워크 노드들, 예컨대 P-GW 디바이스, 로컬 인가 서버, 및/또는 네트워크 액세스 노드와 통신하기 위한 입/출력 모듈/회로/기능부 (1010) 를 포함하도록 구성될 수도 있다. 당업자에 의해 인지되는 바와 같이, 다른 회로들/기능부들/모듈들이 인가 서버 (1000) 의 네트워크 통신 회로 (1002) 에 포함될 수도 있다.

[0157] 프로세싱 회로 (1004) 는 인가 합의들의 동적 확인 및 시행을 지원하도록 구성되는 하나 이상의 프로세서들, 애플리케이션 특정 프로세서들, 하드웨어 및/또는 소프트웨어 모듈들 등을 포함 또는 구현하도록 구성될 수도 있다. 프로세싱 회로 (1004) 는, 인가 서버 (1000) 에 저장된 인가 합의들의 수집, 유지, 및 구성을 관리할 수도 있는, 인가 합의 관리 회로/기능부/모듈 (1012) 을 포함할 수도 있다. 프로세싱 회로 (1004) 는, 디바이스들 (예를 들어, 칩 컴포넌트들, 클라이언트 디바이스들, 네트워크 노드들) 의 선택적으로 활성화된 피처들을 활성화시키는데 사용될 수도 있는 피처 활성화 키들을 도출하는데 사용될 수도 있는, 피처 활성화 키 도출 회로/기능부/모듈 (1014) 을 포함할 수도 있다. 프로세싱 회로 (1004) 는, 피처 활성화 키들과 함께 디바이스들로 패스될 수도 있는 인가 파라미터들 (예를 들어, 인가된 선택적으로 활성화된 피처의 만료 날짜) 을 도출하는데 사용될 수도 있는, 인가 파라미터 도출 회로/기능부/모듈 (1016) 을 포함할 수도 있다. 프로세싱 회로 (1004) 는, 인가 합의에 기초하여 인가 인증서를 도출할 수도 있고 인가 서버 (1000) 의 사설 키로 인가 인증서에 서명할 수도 있는, 인가 인증서 도출 회로/기능부/모듈 (1018) 을 포함할 수도 있다. 당업자에 의해 인지되는 바와 같이, 다른 회로들/기능부들/모듈들이 인가 서버 (1000) 의 프로세싱 회로 (1004) 에 포함될 수도 있다.

[0158] 메모리 회로 (1006) 는 인가 합의 관리 명령들 (1020), 피처 활성화 키 도출 명령들 (1022), 인가 파라미터 도출 명령들 (1024), 인가 인증서 도출 명령들 (1026), 뿐만 아니라 피처 활성화 키 스토리지 (1030), 인가 파라미터 스토리지 (1032), 공용 키 스토리지 (1034), 및 인가 인증서 스토리지 (1036) 를 위한 공간을 포함하도록 구성될 수도 있다. 당업자에 의해 인지되는 바와 같이 데이터의 저장을 위한 다른 명령들 및 로케이션들이 메모리 회로 (1006) 에 포함될 수도 있다.

[0159] **예시적인 로컬 인가 서버**

[0160] 도 11 은 본원에 설명된 양태들에 따른 인가 합의들의 동적 확인 및 시행을 지원하도록 구성된 로컬 인가 서버 (1100) 를 예시하는 블록도이다. 로컬 인가 서버 (1100) 는 인가 서버 (예를 들어, 도 10 의 1000) 에 대한 프록시일 수도 있다. 일 예에서, 로컬 인가 서버 (1100) 는 네트워크 통신 회로 (1102), 프로세싱 회로 (1104), 및 (메모리 회로 (1106) 로서 본원에 지칭된) 메모리 회로/저장 디바이스를 포함할 수도 있다. 네트워크 통신 회로 (1102), 프로세싱 회로 (1104), 및 메모리 회로 (1106) 는 데이터 및 명령들의 교환을 위해 통신 버스 (1108) 에 커플링될 수도 있다.

[0161] 네트워크 통신 회로 (1102) 는 네트워크 노드들, 예컨대 인가 서버, 및/또는 네트워크 액세스 노드와 통신하기 위한 입/출력 모듈/회로/기능부 (1110) 를 포함하도록 구성될 수도 있다. 당업자에 의해 인지되는 바와 같

이, 다른 회로들/기능부들/모듈들이 로컬 인가 서버 (1100) 의 네트워크 통신 회로 (1102) 에 포함될 수도 있다.

[0162] 프로세싱 회로 (1104) 는 인가 합의들의 동적 확인 및 시행을 지원하도록 구성되는 하나 이상의 프로세서들, 애플리케이션 특정 프로세서들, 하드웨어 및/또는 소프트웨어 모듈들 등을 포함 또는 구현하도록 구성될 수도 있다. 프로세싱 회로 (1104) 는, 로컬 인가 서버 (1100) 에 저장된 인가 합의들의 수집, 유지, 및 구성을 관리할 수도 있는, 인가 합의 관리 회로/기능부/모듈 (1112) 을 포함할 수도 있다. 프로세싱 회로 (1104) 는, 디바이스들의 선택적으로 활성화된 피처들을 활성화시키는데 사용될 수도 있는 피처 활성화 키들을 도출하는데 사용될 수도 있는, 피처 활성화 키 도출 회로/기능부/모듈 (1114) 을 포함할 수도 있다. 프로세싱 회로 (1104) 는, 피처 활성화 키들과 함께 디바이스들로 패스될 수도 있는 인가 파라미터들 (예를 들어, 인가된 선택적으로 활성화된 피처의 만료 날짜) 을 도출하는데 사용될 수도 있는, 인가 파라미터 도출 회로/기능부/모듈 (1116) 을 포함할 수도 있다. 프로세싱 회로 (1104) 는, 예를 들어 인가 합의에서의 데이터에 기초하여 인가 인증서를 도출하고, 디바이스의 공용 키로 인가 인증서를 암호화할 수도 있는, 인가 인증서 도출 회로/기능부/모듈 (1118) 을 포함할 수도 있다. 프로세싱 회로 (1104) 는, 로컬 인가 서버 (1100) 에 커플링된 디바이스들로부터 피처 사용 데이터를 수집할 수도 있는, 피처 사용 보고 회로/기능부/모듈 (1138) 을 포함할 수도 있다. 당업자에 의해 인지되는 바와 같이, 다른 회로들/기능부들/모듈들이 로컬 인가 서버 (1100) 의 프로세싱 회로 (1104) 에 포함될 수도 있다.

[0163] 메모리 회로 (1106) 는 인가 합의 관리 명령들 (1120), 피처 활성화 키 도출 명령들 (1122), 인가 파라미터 도출 명령들 (1124), 인가 인증서 도출 명령들 (1126), 뿐만 아니라 피처 활성화 키 스토리지 (1130), 인가 파라미터 스토리지 (1132), 인가 인증서 스토리지 (1134), 및 공용 키 스토리지 (1136) 를 위한 공간을 포함하도록 구성될 수도 있다. 메모리 회로 (1106) 는 또한, 피처 사용 보고 명령들 (1140) 을 포함하도록 구성될 수도 있다. 당업자에 의해 인지되는 바와 같이 데이터의 저장을 위한 다른 명령들 및 로케이션들이 메모리 회로 (1106) 에 포함될 수도 있다.

[0164] **피처 활성화의 예시적인 호 흐름도**

[0165] 도 12 는 본원에 설명된 양태들에 따른 인가 합의들의 동적 확인 및 시행에 관련된 호 흐름도 (1200) 이다. 도 12 는 디바이스 (1202)(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드), 로컬 인가 서버 (1204), 및 인가 서버 (1206) 간의 예시적인 상호작용들을 도시한다. 일 양태에서, 디바이스 (1202) 로의 및 디바이스로부터의 호 흐름은 디바이스 (1202) 의 인가 기능부로 및 인가 기능부로부터일 수도 있다.

[0166] 인가 서버 (1206) 는 벤더/OEM 또는 다른 엔티티로부터 디바이스 검증 정보를 획득 (1208) 할 수도 있다. 디바이스 검증 정보는, 예를 들어 디바이스 식별자, 디바이스 인증서, 디바이스 공용 키, 소프트웨어 버전 (예를 들어, 디바이스 (1202) 상에 상주하는 인가 기능부와 연관된 소프트웨어의 소프트웨어 버전) 및/또는 디바이스 능력들을 포함할 수도 있다. 디바이스 능력들은 디바이스 (1202) 에서 선택적으로 활성화된 피처들의 리스팅을 포함할 수도 있다. 인가 서버 (1206) 에서 디바이스 검증 정보를 획득하는 것은 진행 중인 프로세스일 수도 있다는 것이 이해될 것이다. 디바이스 검증 정보가 인가 서버 (1206) 에 추가되고, 수정되고, 또는 이로부터 제거될 수도 있는 때에 관하여 제한이 존재한다.

[0167] 2 개의 엔티티들 간에 인가 합의가 시작될 수도 있다. 인가 합의 (또는 그 복사본) 는 저장을 위해 로컬 인가 서버 (1204) 에서 획득 (1210) 될 수도 있고, 저장을 위해 인가 서버 (1206) 에서 획득 (1211) 될 수도 있고, 또는 저장을 위해 로컬 인가 서버 (1204) 및 인가 서버 (1206) 양자 모두에서 획득될 수도 있다. 일 예에서, 인가 합의는 로컬 인가 서버에서 실행하는 소프트웨어의 검증을 위한 프로비전 호출을 포함할 수도 있다.

[0168] 디바이스 (1202)(또는 디바이스 (1202) 의 인가 기능부) 는 로컬 인가 서버 (1204) 로, 피처 활성화 요청 (예를 들어, 하나 이상의 선택적으로 활성화된 피처들을 활성화시키기 위한 요청) 을 전송 (1212) 할 수도 있다. 피처 활성화 요청은 인증서 기반의 확인을 위한 인증서 서명 요청을 포함할 수도 있다.

[0169] 디바이스 (1202) 및 로컬 인가 서버 (1204) 는 원격 증명 (1214) 에 참여할 수도 있다. 원격 증명 (1214) 은, 제 2 엔티티가 (예를 들어, 알려진 정확한 상태에 기초하여) 정확하게 작동 중이라는 것을 확인하도록 제 1 엔티티에 의해 사용될 수도 있다. 예를 들어, 로컬 인가 서버 (1204) 는, 디바이스 (1202) 에서 실행되는 소프트웨어를 검증함으로써 디바이스 (1202) 가 정확하게 작동되고 있다는 것을 확인할 수도 있다. 일 예에서, 소프트웨어를 검증하는 것은, 로컬 인가 서버 (1204) 로 전송된 디바이스 검증 정보에서 식별된 소프트웨어가 디바이스 (1202) 에서 실행되는 소프트웨어에 일치하는지를 비교하는 것을 수반할 수도 있다. 원격 증명

(1214) 의 결과는 인가 서버 (1206) 로 전송될 수도 있다. 원격 증명 (1214) 의 결과는, 공격자가 디바이스 (1202) 를 손상시키지 않았다는 것 및 디바이스 (1202) 가 벤더/OEM 에 의해 설명된/식별된 소프트웨어를 실행하고 있다는 것을 인증 서버 (1206) 에 보증하는데 사용될 수도 있다. 원격 증명이 성공적이지 않으면, 피처 활성화 요청이 무시될 수도 있다.

[0170] 원격 증명 (1214) 이 성공적이면, 인가 합의 (예를 들어, 저장을 위한 로컬 인가 서버에서 획득된 인가 합의) 에 기초하여, 로컬 인가 서버 (1204) 는 디바이스에 대한 피처 활성화를 인가 서버 (1206) 로 요청 (예를 들어, 피처 활성화 요청 을 전송 (1216)) 할지 여부를 결정하고 또는 그 자신의 권한으로 디바이스에 대한 피처 활성화를 인가 (예를 들어, 인가 합의/인가 인증서/인가 파일(들)을 전송 (1222)) 할 수도 있다. 후자의 시나리오는, 예를 들어 로컬 인가 서버 (1204) 가 인가 합의에 기초하여 미리 인가 서버 (1206) 로부터 하나 이상의 인가 키들 (예를 들어, 피처 활성화 키들) 을 획득한 경우 발생할 수도 있다.

[0171] 로컬 인가 서버 (1204) 가 디바이스에 대한 피처 활성화를 인가 서버 (1206) 로 요청하도록 결정하면, 로컬 인가 서버 (1204) 는 인가 서버 (1206) 로, 피처 활성화 요청을 전송 (1216) (예를 들어, 포워딩) 할 수도 있고, 이 경우에서 로컬 인가 서버 (1204) 는 디바이스 (1202) 와 인가 서버 (1206) 간의 보안 터널을 제공하는 프록시 서버일 수도 있다. 피처 활성화 요청은 디바이스 검증 정보 (예를 들어, 디바이스 식별자, 디바이스 인증서, 디바이스 공용 키, 소프트웨어 버전, 및/또는 디바이스 능력들) 및 원격 증명 (1214) 결과들을 포함할 수도 있다. 인가 서버 (1206) 로 전송된 피처 활성화 요청 (1216) 은 또한, 인증서 서명 요청이 디바이스로부터 로컬 인가 서버로 전송된 피처 활성화 요청에 포함되었다면, 인증서 서명 요청을 포함할 수도 있다.

[0172] 일 양태에서, 로컬 인가 서버 (1204) 및 인가 서버 (1206) 는 원격 증명 (1218) 에 참여할 수도 있다. 예를 들어, 로컬 인가 서버 (1204) 는, 로컬 인가 서버 (1204) 가 정확한 소프트웨어를 실행하고 있다는 증거를 인가 서버 (1206) 로 전송할 수도 있다. 이 방식에서, 인가 서버 (1206) 는 로컬 인가 서버 (1204) 에 의해 인가 서버 (1206) 로 전송된 디바이스 (1202) 에 관한 정보를 신뢰할 수도 있다. 이러한 양태에 따르면, 인가 서버 (1206) 는 디바이스 (1202) 와 로컬 인가 서버 (1204) 간에 수행된 원격 증명의 결과를 수락할 수도 있다.
선택적으로 또는 대안으로, 인가 서버 (1206) 및 디바이스 (1202) 는 원격 증명 (1219) 에 참여할 수도 있다.

[0173] 일단 인가 서버 (1206) 가 (로컬 인가 서버 (1204) 및 디바이스 (1202) 중 어느 하나 또는 양자 모두와의) 원격 증명의 결과를 수락하고 (예를 들어, 확인이 성공적이고) 인가 서버 (1206) 가, 피처 활성화 요청이 인가 합의의 조항들을 준수한다는 것을 확인할 수 있으면, 인가 서버 (1206) 는 로컬 인가 서버 (1204) 로, 인가 합의, 인가 인증서, 또는 디바이스 (1202) 에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스 (1202) 의 인가 인증서 (예를 들어, 권한의 증거) 와 인가 합의 및 피처 활성화 키(들)을 포함하는 인가 파일을 전송 (1220) 할 수도 있다. 일 양태에서, 인가 서버 (1206) 는 네트워크 오퍼레이터 (예를 들어, MNO) (또는 제 3 엔티티) 와 디바이스 (1202) 의 인가 합의를 확인할 수도 있다. 인가 서버 (1206) 에 의해 전송된 권한의 증거는 인가 합의, 인가 인증서, 또는 인가 합의 및 인가 인증서 양자 모두를 포함할 수도 있다. 선택적으로, 인가 서버 (1206) 는 디바이스 (1202) 로, 인가 합의/인가 인증서/피처 활성화 키들을 포함하는 인가 파일(들)을 직접 전송 (1223) 할 수도 있다.

[0174] 로컬 인가 서버 (1204) 가 피처 활성화 요청을 인가 서버 (1206) 로 전송 (예를 들어, 디바이스에 대한 피처 활성화를 인가 서버 (1206) 에 요청) 하도록 결정했고 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거 및 피처 활성화 키(들)을 포함하는 인가 파일을 인가 서버 (1206) 로부터 획득했으면, 또는 (예를 들어, 로컬 인가 서버 (1204) 가 인가 합의에 기초하여, 미리 인가 서버 (1206) 로부터 하나 이상의 인가 키들을 획득한 경우에서) 그 자신의 권한으로 인가 파일 및 디바이스에 대한 권한의 증거를 전송하도록 결정했으면, 로컬 인가 서버는 디바이스 (1202) 로, 인가 합의/인가 인증서/인가 파일(들)을 전송 (1222) 할 수도 있다. 즉, 로컬 인가 서버 (1204) 는 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스의 권한의 증거 및 피처 활성화 키(들)(및, 이용 가능하다면 소프트웨어) 을 포함하는 인가 파일을 디바이스 (1202) 로 전송할 수도 있다.

[0175] 일단 디바이스 (1202) 가 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거 (예를 들어, 인가 합의, 인가 인증서, 또는 인가 합의 및 인가 인증서 양자 모두) 및 (예를 들어, 피처 활성화 요청에 응답하여) 피처 활성화 키(들)을 포함하는 인가 파일을 획득하면, 디바이스 (1202)(및/또는 디바이스의 인가 기능부) 는 권한의 증거를 검증 (예를 들어, 디바이스가 요청된 선택적으로 활성화된 피처(들)을 활성화 및 사용하도록 인가되는지 여부를 결정) 할 수도 있다. 디바이스 (및/또는 디바이스의 인가

기능부) 가, 요청된 선택적으로 활성화된 피처(들)을 사용하도록 디바이스가 인가된다고 결정하면, 디바이스 (및/또는 디바이스의 인가 기능부) 는 요청된 선택적으로 활성화된 피처들에 대한 피처 활성화 키(들) 을 취출하고 요청된 선택적으로 활성화된 피처(들)을 활성화 (1224) 시킬 수도 있다. 일부 구현들에서, 요청된 선택적으로 활성화된 피처(들)은 권한의 증거에 (예를 들어, 인가 인증서에) 지정된 만료 시간 또는 인가 파일에 지정된 만료 시간까지 활성화된 채로 있을 수도 있다.

[0176] 디바이스 (1202) 는 선택적으로 활성화된 피처들의 사용에 관한 주기적 레포트 (1226) 를 로컬 인가 서버 (1204) 로 전송할 수도 있다. 로컬 인가 서버 (1204) 는 복수의 디바이스들로부터 수신된 레포트들을 집성할 수도 있고, 선택적으로 활성화된 피처들의 사용에 관한 주기적 레포트 (1228) 를 인가 서버 (1206) 로 전송할 수도 있다. 당업자는, 다양한 시스템들이 다양한 유형들의 사용 보고 포맷들을 사용할 수도 있다는 것을 인지할 것이다. 본원에 설명된 양태들은 임의의 하나의 사용 보고 포맷에 제한되지 않는다.

[0177] 주기적 레포트들은, 활성화된 선택적으로 활성화된 피처들의 총 수가 적절한 인가 합의의 조항들을 충족시키는 한, 오퍼레이터가 복수의 디바이스들 (예를 들어, 칩 컴포넌트들, 클라이언트 디바이스들, 네트워크 노드들) 에서 선택적으로 활성화된 피처를 활성화시키는 것을 허용함으로써 로컬 인가 관리에 유연성을 제공할 수도 있다. 예를 들어, 주기적 보고는 오퍼레이터가 선택적으로 활성화된 피처들의 최대 허용 가능한 수를 동시에 활성화시키는 것을 허용할 수도 있다.

[0178] **사용을 위한 인가의 검증의 예시적인 시스템 레벨 호 흐름도들**

[0179] 네트워크 서비스를 사용하기 전에, 각각의 측 (예를 들어, 클라이언트 측 및 서빙 측; 클라이언트 디바이스 및 네트워크 노드) 은, 다른 측이 네트워크 서비스를 사용하기 위해 필요한, 및/또는 네트워크 서비스를 제공하기 위해 필요한 하나 이상의 선택적으로 활성화된 피처들을 활성화시키고 사용하도록 인가된다는 것을 검증할 수도 있다. 다시 말해, 상호 피처 확인의 액트가 발생할 수도 있다. 이 방식에서, 각각의 측은 하나 이상의 선택적으로 활성화된 피처들을 사용/제공하도록 디바이스들 (예를 들어, 칩 컴포넌트들, 클라이언트 디바이스들, 네트워크 노드들) 의 권리들을 통제할 수도 있는 인가 합의들의 조항들을 시행할 수도 있다. 따라서, 네트워크 서비스를 사용/제공하기 전에, 각각의 측은 네트워크 서비스를 제공/사용하는데 필요한 선택적으로 활성화된 피처들을 사용할 다른 측의 권리의 권한의 증거를 획득할 수도 있고, 그 권한의 증거를 검증할 수도 있다.

[0180] 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 에 대한 권한의 증거를 검증하기 위한 2 개의 예시적인 시스템 레벨 방법들이 이하에서 제공된다. 제 1 방법은 디바이스의 가입 프로파일에 기초한 검증에 대해 제공한다. 제 2 방법은 디바이스에 의해 전송된 인가 정보에 기초한 검증에 대해 제공한다. 예시적인 시스템 레벨 방법들은 배타적이지 않다.

[0181] 어느 하나의 예시적인 시스템 레벨 방법의 구현 전에, 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 단위 마다의 인가 정보는 디바이스에 의해 저장될 수도 있다. 부가적으로, 인가 정보, 또는 디바이스의 새로운 및/또는 업데이트된 선택적으로 활성화된 피처들을 반영하는 정보는 또한, 홈 가입자 서버 (HSS) 에 저장될 수도 있다. 예를 들어, 디바이스가 선택적으로 활성화된 피처를 활성화시키는 경우, 인가 서버 또는 로컬 인가 서버는 선택적으로 활성화된 피처의 활성화를 HSS 에 보고할 수도 있다. HSS 는, 디바이스의 인가된 새로운 및/또는 업데이트된 선택적으로 활성화된 피처들이 네트워크 오퍼레이터 (예를 들어, MNO) 에 의해 확인되는 경우 디바이스의 능력 프로파일을 업데이트할 수 있다. 디바이스의 능력 프로파일은 디바이스의 가입 프로파일과 연관될 수 있다. 능력 프로파일은, 디바이스가 사용하도록 인가되는 선택적으로 활성화된 피처들을 식별할 수도 있다. 일 예에서, HSS 에 저장된, 디바이스의 능력 프로파일은 디바이스에, 네트워크 노드에, 또는 디바이스 및 네트워크 노드에 이용 가능할 수도 있다.

[0182] 부가적으로, 일 양태에 따르면, 네트워크 노드 (예를 들어, eNB) 는 디바이스들 (예를 들어, 칩 컴포넌트들, 클라이언트 디바이스들) 에, 네트워크 노드에서 활성화된 (예를 들어, 인에이블된, 사용된) 선택적으로 활성화된 피처들의 세트를 알릴 수도 있다. 피처들의 세트는, 예를 들어 시스템 정보 블록 (SIB) 메시지들을 사용하여 또는 서비스 질의 프로토콜 (SQP) 과 같은 질의하는 프로토콜을 통해 알려질 수 있다.

[0183] 도 13 은 본원에 설명된 양태들에 따른, 디바이스의 가입 프로파일에 기초하여, 선택적으로 활성화된 피처들의 제 1 세트를 사용하도록 디바이스에 대한 권한의 증거를 검증하는 것과 연관되어 발생할 수도 있는 시스템 레벨 호 흐름을 예시하는 예시적인 호 흐름도 (1300) 이다. 디바이스 (1302)(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드), (예를 들어, 하나 이상의 eNB들 및/또는 액세스 포인트들을 포함하는) 무선 액세

스 네트워크 (RAN)(1304), 네트워크 노드 (1306)(예를 들어, MME), HSS (1308), 로컬 인가 서버 (1310), 및 인가 서버 (1312) 가 예시된다.

[0184] 일부 구현들에서, 인가 서버 (1312) 는 벤더/OEM 또는 다른 엔티티로부터 디바이스 검증 정보를 획득 (1314) 할 수도 있다. 디바이스 검증 정보는, 예를 들어 디바이스 식별자, 디바이스 인증서, 디바이스 공용 키, 소프트웨어 버전 (예를 들어, 디바이스 (1302) 상에 상주하는 인가 기능부와 연관된 소프트웨어의 소프트웨어 버전) 및/또는 디바이스 능력들을 포함할 수도 있다. 디바이스 능력들은 디바이스 (1302) 에서 선택적으로 활성화된 피처들의 리스팅을 포함할 수도 있다. 인가 서버 (1312) 에서 디바이스 검증 정보를 획득하는 것은 진행중인 프로세스일 수도 있다는 것이 이해될 것이다. 디바이스 검증 정보가 인가 서버 (1312) 에 추가되고, 수정되고, 또는 이로부터 제거될 수도 있는 때에 관한 제한은 없다.

[0185] 2 개의 엔티티들 간에 인가 합의가 시작될 수도 있다. 인가 합의는 저장을 위해 인가 서버 (1312) 에서 획득 (1315) 될 수도 있고, 인가 합의는 저장을 위해 로컨 인가 서버 (1310) 에서 획득 (1316) 될 수도 있고, 또는 인가 합의는 저장을 위해 로컬 인가 서버 (1310) 및 인가 서버 (1312) 양자 모두에서 획득될 수도 있다. 일 예에서, 인가 합의는 로컬 인가 서버에서 실행하는 소프트웨어의 검증을 위한 프로비전 호출을 포함할 수도 있다.

[0186] 피처 활성화 동안, 인가 서버 (1312) 는 모두 전술된 바와 같은 인가 인증서들, 인가 파일들, 및 피처 활성화 키들 모두를 도출할 수도 있다. 또한 피처 활성화 동안, 인가 서버 (1312) 는, 전술된 바와 같이, 로컬 인가 서버 (1310) 로, 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거 (예를 들어, 인가 합의, 인가 인증서, 또는 인가 합의 및 인가 인증서 형태의 인가 정보) 및 피처 활성화 키(들)을 포함할 수도 있는 인가 파일을 전송 (1318) 할 수도 있다. 대안이지만, 도면에서 과밀을 방지하도록 도면에 도시되지 않은, 인가 서버 (1312) 는, 모두 전술된 바와 같이, 권한의 증거를 디바이스 (1302) 로 전송할 수도 있다. 부가적으로 또는 대안으로, 피처 활성화 동안, 로컬 인가 서버 (1310) 는, 모두 전술된 바와 같이, 디바이스에서 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거 (예를 들어, 인가 합의, 인가 인증서, 또는 인가 합의 및 인가 인증서 형태의 인가 정보) 및 피처 활성화 키(들)을 포함할 수도 있는 인가 파일을 디바이스 (1302) 로 전송 (1320) 할 수도 있다. 일 양태에서, 로컬 인가 서버 (1310) 는 디바이스 (1302) 의 능력 프로파일 (1322) 을 HSS (1308) 로 전송할 수도 있다. 디바이스 (1302) 의 능력 프로파일은 디바이스 (1302) 에서 활성화되도록 인가된 선택적으로 활성화된 피처들을 나열할 수도 있다. 능력 프로파일은 선택적으로 활성화된 피처들과 연관된 파라미터들을 나열할 수도 있다. 디바이스의 능력 프로파일은 HSS (1308) 에 저장될 수 있는 디바이스 (1302) 의 대응하는 능력 프로파일로 업데이트하는데 사용될 수도 있다. 일 양태에서, 인가 서버 (1312) 는 디바이스 (1302) 의 능력 프로파일을 HSS (1308) 로 전송 (1324) 할 수도 있다.

[0187] HSS (1308) 을 참조하여, 디바이스 (1302) 의 능력 프로파일은 디바이스 (1302) 에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 리스트를 포함할 수도 있고, 디바이스 (1302) 의 가입 프로파일과 연관될 수도 있다. HSS (1308) 에 의해 획득된, 디바이스 (1302) 의 능력 프로파일은 HSS (1308) 로 하여금, 디바이스 (1302) 의 새로운 및/또는 업데이트된 선택적으로 활성화된 피처들의 인가 스테이터스를 학습하게 할 수 있다. 일 양태에서, HSS (1308) 는 네트워크 오퍼레이터 (예를 들어, MNO) 와 협의하여, HSS (1308) 가 HSS (1308) 에 저장된 디바이스 (1302) 의 대응하는 능력 프로파일을 업데이트해야 하는지를 결정할 수도 있다. 일 양태에서, 네트워크 오퍼레이터의 합의로 또는 합의 없이, HSS (1308) 는 HSS (1308) 에 저장된 디바이스 (1302) 의 능력 프로파일을 업데이트 (1325) 할 수도 있다. 따라서, HSS (1308) 는 로컬 인가 서버 (1310) 또는 인가 서버 (1312) 로부터 획득된 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 리스트에 기초하여 디바이스 (1302) 의 선택적으로 활성화된 피처들의 리스트를 업데이트 (1325) 할 수도 있다. 리스트를 업데이트하는 것은 디바이스 (1302) 에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 세트에서의 적어도 하나의 선택적으로 활성화된 피처의 인가 스테이터스에 대한 변화를 반영할 수도 있다.

[0188] 디바이스 (1302) 의 초기 어태치 절차 (1326) 시에, 네트워크 노드 (1306)(예를 들어, MME) 는 HSS (1308) 로부터 디바이스 (1302) 의 능력 프로파일을 획득 (1328) 할 수도 있다. 일 양태에서, 네트워크 노드 (1306)(예를 들어, MME) 는 요청을 HSS (1308) 로 전송함으로써 HSS (1308) 로부터 디바이스 (1302) 의 능력 프로파일을 획득 (1328) 할 수도 있다.

[0189] 일 예에서, 능력 프로파일은 디바이스 (1302) 의 보안/인증된 부트 프로세스 동안 획득된 무결성 정보 (예를 들어, 디바이스 (1302) 의 인가 기능부의 소프트웨어 무결성 정보) 를 포함할 수도 있다. 예로서, 무결성 프

로파일이 보안/인증 부트 프로세스 동안 (예를 들어, 인증 및 키 합의 (AKA) 절차 동안) 획득되는 경우에서, 네트워크 노드 (1306)(예를 들어, MME) 는 디바이스 (1302) 에서 실행되는 소프트웨어의 무결성을 입증하는 무결성 정보를 전송하도록 디바이스 (1302) 에 요청할 수도 있다. 디바이스 (1302) 의 무결성 정보는, 디바이스 (1302) 가 적합한 포스트웨어를 실행하고 있다 (즉, 디바이스가 인가된 소프트웨어를 실행하고 있다) 는 증거로서 디바이스 (11302) 에 의해 전송될 수도 있다. 일 양태에서, 네트워크 노드 (1306)(예를 들어, MME) 는 디바이스 (1302) 와의 상호 인증 (1330)(예를 들어, 원격 증명) 동안 무결성 정보에 대한 요청을 할 수도 있다.

무결성 정보는 상호 인증 (1330) 동안 사용될 수도 있다. 선행기술은 예시적인 것이 주목되고; 무결성 정보를 전송하기 위한 요청은 AKA 절차 동안 또는 별개의 절차로서 발생할 수도 있다.

[0190] 네트워크 노드 (1306)(예를 들어, MME) 는 HSS (1308) 으로부터 획득된 디바이스 (1302) 의 능력 프로파일에 기초하여 디바이스 콘텍스트 (예를 들어, 특정 신호 무선 베어러 또는 디폴트 무선 베어러 또는 데이터 흐름을 식별할 수도 있는 UE 콘텍스트) 를 구성 (1332) 할 수도 있다. 네트워크 노드 (1306)(예를 들어, MME) 는 RAN (1304)(예를 들어, RAN 의 eNB들) 과 디바이스 콘텍스트를 구성 (1332) 할 수도 있고, 디바이스 콘텍스트 및/또는 능력 프로파일을 RAN (1304) 으로 전송할 수도 있다. 이것은, RAN (1304) 이 선택적으로 활성화된 피처들을 활성화/비활성화시키는 것을 허용할 수 있고, 이에 의해 디바이스 (1302) 에 제공된 네트워크 서비스를 인에이블 (또는 디스에이블) 할 수 있다. 디바이스 (1302) 에 대한 네트워크 서비스의 인에이블먼트/디스에이블먼트는 디바이스 (1302) 의 능력 프로파일에 따라 디바이스 콘텍스트를 업데이트/설정함으로써 달성될 수도 있다. 비-액세스 계층 (NAS) 및 무선 리소스 제어 (RRC) 절차들은 이 목적을 위해 사용될 수도 있다.

[0191] S1 핸드오버 동안, 디바이스 콘텍스트 (예를 들어, UE 콘텍스트) 는, MME 리로케이션이 수행되면 타겟 MME 로 트랜스퍼될 수도 있다는 것이 주목될 수도 있다. X2 핸드오버 동안, 소스 네트워크 액세스 노드 (예를 들어, 소스 eNB) 는 디바이스 능력을 지정하는 디바이스 콘텍스트 (예를 들어, UE 콘텍스트) 를 타겟 네트워크 액세스 노드 (예를 들어, 타겟 eNB) 로 전송할 수도 있다.

[0192] 디바이스 (1302) 의 능력 프로파일이, 소정의 선택적으로 활성화된 피처들이 (예를 들어, 만료로 인해) 비활성화될 필요가 있다는 것을 나타내면, 네트워크 노드 (1306)(예를 들어, MME) 는 선택적으로 활성화된 피처들을 비활성화할 수도 있고 대응하는 구성을 (RAN (1304) 내의) 네트워크 액세스 노드 (예를 들어, eNB) 에 적용할 수도 있다. 대응하는 구성은, 예를 들어 디바이스 콘텍스트 수정 절차 (예를 들어, UE 콘텍스트 수정 절차) 를 사용하여 네트워크 액세스 노드에 적용될 수도 있다. 디바이스 (1302) 는 (인가 서버에 저장된) 인가 합의를 갱신함으로써 임의의 비활성화된 선택적으로 활성화된 피처를 재활성화시킬 수도 있고, 그 후 전술된 바와 같은 피처 활성화를 수행 (예를 들어, 피처 활성화 요청을 전송) 한다.

[0193] 제 1 예시적인 시스템 레벨 방법은, HSS (1308) 에서, 디바이스 (1302) 의 가입 프로파일과 연관된, 디바이스 (1302) 의 능력 프로파일에 저장된 인가 정보를 사용할 수도 있다. HSS (1308) 는 디바이스 (1302) 에서, 활성화되는, 또는 활성화되도록 인가되는 하나 이상의 선택적으로 활성화된 피처들을 식별하도록 질의-응답 유형 프로토콜에서 사용될 수도 있는 (액세스 네트워크 질의 프로토콜 (ANQP) 에서의 정보 엘리먼트와 유사한) 정보의 엘리먼트를 구현할 수도 있다. 정보의 엘리먼트는 디바이스 (1302)(예를 들어, 클라이언트 디바이스, 네트워크 액세스 노드 등) 상에서 이용 가능한 피처들이 무엇인지 (예를 들어, 선택적으로 활성화된 피처들이 무엇인지) 에 관한 질의들에 대한 응답들을 용이하게 하는데 사용될 수도 있다. 정보의 엘리먼트는, 서비스 질의 프로토콜 (SQP) 로서 본원에서 지칭될 수도 있는, 강화된 ANQP 프로토콜과 연관된 파라미터로서 생각될 수도 있다.

[0194] 예로서, 디바이스 (1302)(예를 들어, 클라이언트 디바이스) 는 디바이스 (1302) 가 인터넷을 사용하지만, 보이스-오버 IP 는 사용하지 않는 것을 허용하는 가입을 가질 수도 있다. 가입 정보는 HSS (1308) 에서 디바이스 (1302) 의 가입 프로파일에 저장될 수도 있다. 디바이스의 능력 프로파일이 또한, HSS (1308) 에 저장될 수도 있다. 능력 프로파일은 가입 프로파일과 연관될 수도 있다. 능력 프로파일 및 가입 정보에 관련한 정보의 엘리먼트들은 초기 어태치 절차 (1326) 동안 네트워크 노드 (1306)(예를 들어, MME) 로 전송될 수도 있다. 초기 어태치 절차 (1326) 는 드물게 발생할 수도 있다는 것이 주목된다.

[0195] 이 예에서, 설명된 정보의 엘리먼트를 수신하는 네트워크 노드 (1306)(예를 들어, MME) 는, 디바이스 (1302) 가 (예를 들어, 제 1 데이터 서비스로서) 인터넷을 사용할 수 있지만, (예를 들어, 제 2 데이터 서비스로서) 보이스 오버 IP 를 사용하지 않도록 네트워크를 구성할 수도 있다. 디바이스 (1302) 의 가입 프로파일과 연관된, 디바이스 (1302) 의 능력 프로파일에 저장된 인가 정보를 사용할 수 있는 제 1 예시적인 방법은 따라서, 능력 프로파일 엘리먼트를 사용할 수도 있다. 능력 프로파일 엘리먼트는 네트워크 서비스를 인에이

블하는데 필요한 하나 이상의 선택적으로 활성화된 피처들을 사용하도록 디바이스 (1302) 의 인가를 검증 및 시행하는데 사용될 수 있다. 인가는 궁극적으로, 인가 서버 (1312) 에서 획득된 인가 합의 (또는 일부 양태들에서, 로컬 인가 서버 (1310) 에서 획득된 인가 합의) 에 기초할 수도 있다.

[0196] HSS (1308) 에서 저장된 디바이스 (1302) 의 능력 프로파일로부터의 정보는 네트워크 노드 (1306)(예를 들어, MME) 에 의해 사용되어 다양한 네트워크 기능들을 구성할 수도 있다. 다양한 네트워크 기능들은 디바이스 (1302) 로 하여금, 디바이스 (1302) 에서 활성화될 수도 있는 (또는 활성화되도록 인가될 수도 있는) 하나 이상의 선택적으로 활성화된 피처들을 사용하게 할 수 있다.

[0197] 도 14 는 본원에 설명된 양태들에 따라 디바이스 (1402) 에 저장된 인가 인증서에서 식별된 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위해 디바이스 (1402)(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 에 대한 권한의 증거를 검증하는 것과 연관될 수도 있는 다른 시스템 레벨 호 흐름을 예시하는 예시적인 호 흐름도 (1400) 이다. 디바이스 (1402)(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드), 무선 액세스 네트워크 (RAN)(1404) (예를 들어, 하나 이상의 eNB들 및/또는 액세스 포인트들), 및 (MME 로서 도 14 에 예시된) 네트워크 노드 (1406) 가 예시된다. MME 로서 예시된 네트워크 노드 (1406) 와 디바이스 (1402) 간에 발생하는, 이하에서 설명되는 교환들은 임의의 디바이스 (1402) 와 네트워크 노드 (예를 들어, 네트워크 액세스 노드, eNB, MME, S-GW, P-GW) 간에 수행될 수도 있다. 디바이스 콘텍스트를 구성 (1426) 하는 동작은 MME 와 같은 네트워크 노드 (1406) 에 대해 적용 가능할 수도 있지만, 디바이스 콘텍스트를 구성 (1426) 하는 동작은 eNB 와 같은 네트워크 노드들의 다른 예들에 대해 적용 가능하지 않을 수도 있다는 것이 주목된다. 따라서, 디바이스 콘텍스트 (1426) 및 (디바이스 콘텍스트를 구성 (1426) 하는 동작의 수신인일 수 있는) RAN (1404) 을 구성하는 동작은 도 14 의 예에 대해 적용 가능하기 때문에 파선 형태로 도시되고, 여기서 네트워크 노드 (1406) 는 MME 로서 예시되지만, (예를 들어, 네트워크 노드 (1406) 가 MME 외의 노드인 경우) 다른 예들에 대해 적용 가능하지 않을 수도 있다.

[0198] 전술된 바와 같이, 예를 들어 피처 활성화 동안, 디바이스 (1402)(예를 들어, 클라이언트 디바이스) 는 디바이스 (1402) 에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스 (1402) 에 대한 권한의 증거 (예를 들어, 제 1 인가 서버에 의해 서명된, 인가 인증서의 형태일 수도 있는 제 1 인가 정보) 및 피처 활성화 키들을 포함하는 인가 파일을 획득 (1408) 할 수도 있다. 네트워크 노드 (1406)(예를 들어, MME) 는 네트워크 서비스를 사용하기 위한 디바이스 (1402) 의 권한을 검증하도록 제 1 인가 정보 (예를 들어, 인가 인증서) 를 사용할 수도 있다. 유사하게, 네트워크 노드 (1406)(예를 들어, MME) 는 네트워크 노드 (1406) 에서 선택적으로 활성화된 피처들의 제 2 세트를 사용하기 위한 네트워크 노드 (1406) 에 대한 권한의 증거 (예를 들어, 제 2 인가 서버에 의해 서명된, 인가 인증서의 형태일 수도 있는 제 2 인가 정보) 를 획득 (1410) 할 수도 있다. 디바이스 (1402)(예를 들어, 클라이언트 디바이스) 는 네트워크 서비스를 제공하기 위한 네트워크 노드 (1406) 의 권한을 검증하도록 제 2 인가 정보 (예를 들어, 인가 인증서) 를 사용할 수도 있다.

[0199] 제 1 인가 정보 (예를 들어, 인가 인증서) 는 디바이스 (1402) 에 인가된 선택적으로 활성화된 피처들을 식별할 수도 있고, 제 1 인가 서버의 사설 키를 사용하여 제 1 인가 서버에 의해 서명될 수도 있다. 제 1 인가 정보 (예를 들어, 인가 인증서) 는 또한, 디바이스 (1402) 의 아이덴티티를 포함할 수도 있고, 또한 인가 인증서의 만료 시간을 포함할 수도 있다. 인가 파일은 피처 활성화 키들 및 연관된 파라미터들을 포함할 수도 있고, 디바이스 (1402) 의 공용 키로 암호화될 수도 있다. 일부 구현들에서, 디바이스 (1402) 는 피처 활성화 동안 제 1 인가 정보 (예를 들어, 인가 인증서) 및 인가 파일을 획득한다.

[0200] 제 1 인가 정보 (예를 들어, 인가 인증서) 는, 제 1 인가 서버에 의해 서명된 디바이스 (1402) 의 공용 키 및 디바이스 식별자를 포함하는 대응하는 아이덴티티 인증서로 사용될 수도 있다. 아이덴티티 인증서는 디바이스 (1402) 로부터 하나 이상의 선택적으로 활성화된 피처들의 비활성화 시에도 여전히 유효한 채로 있을 수도 있다. 일 양태에서, 디바이스 식별자는, 예를 들어 디바이스 시리얼 넘버 또는 국제 이동국 장비 아이덴티티 (IMEI) 일 수도 있다. 본원의 구현들에서, 디바이스 식별자는, 디바이스 (1402) 가 디바이스 식별자의 그 자신의 소유권을 입증할 수 있도록 디바이스 공용 키와 항상 연관될 수도 있다.

[0201] 일 양태에서, 디바이스 (1402) 의 공용 키 (또는 공용 키의 해시) 는 디바이스 식별자로서 사용될 수도 있다. 이 경우에서, 아이덴티티 인증서는 불필요할 수도 있지만, 디바이스 (1402) 의 아이덴티티는 제 1 인가 서버 및/또는 로컬 인가 서버 및/또는 제 3 엔티티를 통해 확인될 수 있어야 한다.

[0202] 제 1 인가 정보 (예를 들어, 인가 인증서) 는 로컬 인가 서버로부터 디바이스 (1402) 에 의해 획득될 수도 있다. 이 경우에서, 디바이스 (1402) 는 예를 들어 피처 활성화 동안, 로컬 인가 서버의 인증서를 획득할

수도 있다.

[0203] 디바이스 (1402) 는 네트워크 노드 (1406) 로 어태치 요청 (1412) 을 전송할 수도 있다. 일 양태에서, 어태치 요청은 네트워크 서비스를 사용하기 위한 요청인 것으로, 또는 이 요청을 포함하는 것으로 이해될 수도 있다. 응답하여, 네트워크 노드 (1406)(예를 들어, MME) 는 디바이스 (1402) 에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스 (1402) 에 대한 권한의 증거에 대한 요청 (1414) 을 디바이스 (1402) 로 전송할 수도 있고, 여기서 선택적으로 활성화된 피처들의 제 1 세트는 네트워크 서비스를 사용하기 위해 디바이스 (1402) 에 의해 필요한 제 1 선택적으로 활성화된 피처들을 포함한다. 다시 말해, 네트워크 노드 (1406)(예를 들어, MME) 는 디바이스에 대한 권한의 증거 (예를 들어, 인가 인증서의 형태일 수도 있는 제 1 인가 정보) 에 대한 요청 (1414) 을 디바이스 (1402) 로 전송할 수도 있다. 일 양태에서, 이러한 요청 (1414) 은 인증 및 키 합의 (AKA) 절차 동안 전송될 수도 있다. 디바이스 (1402) 는, 요청 (1414) 에 응답하여 디바이스 (1402) 에 대한 권한의 증거를 네트워크 노드 (1406) 로 전송 (1416) 할 수도 있다.

[0204] 상호 인증 (1418) 이 디바이스 (1402) 와 네트워크 노드 (1406) 간에 발생할 수도 있다. 상호 인증 (1418) 은 선택적일 수 있다. 상호 인증 (1418) 은, 디바이스 (1402) 및 네트워크 노드 (1406) 가 보안 채널을 확립함으로써 정확한 엔티티와 통신하고 있다는 확신을 제공하도록 구현될 수도 있다. 디바이스 (1402) 와의 상호 인증 (1418)(예를 들어, 원격 증명) 은 네트워크에 등록하기 위해 디바이스 (1402) 에 대해 사용되는 AKA 절차와 상이하다는 것이 주목된다.

[0205] 부가적으로, 일부 예들에서, 상호 인증 (1418) 은, 네트워크 노드 (1406) 가 디바이스 (1402) 에 대한 권한의 증거에 대한 요청 (1414) 을 디바이스 (1402) 로 전송하기 전에 구현될 수도 있다는 것이 주목된다. 예를 들어, 네트워크 노드 (1406) 가 (도 14 에 예시된 바와 같이) MME 인 경우, 일단 AKA 절차가 완료되면, 디바이스 (1402) 및 MME 는 보안 전송 (즉, NAS 메시지들) 을 통해 서로와 통신할 수 있다. 결과적으로, 디바이스 (1402) 및 MME 는 서로 인증할 수도 있다.

[0206] 일 양태에서, 네트워크 노드 (1406)(예를 들어, MME) 는 디바이스 (1402) 의 보안/인증된 부트 프로세스 동안 생성된 무결성 정보 (예를 들어, 디바이스 (1402) 의 인가 기능부의 소프트웨어 무결성 정보) 를 전송하도록 디바이스 (1402) 에 요청할 수도 있다. 예로서, 무결성 정보가 보안/인증된 부트 프로세스 동안 획득되는 경우에서, 무결성 정보는 디바이스 (1402) 에서 실행되는 소프트웨어의 무결성을 입증하는데 사용될 수도 있다. 일 양태에서, 네트워크 노드 (1406)(예를 들어, MME) 는 디바이스 (1402) 와의 상호 인증 (1418)(예를 들어, 원격 증명) 동안 무결성 정보에 대한 요청을 할 수도 있다. 무결성 정보는 상호 인증 동안 사용될 수도 있다.

[0207] 네트워크 노드 (1406)(예를 들어, MME) 는 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트 (예를 들어, 제 1 인가 정보) 를 사용하기 위한 디바이스 (1402) 에 대한 권한의 증거를 검증 (1420) 할 수도 있다. 인가 서버 공용 키를 사용하여 (또는 로컬 인가 서버가 디바이스 (1402) 에 대한 권한의 증거를 생성한 경우 로컬 인가 서버의 공용 키를 사용하여) 디바이스 (1402) 에 대한 권한의 증거 (예를 들어, 제 1 인가 정보) 를 검증함으로써 검증이 수행될 수도 있다. 또한, 일 양태에서, 네트워크 노드 (1406) 는, 디바이스 (1402) 에 대한 권한의 증거 (예를 들어, 제 1 인가 정보) 를 전송했던 디바이스 (1402) 가 디바이스 (1402) 에 대한 권한의 증거 (예를 들어, 제 1 인가 정보) 에 포함된 디바이스 (1402) 의 공용 키에 대응하는 사설 키를 홀딩한다는 것을 확인 (1422) 할 수도 있다. 예를 들어, 디바이스 (1402) 에 대한 권한의 증거 (예를 들어, 제 1 인가 정보) 에 포함된 디바이스 (1402) 의 공용 키를 사용하여 디바이스 (1402) 에 대한 권한의 증거 (예를 들어, 제 1 인가 정보) 와 함께 전송될 수도 있는 디바이스 (1402) 의 서명을 검증함으로써, 확인이 수행될 수도 있다.

[0208] 도 14 의 예시적인 예시에서와 같이, 네트워크 노드가 MME 이면, 그 후 검증 (1420) 및 확인 (1422) 양자 모두가 성공적이면, 네트워크 노드 (1406)(예를 들어, MME) 는 RAN (1404) 에서 네트워크 서비스의 사용을 구현하도록 디바이스 콘텍스트를 구성 (1426) 하는 동작을 구현할 수도 있다. 일 예에서, 네트워크 노드 (1406) 는, 네트워크 노드가 예를 들어, MME 인 경우, 디바이스 (1402) 가 인가된 선택적으로 활성화된 피처들을 사용할 수 있도록 RAN (1404) 을 구성할 수도 있다. 다른 예에서, 네트워크 노드 (1406) 는, 네트워크 노드가 예를 들어, MME 인 경우, 디바이스 (1402) 가 인가된 선택적으로 활성화된 피처들 만을 사용할 수 있도록 RAN (1404) 을 구성할 수도 있다.

[0209] 그러나, 위에서 주목된 바와 같이, 네트워크 노드가 eNB 였다면, 디바이스 콘텍스트를 구성 (1426) 하는 동작은 적용 가능하지 않을 수도 있다. 따라서, 디바이스 콘텍스트를 구성 (1426) 하는 동작 및 RAN (1404) 은 파선 형태로 도시된다.

[0210] 일부 양태들에 따르면, 검증 (1420) 및 확인 (1422) 양자 모두가 성공적이면, 네트워크 노드 (1406) 는, 네트워크 서비스를 획득하기 위해 디바이스 (1402) 에 의해 사용될 필요가 있는 선택적으로 활성화된 피처들이 제 1 인가 정보에 따라 디바이스 (1402) 에서 활성화된 선택적으로 활성화된 피처들에 일치한다는 것을 확인할 수도 있다. 다시 말해, 선택적으로 활성화된 피처들에 필요한 활성화를 확인 (1423) 하는 선택적 동작이 발생할 수도 있다. 일 양태에서, 선택적으로 활성화된 피처들에 필요한 활성화를 확인 (1423) 하는 것은 네트워크 서비스를 사용하기 위해 디바이스 (1402) 에 의해 필요한 선택적으로 활성화된 피처들의 필요한 세트를 식별하는 것, 및 선택적으로 활성화된 피처들의 필요한 세트가 선택적으로 활성화된 피처들의 제 1 세트에 포함되는지 여부를 결정하는 것에 기초하여 요청에 대한 응답 (1424) 을 전송하는 것을 수반할 수도 있고, 여기서 선택적으로 활성화된 피처들의 제 1 세트는 디바이스에 대한 권한의 증거 (예를 들어, 제 1 인가 정보) 에서 식별된 선택적으로 활성화된 피처들의 세트이다.

[0211] 일 양태에서, 선택적으로 활성화된 피처들의 필요한 세트를 식별하는 것은 제 1 인가 서버에 의해 유지된, 인가된 선택적으로 활성화된 피처들의 모델-특정 및/또는 디바이스-특정 리스트로부터 네트워크 서비스를 사용하기 위해 디바이스 (1402) 에 의해 필요한 선택적으로 활성화된 피처들을 도출하는 것을 포함할 수도 있다. 다른 양태에서, 선택적으로 활성화된 피처들의 필요한 세트를 식별하는 것은 제 1 인가 서버에 의해 유지된 라이선싱 가능한 선택적으로 활성화된 피처들의 모델-특정 및/또는 디바이스-특정 리스트로부터 네트워크 서비스를 사용하기 위해 디바이스 (1402) 에 의해 필요한 선택적으로 활성화된 피처들을 도출하는 것을 포함할 수도 있다.

[0212] 일 양태에서, 네트워크 노드 (1406) 는 어태치 요청의 허가를 나타내는 응답 (1424) 을 전송할 수도 있다.

[0213] 본원에 설명된 양태들은 네트워크 노드 (1406) 가 네트워크 서비스를 사용하기 위한 디바이스 (1402) 의 권리를 검증하는 것을 허용한다; 그러나 이들은 또한, 디바이스 (1402) 가 네트워크 서비스를 제공하기 위한 네트워크 노드 (1406) 의 권리를 검증하는 것을 허용한다. 일부 네트워크 노드들은 피처들 (예를 들어, 선택적으로 활성화된 피처들) 의 이용 가능성을 디바이스 (1402) 에 허위로 광고할 수도 있다. 실제로, 소정 피처는 네트워크 노드가 반대로 광고하더라도 활성화되지 않을 수도 있다. 네트워크가 광고된 피처 또는 서비스를 디바이스 (1402) 에 제공하지 않으면, 네트워크는 예를 들어 열악한 서비스를 사용함으로써 디바이스 (1402) 를 더 많이 차징할 수도 있다. 따라서, 디바이스 (1402) 는, 피처를 광고하는 네트워크 노드가 그 피처를 제공하도록 인가된다는 것을 확인하는데 관심을 갖는다. 일단 디바이스 (1402) 가, 네트워크가 피처를 제공하도록 인가된다는 것을 확인하고, 이에 의해 피처가 네트워크에서 이용 가능하다는 것을 확인하면, 디바이스 (1402) 는 네트워크에 커플링되고 네트워크 서비스를 사용할 수도 있다.

[0214] 따라서, 디바이스 (1402) 는 네트워크 서비스를 제공하기 위해 네트워크 노드에 대한 권한의 증거에 대한 요청을 전송 (1428) 할 수도 있다. 응답하여, 네트워크 노드 (1406) 는, 제 2 인가 서버에 의해 서명된 네트워크 노드에서 선택적으로 활성화된 피처들의 제 2 세트 (예를 들어, 제 2 인가 정보) 를 사용하기 위한 네트워크 노드에 대한 권한의 증거를 전송 (1430) 할 수도 있고, 여기서 선택적으로 활성화된 피처들의 제 2 세트는 네트워크 서비스를 제공하기 위해 네트워크 노드에 의해 필요한 제 2 선택적으로 활성화된 피처들을 포함한다. 디바이스 (1402) 는 네트워크 노드 (1406) 에 의해 디바이스 (1402) 로 전송된 제 2 인가 정보 (예를 들어, 제 2 인가 인증서) 를 검증 (1432) 할 수도 있다. 제 2 인가 서버 공용 키를 사용하여 (또는 제 2 로컬 인가 서버가 네트워크 노드 (1406) 에 대한 권한의 증거를 생성한 경우 제 2 로컬 인가 서버의 공용 키를 사용하여) 검증이 수행될 수도 있다.

[0215] 또한, 일 양태에서, 디바이스 (1402) 는, 네트워크 노드 (1406) 에 대한 권한의 증거 (예를 들어, 제 2 인가 정보) 를 전송했던 네트워크 노드 (1406) 가 네트워크 노드 (1406) 에 대한 권한의 증거 (예를 들어, 제 2 인가 정보) 에 포함된 네트워크 노드 (1406) 의 공용 키에 대응하는 사설 키를 홀딩한다는 것을 확인 (1434) 할 수도 있다. 예를 들어, 네트워크 노드 (1406) 에 대한 권한의 증거 (예를 들어, 제 2 인가 정보) 에 포함된 네트워크 노드 (1406) 의 공용 키를 사용하여 네트워크 노드 (1406) 에 대한 권한의 증거 (예를 들어, 제 2 인가 정보) 와 함께 전송될 수도 있는 네트워크 노드 (1406) 의 서명을 검증함으로써, 확인이 수행될 수도 있다.

[0216] 일부 양태들에 따르면, 검증 (1432) 및 확인 (1434) 양자 모두가 성공적이면, 디바이스 (1402) 는, 네트워크 서비스를 제공하기 위해 네트워크 노드 (1406) 에 의해 사용될 필요가 있는 선택적으로 활성화된 피처들이 제 2 인가 정보에 따라 네트워크 노드 (1406) 에서 활성화된 선택적으로 활성화된 피처들에 일치한다는 것을 확인할 수도 있다. 다시 말해, 네트워크 노드가 네트워크 서비스를 제공하도록 인가된다는 것을 확인 (1436) 하는 선택적 동작이 발생할 수도 있다. 일 양태에서, 네트워크 노드가 네트워크 서비스를 제공하도록 인가된다는

것을 확인 (1436) 하는 것은 네트워크 서비스를 사용하기 위해 네트워크 노드 (1406) 에 의해 필요한 선택적으로 활성화된 피처들의 제 3 세트를 식별하는 것, 및 선택적으로 활성화된 피처들의 제 3 세트가 선택적으로 활성화된 피처들의 제 2 세트에 포함되는지 여부를 결정하는 것에 기초하여 네트워크 서비스를 사용하는 것을 수반할 수도 있고, 여기서 선택적으로 활성화된 피처들의 제 2 세트는 네트워크 노드 (1406) 에 대한 권한의 증거 (예를 들어, 제 2 인가 정보) 에서 식별된다. 일 양태에서, 검증 (1432), 확인 (1434), 및 네트워크 노드가 네트워크 서비스를 제공하도록 인가된다는 것을 확인 (1436) 하는 것이 성공적이면, 디바이스 (1402) 는 네트워크 노드 (1406) 에 의해 제공된 네트워크 서비스를 사용할 수도 있다.

[0217] **예시적인 디바이스**

[0218] 도 15 는 인가 합의들의 동적 확인 및 시행을 지원하도록 구성된 예시적이 디바이스 (1500)(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 를 예시하는 블록도이고, 여기서 시행은 본원에 설명된 양태들에 따라, 인가 합의들의 조항들에 따른 선택적으로 활성화된 피처들의 활성화/비활성화 및 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거의 동적 검증을 포함한다. 일 예에서, 예시적인 디바이스 (1500) 는 네트워크 통신 회로 (1502), 프로세싱 회로 (1504), 및 (메모리 회로 (1506) 로서 본원에 지칭된) 메모리 회로/저장 디바이스를 포함할 수도 있다. 네트워크 통신 회로 (1502), 프로세싱 회로 (1504), 및 메모리 회로 (1506) 는 데이터 및 명령들의 교환을 위해 통신 버스 (1508) 에 커플링될 수도 있다.

[0219] 네트워크 통신 회로 (1502) 는 사용자와의 입/출력 동작들을 위해 제 1 입/출력 회로/기능부/모듈 (1510) 을 포함할 수도 있다. 네트워크 통신 회로 (1502) 는 무선 통신을 위한 제 2 입/출력 회로/기능부/모듈 (1511) (예를 들어, 수신기/송신기 모듈/회로/기능부) 을 포함할 수도 있다. 당업자에 의해 인지되는 바와 같이, 다른 회로들/기능부들/모듈들이 네트워크 통신 회로 (1502) 에 포함될 수도 있다.

[0220] 프로세싱 회로 (1504) 는 인가 합의들의 동적 확인 및 시행을 지원하도록 구성되는 하나 이상의 프로세서들, 애플리케이션 특정 프로세서들, 하드웨어 및/또는 소프트웨어 모듈들 등을 포함 또는 이들을 구현하도록 구성될 수도 있고, 여기서 시행은 인가 합의들의 조항들에 따라 선택적으로 활성화된 피처들의 활성화/비활성화 및 선택적으로 활성화된 피처들의 세트를 사용하기 위한 디바이스에 대한 권한의 증거의 동적 검증을 포함한다. 프로세싱 회로 (1504) 는 인가 기능부 회로/기능부 모듈 (1512), 인가 인증서 확인 회로/기능부 모듈 (1514), 인가 파라미터 평가 회로/기능부 모듈 (1516), 및 피처 활성화 키 추출 회로/기능부 모듈 (1518) 을 포함하도록 구성될 수도 있다. 당업자에 의해 인지되는 바와 같이, 다른 회로들/기능부들/모듈들이 프로세싱 회로 (1504) 에 포함될 수도 있다.

[0221] 메모리 회로 (1506) 는 인가 명령들 (1520), 인가 인증서 확인 명령들 (1522), 인가 파라미터 평가 명령들 (1524), 및 피처 활성화 키 추출 명령들 (1526) 을 포함하도록 구성될 수도 있다. 메모리 회로 (1506) 의 별개의 부분이 보안 스토리지를 지원하도록 구성될 수도 있다. 따라서, 메모리 회로 (1506) 는 보안 저장 회로 (1528) 를 더 포함할 수도 있다. 보안 스토리지 회로 (1528) 는 사설 키 스토리지 (1530) 를 포함할 수도 있다. 사설 키 스토리지 (1530) 는 공용/사설 키 쌍의 사설 키를 저장할 수도 있고, 여기서 인가 서버 또는 로컬 인가 서버는 공용/사설 키 쌍의 공용 키를 사용하여 인가 인증서를 암호화한다. 보안 저장 회로 (1528) 는 피처 활성화 키 스토리지 (1532) 를 더 포함할 수도 있다. 메모리 회로 (1506) 는 또한, 디바이스의 선택적으로 활성화된 피처들 각각에 대한 인가 파라미터들 (1536) 의 리스팅 뿐만 아니라, 선택적으로 활성화된 피처들 (1534) 의 리스팅을 저장할 수도 있다. 당업자에 의해 인지되는 바와 같이 데이터의 저장을 위한 다른 명령들 및 로케이션들이 메모리 회로 (1506) 에 포함될 수도 있다.

[0222] **인가 합의들의 확인 시행의 예시적인 방법들**

[0223] 도 16 은 본원에 설명된 양태들에 따른 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 에서 동작하는 예시적인 방법 (1600) 의 플로우차트이다. 일 양태에서, 디바이스는 도 15 의 예시적인 디바이스 (1500) 및/또는 도 3 의 디바이스 (302) 와 유사할 수도 있다. 예시적인 방법 (1600) 을 구현하기 전에, 디바이스는 네트워크 서비스의 사용과 연관된 하나 이상의 선택적으로 활성화된 피처들의 결정된 세트를 가질 수도 있다. 예시적인 방법 (1600) 을 구현하기 전에, 디바이스는 피처 활성화 요청 (예를 들어, 하나 이상의 선택적으로 활성화된 피처들을 활성화시키기 위한 인가의 요청) 을 (인가 서버 또는 로컬 인가 서버로) 전송했을 수도 있다. 피처 활성화 요청, 또는 일부 다른 이벤트는, 인가 서버 (또는 로컬 인가 서버) 로 하여금 제 1 인가 서버에 의해 서명된, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 디바이스로 전송하게 할 수 있는 트리거 이벤트로서 작용할 수도 있다.

[0224] 디바이스는 제 1 인가 서버에 의해 서명된, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 획득 (1602) 할 수도 있다. 디바이스에 대한 권한의 증거는 인가 정보로서 본원에서 지칭될 수도 있다. 디바이스에 대한 권한의 증거는 인가 인증서를 포함할 수도 있다. 디바이스에 대한 권한의 증거는 인가 파일로 획득될 수도 있다. 인가 파일은 인가 파라미터들 및 하나 이상의 피처 활성화 키들을 포함할 수도 있다. 본원에 설명된 바와 같이, 디바이스는 인가 인증서를 검증하고, 디바이스에 대한 권한의 증거를 전송하는 인가 서버가 정확한 (예를 들어, 임포스터가 아닌) 인가 서버였다는 것을 확인하고, 피처 활성화 키들을 해독하며, 디바이스에 선택적으로 활성화된 피처들의 제 1 세트를 활성화시키도록 해독된 피처 활성화 키들을 사용했을 수도 있다.

[0225] 디바이스는 네트워크 서비스를 사용하기 위한 요청을 네트워크 노드로 전송 (1604) 할 수도 있다. 선택적으로 활성화된 피처들의 제 1 세트는 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 제 1 선택적으로 활성화된 피처들을 포함할 수도 있다. 제 1 선택적으로 활성화된 피처들은 인가 서버로부터 획득된 권한의 증거에 의해 디바이스에 활성화되도록 인가될 수도 있다. 일부 양태들에 따르면, 제 1 선택적으로 활성화된 피처들의 일부 또는 전부는 네트워크 서비스를 사용하기 위한 요청을 디바이스가 전송하는 시간에 또는 그 전에 디바이스에서 활성화될 수도 있다.

[0226] 디바이스는, 네트워크 서비스를 사용하기 위한 요청을 전송하는 것에 응답하여, 디바이스에 대한 권한의 증거에 대한 요청을 네트워크 노드로부터 획득 (1606) 할 수도 있다. 응답하여, 디바이스는 디바이스에 대한 권한의 증거 (예를 들어, 제 1 인가 서버에 의해 서명된, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거) 를 네트워크 노드로 전송 (1608) 할 수도 있다.

[0227] 디바이스는 네트워크 서비스를 제공하기 위한 네트워크 노드에 대한 권한의 증거에 대한 요청을 네트워크 노드로 전송 (1610) 할 수도 있다.

[0228] 선택적으로, 디바이스는 디바이스 무결성 정보를 전송 (1612) 할 수도 있다. 디바이스 무결성 정보는 보안 부트 프로세스 동안 획득되었을 수도 있다. 더 추가하여 선택적으로, 디바이스는 네트워크 서비스를 사용하기 위한 요청을 검증하는 네트워크 노드와 디바이스 간의 상호 인증 (예를 들어, 원격 증명) 을 수행 (1614) 할 수도 있다.

[0229] 선택적으로, 디바이스는 네트워크 서비스를 사용하기 위한 요청을 허가하는 응답을 획득 (1616) 할 수도 있다. 응답은, 제 1 인가 서버에 의해 서명된, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 전송하는 것의 응답일 수도 있다.

[0230] 디바이스는, 네트워크 노드로부터, 제 2 인가 서버에 의해 서명된, 네트워크 노드에서 선택적으로 활성화된 피처들의 제 2 세트를 사용하기 위한 네트워크 노드에 대한 권한의 증거를 획득 (1618) 할 수도 있다. 선택적으로 활성화된 피처들의 제 2 세트는 네트워크 서비스를 제공하기 위해 네트워크 노드에 의해 필요한 제 2 선택적으로 활성화된 피처들을 포함할 수도 있다.

[0231] 디바이스는, 네트워크 서비스를 사용하기 전에 네트워크 노드에 대한 권한의 증거를 검증 (1620) 할 수도 있다.

[0232] 일부 양태들에서, 디바이스에 대한 권한의 증거 (예를 들어, 인가 서버에서 비롯된 디바이스에 대한 권한의 증거) 는 인가 서버로부터 디바이스에 의해 획득될 수도 있다. 일부 양태들에서, 디바이스에 대한 권한의 증거 (예를 들어, 로컬 인가 서버에서 비롯된 디바이스에 대한 권한의 증거) 는 로컬 인가 서버로부터 디바이스에 의해 획득될 수도 있다. 일부 양태들에서, 디바이스에 대한 권한의 증거는 인가 인증서를 포함할 수도 있다. 일부 양태들에서, 디바이스에 대한 권한의 증거는 피처 활성화 프로세스 동안 (예를 들어, 디바이스에서 네트워크 서비스를 사용하기 위해 필요한 선택적으로 활성화된 피처들의 활성화 동안) 인가 서버, 또는 로컬 인가 서버로부터 획득될 수도 있다.

[0233] 일부 양태들에 따르면, 디바이스는 칩 컴포넌트, 클라이언트 디바이스, 네트워크 액세스 노드, 이동성 관리 엔티티, 또는 게이트웨이 디바이스일 수도 있다. 일 양태에 따르면, 디바이스는 클라이언트 디바이스 또는 칩 컴포넌트일 수도 있고, 네트워크 노드는 네트워크 액세스 노드일 수도 있다. 일 양태에서, 디바이스에 대한 권한의 증거는 제 1 인가 서버에서 비롯되고, 제 1 인가 서버의 사설 키로 서명되며, 제 1 선택적으로 활성화된 피처들의 리스팅을 포함한다. 이러한 양태에서, 방법은 제 1 인가 서버의 공용 키를 사용하여 제 1 선택적으로 활성화된 피처들의 리스팅을 검증함으로써 디바이스에 대한 권한의 증거를 검증하는 것을 더 포함할 수도 있다. 방법은 디바이스의 공용 키로 암호화된, 제 1 선택적으로 활성화된 피처들과 연관된 피처 활성화 키들을 획득하는 것을 더 포함할 수도 있다. 방법은 디바이스에만 알려진, 디바이스의 사설 키를 사용하여,

피처 활성화 키들을 해독하는 것을 더 포함할 수도 있다. 방법은 피처 활성화 키들로 제 1 선택적으로 활성화된 피처들의 활성화를 활성화시키는 것 및/또는 유지하는 것을 더 포함할 수도 있다.

[0234] 일 양태에 따르면, 네트워크에 대한 권한의 증거는 제 2 인가 서버에서 비롯되고, 제 2 인가 서버의 사설 키로 서명되며, 제 2 선택적으로 활성화된 피처들의 리스팅을 포함할 수도 있다. 이러한 양태에서, 방법은 또한, 제 2 인가 서버의 공용 키를 사용하여 제 2 선택적으로 활성화된 피처들의 리스팅을 검증함으로써 네트워크 노드에 대한 권한의 증거를 검증하는 것을 더 포함할 수도 있다.

[0235] 일부 양태들에 따르면, 제 1 인가 서버는 로컬 인가 서버일 수도 있다.

[0236] 일 양태에서, 방법은 또한, 네트워크 서비스를 사용하기 위해 네트워크 노드에 의해 필요한 선택적으로 활성화된 피처들의 제 3 세트를 식별하는 것, 및 선택적으로 활성화된 피처들의 제 3 세트가 선택적으로 활성화된 피처들의 제 2 세트에 포함되는지 여부를 결정하는 것에 기초하여 네트워크 서비스를 사용하는 것을 포함할 수도 있다.

[0237] 또 다른 양태에서, 디바이스에 대한 권한의 증거는 제 1 인가 서버에서 비롯되고 디바이스에서 제 1 인가 서버로부터 획득될 수도 있는 한편, 네트워크 노드에 대한 권한의 증거는 제 2 인가 서버에서 비롯되고 디바이스에서 네트워크 노드로부터 획득된다.

[0238] 일부 양태들에서, 제 1 인가 서버 및 제 2 인가 서버는 하나의 인가 서버이다.

[0239] 일 양태에서, 디바이스에 대한 권한의 증거는 피처 활성화 프로세스 동안 제 1 인가 서버로부터 획득될 수도 있고, 이 동안 디바이스는 제 1 선택적으로 활성화된 피처들을 활성화시키기 위한 인가를 획득한다.

[0240] 일 예에서, 네트워크 노드에 대한 권한의 증거는 인증 및 키 합의 (AKA) 프로세스 동안 네트워크 노드로부터 획득된다.

[0241] 일 양태에서, 디바이스에 대한 권한의 증거는 인가 인증서를 나타내는 데이터일 수 있다. 일 양태에서, 디바이스에 대한 권한의 증거는, 디바이스가 제 1 선택적으로 활성화된 피처들을 활성화시키도록 인가된다는 것을 나타내는 인가 합의를 나타내는 데이터일 수 있다.

[0242] 일 양태에 따르면, 제 1 인가 정보는, 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들 각각에 대해, 선택적으로 활성화된 피처를 활성화시키기 위한 인가가 만료될 때의 날짜를 포함할 수도 있다.

[0243] 도 17 은 본원에 설명된 양태들에 따른 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 에서 동작하는 예시적인 방법 (1700) 의 플로우차트이다. 일 양태에서, 디바이스는 도 15 의 예시적인 디바이스 (1500) 와 유사할 수도 있다. 디바이스는 네트워크 서비스를 제공하기 위한 네트워크 액세스 노드의 능력을 식별하는 정보를 획득 (1702) 할 수도 있다. 정보는 임의의 적합한 방식으로 수신될 수도 있다. 예를 들어, 정보는 네트워크 액세스 노드 (예를 들어, eNB) 로부터 광고의 형태로 수신될 수도 있다. 광고는 공중파 브로드캐스트를 통해 네트워크 능력을 광고 (예를 들어, 시스템 정보 블록 (SIB) 에 제시된 정보를 통해 광고) 할 수도 있다. 다른 예로서, 정보는 액세스 네트워크 질의 프로토콜 (ANQP) 또는 서비스 질의 프로토콜 (SQP) 질의에 응답하여 수신될 수도 있다. 네트워크 능력은, 예를 들어 네트워크 액세스 노드에 의해 제공된 네트워크 서비스를 포함할 수도 있다.

[0244] 디바이스는, 네트워크 액세스 노드로부터 네트워크 서비스를 제공하기 위한 네트워크 액세스 노드의 권한을 확인하도록 인가 정보를 획득 (1704) 할 수도 있다. 일 양태에서, 인가 정보는 인가 인증서의 형태로 있을 수도 있다. 인가 서버 (또는 로컬 인가 서버) 는 인가 인증서를 네트워크 액세스 노드로 전송했을 수도 있다. 디바이스는, 예를 들어, 네트워크 액세스 노드가 네트워크 서비스를 제공하도록 인가된다는 것을 확인하기 위해 인가 정보를 전송하도록 네트워크 액세스 노드로 요청을 전송함으로써 인가 정보를 획득할 수도 있다.

[0245] 디바이스는 네트워크 서비스를 제공하기 위한 네트워크 액세스 노드의 권한 및/또는 네트워크 액세스 노드를 검증하도록 인가 정보를 검증 (1706) 할 수도 있다. 일부 양태들에서, 인가 정보는 인가 인증서를 검증함으로써 검증될 수도 있다. 일부 양태들에서, 인가 서버가 인가 인증서를 발행했으면, 인가 인증서는 인가 서버의 공용 키를 사용하여 검증될 수도 있다. 일부 양태들에서, 로컬 인가 서버가 인가 인증서를 발행했으면, 인가 인증서는 로컬 인가 서버의 공용 키를 사용하여 검증될 수도 있다. 디바이스는, 인가 정보의 검증이 성공적이었는지를 결정 (1708) 할 수도 있다. 디바이스가, 인가 정보의 검증이 성공적이었다고 결정하면, 디바이스는 네트워크 서비스를 사용 (1710) 할 수도 있다. 디바이스가, 인가 정보의 검증이 성공적이지 않

았다고 결정하면, 디바이스는 네트워크 서비스를 사용하지 않을 (1712) 수도 있다.

[0246] 도 18 은 본원에 설명된 양태들에 따라 네트워크 노드 (예를 들어, 네트워크 액세스 노드, eNB, MME, S-GW, P-GW) 에서 동작하는 예시적인 방법 (1800) 의 플로우차트이다. 일 양태에서, 네트워크 노드는 도 15 의 예시적인 디바이스 (1500) 와 유사할 수도 있다. 네트워크 노드는 디바이스로부터, 네트워크 서비스를 사용하기 위한 요청을 획득 (1802) 할 수 있다. 네트워크 노드는 또한, 디바이스로부터, 인가 서버에 의해 서명된, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 획득 (1804) 할 수도 있다.

[0247] 네트워크 노드는 디바이스에 대한 권한의 증거를 검증 (1806) 할 수도 있다. 즉, 네트워크 노드는 인가 서버에 의해 서명된, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 검증할 수도 있다. 네트워크 노드는 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스의 권한을 검증하기 위해 디바이스에 대한 권한의 증거를 검증할 수도 있다. 선택적으로 활성화된 피처들의 제 1 세트는 네트워크 서비스를 사용하도록 디바이스에 의해 필요로될 수도 있다. 일부 양태들에서, 디바이스에 대한 권한의 증거는 인가 인증서를 검증함으로써 검증될 수도 있다. 일부 양태들에서, 인가 서버가 인가 인증서를 발행한 경우, 인가 인증서는 인가 서버의 공용 키를 사용하여 검증될 수도 있다. 일부 양태들에서, 로컬 인가 서버가 인가 인증서를 발행한 경우, 인가 인증서는 로컬 인가 서버의 공용 키를 사용하여 검증될 수도 있다.

[0248] 네트워크 노드는 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 피처들을 독립적으로 식별하고, 그 후에 선택적으로 활성화된 피처들의 제 1 세트를 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 독립적으로 식별된 피처들에 비교할 수도 있다. 네트워크 노드는, 독립적으로 식별된 피처들이 선택적으로 활성화된 피처들의 제 1 세트에 일치하는 경우 디바이스가 네트워크 서비스를 사용할 수 있다고 결정할 수도 있다.

[0249] 따라서, 네트워크 노드는 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 선택적으로 활성화된 피처들의 제 2 세트를 식별 (1808) 할 수도 있다. 다른 양태에 따르면, 네트워크 노드는 인가 서버 (또는 로컬 인가 서버) 에 의해 유지된, 인가된 선택적으로 활성화된 피처들의 모델-특정 리스트, 인가 서버 (또는 로컬 인가 서버) 에 의해 유지된, 인가된 선택적으로 활성화된 피처들의 디바이스-특정 리스트, 또는 인가 서버 (또는 로컬 인가 서버) 에 의해 유지된, 인가된 선택적으로 활성화된 피처들의 모델-특정 및 디바이스-특정 리스트로부터 피처들을 획득 또는 도출함으로써 선택적으로 활성화된 피처들의 제 2 세트를 식별할 수도 있다. 일 양태에 따르면, 네트워크 노드는 인가 서버 (또는 로컬 인가 서버) 에 의해 유지된 라이선싱 가능한 선택적으로 활성화된 피처들의 모델-특정 리스트, 인가 서버 (또는 로컬 인가 서버) 에 의해 유지된 라이선싱 가능한 선택적으로 활성화된 피처들의 디바이스-특정 리스트, 또는 인가 서버 (또는 로컬 인가 서버) 에 의해 유지된 라이선싱 가능한 선택적으로 활성화된 피처들의 모델-특정 및 디바이스-특정 리스트로부터 피처들을 획득 또는 도출함으로써 선택적으로 활성화된 피처들의 제 2 세트를 식별할 수도 있다.

[0250] 네트워크 노드는, 디바이스에 대한 권한의 증거를 검증하고 선택적으로 활성화된 피처들의 제 2 세트가 선택적으로 활성화된 피처들의 제 1 세트에 포함되는지 여부를 결정한 결과들에 기초하여 요청에 대한 응답을 전송 (1810) 할 수도 있다. 네트워크 노드에 의해 독립적으로 식별된 피처들 (즉, 선택적으로 활성화된 피처들의 제 2 세트) 이 디바이스에 활성화되도록 인가된 선택적으로 활성화된 피처들의 제 1 세트에 또는 그 서브세트에 포함되고, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거가 성공적으로 확인되면, 네트워크 서비스를 사용하기 위한 요청에 대한 응답은, 디바이스가 네트워크 서비스를 사용하도록 허용된다는 것을 나타낼 수도 있다.

[0251] 그러나, 선택적으로 활성화된 피처들의 제 2 세트가 선택적으로 활성화된 피처들의 제 1 세트에 포함되지 않으면 또는 디바이스에 대한 권한의 증거가 성공적으로 검증되지 않으면, 네트워크 노드는 네트워크 서비스를 사용하기 위한 요청을 무시할 수도 있고 또는 디바이스가 네트워크 서비스를 사용하도록 허용되지 않는다는 것을 나타내도록 응답을 전송할 수도 있다.

[0252] 일부 양태들에 따르면, 네트워크 노드는 네트워크 액세스 노드 (예를 들어, eNB), 이동성 관리 엔티티, 및/또는 게이트웨이 디바이스일 수도 있다.

[0253] 일 양태에서, 선택적으로 활성화된 피처들의 제 1 세트는 제 1 선택적으로 활성화된 피처들을 포함하고, 디바이스에 대한 권한의 증거는 인가 서버에서 비롯된다. 디바이스에 대한 권한의 증거는, 인가 서버의 사설 키로

서명된, 제 1 선택적으로 활성화된 피처들의 리스팅을 포함할 수 있다. 일 예에서, 방법은 인가 서버의 공용 키를 사용하여 제 1 선택적으로 활성화된 피처들의 리스팅을 검증함으로써 디바이스에 대한 권한의 증거를 검증하는 것을 더 포함할 수 있다.

[0254] 일 양태에서, 디바이스에 대한 권한의 증거는 인가 서버에서 비롯되고, 네트워크 노드에서 디바이스로부터 획득될 수 있다. 다른 양태에서, 디바이스에 대한 권한의 증거는 인가 서버에서 비롯되고, 홈 가입자 서버 (HSS) 로부터, 디바이스의 능력 프로파일의 형태로 네트워크 노드에서 획득될 수 있다. 다른 양태에서, 디바이스에 대한 권한의 증거는 인증 및 키 합의 (AKA) 프로세스 동안 디바이스로부터 획득될 수 있다. 일부 양태들에서, 디바이스에 대한 권한의 증거는 인가 인증서를 나타내는 데이터일 수 있다. 또 다른 양태들에서, 디바이스에 대한 권한의 증거는, 디바이스가 선택적으로 활성화된 피처들의 제 1 세트를 활성화시키도록 인가된다는 것을 나타내는 인가 합의를 나타내는 데이터일 수 있다.

[0255] 일 예에서, 선택적으로 활성화된 피처들의 제 2 세트를 식별하는 것은 인가 서버에 의해 유지된, 인가된 선택적으로 활성화된 피처들의 모델-특정 및/또는 디바이스-특정 리스트로부터 네트워크 서비스를 사용하기 위해 디바이스에 의해 제 2 선택적으로 활성화된 피처들을 도출하는 것을 포함할 수 있다. 다른 예에서, 선택적으로 활성화된 피처들의 필요한 세트를 식별하는 것은 인가 서버에 의해 유지된 라이선싱 가능한 선택적으로 활성화된 피처들의 모델-특정 및/또는 디바이스-특정 리스트로부터 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 선택적으로 활성화된 피처들을 네트워크 노드가 도출하는 것을 포함할 수 있다.

[0256] 일 양태에서, 방법은 디바이스에 대한 권한의 증거에 포함된 디바이스의 공용 키에 대응하는 사설 키를 디바이스가 홀딩한다는 것을 확인하는 것을 더 포함할 수 있고, 여기서 요청에 대한 응답을 전송하는 것은 확인하는 것의 결과에 더 기초할 수 있다.

[0257] 일부 양태들에서, 방법은 디바이스의 무결성 정보를 수신하는 것을 더 포함할 수도 있다. 이러한 양태들에서, 요청에 대한 응답은, 무결성 정보가 수용 가능한지 여부를 결정하는 것에 더 기초할 수도 있다. 일부 양태들에 따르면, 디바이스 능력 프로파일은 보안 부트 프로세스, 인증된 부트 프로세스, 또는 보안 및 인증된 부트 프로세스 동안 생성된 디바이스 무결성 정보를 포함할 수도 있다. 일 예에서, 디바이스 무결성 정보는 디바이스의 인가 회로/기능부/모듈의 무결성을 입증할 수도 있다.

[0258] 일부 양태들에서, 디바이스에 대한 권한의 증거는 인가 서버, 로컬 인가 서버, 또는 인가 서버 및 로컬 인가 서버에서 비롯 (예를 들어, 먼저 획득되고, 먼저 도출) 될 수도 있다. 인가 서버 및 로컬 인가 서버는 인가, 인증, 및 어카운팅 (AAA) 서버와 상이할 수도 있다. 인가 서버 및 로컬 인가 서버는 홈 가입자 서버 (HSS) 와 상이할 수도 있다.

[0259] 일부 양태들에 따르면, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거는, 선택적으로 활성화된 피처들 각각에 대해, 선택적으로 활성화된 피처를 활성화시키기 위한 인가가 만료될 때의 날짜를 포함한다.

[0260] 일 양태에서, 디바이스에 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거는 적절한 시간에 디바이스로부터 네트워크 노드에 의해 획득될 수도 있다. 일 예로서, 디바이스에 대한 권한의 증거는 디바이스가 네트워크에 어태치하는 경우 디바이스로부터 획득될 수도 있다. 다른 예로서, 디바이스에 대한 권한의 증거는 피처 활성화 프로세스 동안 인가 서버 또는 로컬 인가 서버로부터 획득될 수도 있다.

[0261] 일 예에서, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거는 홈 가입자 서버 (HSS) 로 전송될 수도 있다. 일부 구현들에서, 디바이스의 선택적으로 활성화된 피처의 인가 스테이터스 (예를 들어, 선택적으로 활성화된 피처가 인가 및 활성화되는지 여부를 나타내는 스테이터스) 는 HSS 로 전송될 수도 있다. 디바이스에 대한 권한의 증거, 디바이스의 선택적으로 활성화된 피처들의 인가 스테이터스, 또는 디바이스의 선택적으로 활성화된 피처들의 인가 스테이터스 및 디바이스에 대한 권한의 증거는 디바이스의 능력 프로파일을 업데이트하는데 사용될 수도 있고, 여기서 능력 프로파일은 HSS 에 저장될 수 있다.

[0262] 일 양태에서, HSS 로부터 디바이스의 능력 프로파일은 획득하는 것은 네트워크 노드 (예를 들어, eNB, MME, S-GW, P-GW) 가 증거의 다른 형태를 획득하기 위해 네트워크 노드에 대한 필요성 없이 선택적으로 활성화된 피처들을 사용하기 위한 디바이스의 인가를 검증하는 것을 허용할 수도 있다 (예를 들어, 디바이스로부터, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 획득하기 위해

네트워크 노드에 대한 필요성을 배제할 수도 있다).

[0263] 일부 구현들에서, 네트워크 노드는 디바이스의 능력 프로파일에 기초하여 디바이스 콘텍스트 (예를 들어, UE 콘텍스트) 를 생성 및/또는 변경할 수 있다. 일부 양태들에 따르면, HSS 는 디바이스에 활성화되도록 인가된 선택적으로 활성화된 피처들을 식별하는 정보 엘리먼트를 전송할 수도 있다. 일 양태에서, 정보 엘리먼트는 디바이스의 능력 프로파일을 포함할 수 있다. HSS 는 정보 엘리먼트를 네트워크 노드로 전송할 수도 있다.

일부 양태들에 따르면, 네트워크 노드는 HSS 에 저장된 디바이스의 능력 프로파일에 대한 변화들에 기초하여 선택적으로 활성화된 피처들을 활성화 및/또는 비활성화시킬 수도 있다. 선택적으로 활성화된 피처들은 네트워크 노드의 선택적으로 활성화된 피처들일 수도 있다. HSS 에 저장된 디바이스의 능력 프로파일에 대한 변화들에 기초하여 선택적으로 활성화된 피처들의 활성화 및/또는 비활성화는 디바이스 콘텍스트 (예를 들어, UE 콘텍스트) 를 생성 및/또는 변경하는 것을 용이하게 할 수도 있다.

[0264] 도 19 는 본원에 설명된 양태들에 따라 네트워크 노드 (예를 들어, 네트워크 액세스 노드, eNB, MME, S-GW, P-GW) 에서 동작하는 다른 예시적인 방법 (1900) 의 플로우차트이다. 일 양태에서, 네트워크 노드는 도 15 의 예시적인 디바이스 (1500) 와 유사할 수도 있다. 네트워크 노드는 디바이스로부터, 네트워크 서비스를 사용하기 위한 요청을 획득 (1902) 할 수 있다. 네트워크 노드는 또한, 인가 서버에 의해 서명된, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 획득 (1904) 할 수도 있다.

[0265] 네트워크 노드는 디바이스에 대한 권한의 증거를 검증 (1906) 할 수도 있다. 일부 양태들에서, 디바이스에 대한 권한의 증거는 인가 인증서를 검증함으로써 검증될 수도 있다. 일부 양태들에서, 인가 서버가 인가 인증서를 발행한 경우, 인가 인증서는 인가 서버의 공용 키를 사용하여 검증될 수도 있다. 일부 양태들에서, 로컬 인가 서버가 인가 인증서를 발행한 경우, 인가 인증서는 로컬 인가 서버의 공용 키를 사용하여 검증될 수도 있다.

[0266] 네트워크 노드는 또한, (디바이스에 대한 권한의 증거를 전송한) 디바이스가 권한의 증거에 포함된 디바이스의 공용 키에 대응하는 사설 키를 홀딩한다는 것을 확인 (1908) 할 수도 있다. 이 방식에서, 네트워크 노드는, 권한의 증거를 전송한 디바이스가 권한의 증거에서 식별된 디바이스라는 것을 확인할 수 있다. 일부 양태들에서, 디바이스가 권한의 증거에 포함된 디바이스의 공용 키에 대응하는 사설 키를 홀딩한다는 것을 확인하는 것은, 권한의 증거에 포함된 디바이스의 공용 키를 사용하여, (디바이스의 사설 키로 디바이스에 의해 이루어진) 디바이스의 서명을 검증하는 것을 수반할 수 있다.

[0267] 네트워크 노드는, 디바이스에 대한 권한의 증거의 검증 및 디바이스의 확인이 성공적이었는지를 결정 (1910) 할 수도 있다. 네트워크 노드가, 디바이스에 대한 권한의 증거의 검증, 디바이스의 확인, 또는 디바이스에 대한 권한의 증거의 검증 및 디바이스의 확인이 성공적이지 않았다고 결정하면, 네트워크 노드는 네트워크 서비스를 사용하기 위한 요청을 무시할 수도 있고 또는 네트워크 서비스를 사용하기 위한 요청을 거부하는 응답을 전송 (1912) 할 수도 있다.

[0268] 네트워크 노드가, 디바이스에 대한 권한의 증거의 검증 및 디바이스의 확인 양자 모두가 성공적이었다고 결정하면, 네트워크 노드는 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 피처들을 식별 (1914) 할 수도 있다. 일 예에서, 네트워크 노드는 식별을 독립적으로 할 수도 있다.

[0269] 디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들의 제 1 세트의 리스팅은 디바이스에 대한 권한의 증거로부터 획득될 수 있다. 네트워크 노드는 권한의 증거에서 나열된 선택적으로 활성화된 피처들을 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 식별된 피처들과 비교 (1916) 할 수도 있다.

[0270] 디바이스에 대한 권한의 증거에 포함된 선택적으로 활성화된 피처들이 네트워크 노드에 의해 식별된 피처들에 일치하는지 여부에 관한 결정이 이루어질 수도 있다 (1918). 이 결정에 기초한 응답이 그 후, 전송될 수도 있다. 피처들이 일치하는 경우, 네트워크 노드는 네트워크 서비스를 사용하기 위한 요청을 허가하는 응답을 전송 (1920) 할 수도 있다. 피처들이 일치하지 않는 경우, 네트워크 노드는 네트워크 서비스를 사용하기 위한 요청을 무시하거나 또는 네트워크 서비스를 사용하기 위한 요청을 거부하는 응답을 전송 (1922) 할 수도 있다.

[0271] **예시적인 홈 가입자 서버 (HSS)**

[0272] 도 20 은 본원에 설명된 양태들에 따른 인가 합의들의 동적 확인 및 시행을 지원하도록 구성된 예시적인 홈 가입자 서버 (HSS) (2000) 를 예시하는 블록도이다. 일 예에서, 예시적인 HSS (2000) 는 네트워크 통신 회로

(2002), 프로세싱 회로 (2004), 및 (메모리 회로 (2006) 로서 본원에 지칭된) 메모리 회로/저장 디바이스를 포함할 수도 있다. 네트워크 통신 회로 (2002), 프로세싱 회로 (2004), 및 메모리 회로 (2006) 는 데이터 및 명령들의 교환을 위해 통신 버스 (2008) 에 커플링될 수도 있다.

[0273] 네트워크 통신 회로 (2002) 는 입/출력 동작들을 위해 제 1 입/출력 회로/기능부/모듈 (2010) 을 포함할 수도 있다. 당업자에 의해 인지되는 바와 같이, 다른 회로들/기능부들/모듈들이 네트워크 통신 회로 (2002) 에 포함될 수도 있다.

[0274] 프로세싱 회로 (2004) 는 인가 합의들의 검증 및 시행을 지원하도록 구성되는 하나 이상의 프로세서들, 애플리케이션 특정 프로세서들, 하드웨어 및/또는 소프트웨어 모듈들 등을 포함 또는 구현하도록 구성될 수도 있다. 프로세싱 회로 (2004) 는 HSS 의 기능성을 구현하도록 HSS 동작들 회로/기능부/모듈 (2012) 을 포함하도록 구성될 수도 있다. 프로세싱 회로 (2004) 는 또한, 인가 기능 회로/기능부/모듈 (2014) 을 포함하도록 구성될 수도 있다. 당업자에 의해 인지되는 바와 같이, 다른 회로들/기능부들/모듈들이 프로세싱 회로 (2004) 에 포함될 수도 있다.

[0275] 메모리 회로 (2006) 는 복수의 디바이스들에 대해, 가입 프로파일들 (2016) 및 능력 프로파일들 (2017) 을 저장하기 위한 저장 공간을 포함하도록 구성될 수도 있다. 메모리 회로 (2006) 는 또한, 본원에서 인가 명령들 (2020) 로서 지칭된, HSS 동작 명령들 (2018) 및 인가 회로/기능부/모듈 명령들을 포함하도록 구성될 수도 있다. 당업자에 의해 인지되는 바와 같이 데이터의 저장을 위한 다른 명령들 및 로케이션들이 메모리 회로 (2006) 에 포함될 수도 있다.

[0276] 네트워크 통신 회로 (2002), 프로세싱 회로 (2004), 메모리 회로 (2006), 및 예시적인 HSS (2000) 의 다른 컴포넌트들 (미도시) 간의 통신은 통신 버스 (2008) 등을 통해서일 수도 있다.

[0277] **홈 가입자 서버에서 동작하는 예시적인 방법**

[0278] 도 21 은 본원에 설명된 양태들에 따른 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드) 의 하나 이상의 선택적으로 활성화된 피처들의 세트의 사용을 위해 인가를 검증하는 것에 관련되는, 서버 (예를 들어, HSS) 에서 동작하는 예시적인 방법 (2100) 을 예시한다. 서버는 도 20 의 예시적인 HSS (2000) 와 유사할 수도 있다.

[0279] 예시적인 방법 (2100) 에서, 서버 (예를 들어, HSS) 는 디바이스의 선택적으로 활성화된 피처들 (예를 들어, 디바이스의 획득된 능력 프로파일) 의 제 1 리스트를 획득 (2102) 할 수도 있다.

[0280] 디바이스의 인가 스테이터스에 대한 변화와 관련한 정보는 디바이스의 능력들에 대한 변화에 관한 정보로서 간주될 수도 있다. 디바이스의 인가 스테이터스에 대한 변화에 관한 정보는 디바이스의 선택적으로 활성화된 피처들의 세트에서 적어도 하나의 선택적으로 활성화된 피처의 인가 스테이터스에 대한 변화에 관련할 수도 있다.

[0281] 서버 (예를 들어, HSS) 는 제 1 리스트에 기초하여, 서버 (예를 들어, HSS) 에 저장된, 디바이스의 선택적으로 활성화된 피처들의 제 2 리스트를 업데이트 (2104) 할 수 있다. 제 2 리스트는 디바이스의 저장된 능력 프로파일로서 지칭될 수도 있다. 일 양태에 따르면, 서버 (예를 들어, HSS) 에 저장된 제 2 리스트는 디바이스의 가입 프로파일과 연관될 수 있다. HSS 에 저장된, 디바이스의 선택적으로 활성화된 피처들의 제 2 리스트에 대한 업데이트는 제 2 리스트에서의 적어도 하나의 선택적으로 활성화된 피처의 인가 스테이터스에 대한 변화를 반영할 수도 있다.

[0282] 일 양태에서, 선택적으로 활성화된 피처들의 제 1 리스트는 인가 서버에서 비롯될 수 있고 인가 서버의 사설 키로 서명될 수 있다. 이러한 양태에 따르면, 방법은 또한, 인가 서버의 공용 키를 사용하여 선택적으로 활성화된 피처들의 제 1 리스트를 검증하는 단계를 포함할 수도 있다.

[0283] 서버 (예를 들어, HSS) 는 디바이스의 능력에 관한 질의를 획득할 수도 있다. 본원에 설명된 양태에 따르면, 서버 (예를 들어, HSS) 는, 디바이스의 능력에 관련한 질의에 응답하여, 디바이스의 선택적으로 활성화된 피처들의 제 2 리스트를 포함하는 능력 프로파일을 전송 (2106) 할 수도 있다.

[0284] 일 예에 따르면, HSS 는 초기 어태치 절차 동안 디바이스의 능력에 관련한 질의를 획득할 수도 있다. 질의는 MME 로부터 획득될 수도 있다. HSS 는, 이 질의에 응답하여, 제 2 리스트를 포함하는 능력 프로파일을 MME 로 전송할 수도 있다. 능력 프로파일은 디바이스의 가입 프로파일과 연관될 수도 있다.

[0285] 대안으로, HSS 는 HSS 에 저장된 정보의 특정 엘리먼트에 대한 요청을 획득할 수도 있다. 정보의 엘리먼트는 디바이스의 능력에 관련할 수도 있다. 정보의 엘리먼트는 디바이스의 선택적으로 활성화된 피처들의 제 2 리스트에서 (예를 들어, 디바이스의 저장된 능력 프로파일에서) 식별된 하나 이상의 선택적으로 활성화된 피처들에 관련할 수도 있다.

[0286] 초기 어태치 절차의 예를 사용하여, HSS 는 제 1 디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스) 의 능력 프로파일을 제 2 디바이스 (예를 들어, MME) 전송할 수 있으므로, 제 2 디바이스 (예를 들어, MME) 는 제 1 디바이스 상에서 이미 인가/활성화된 선택적으로 활성화된 피처들을 구현 또는 준수하도록 다양한 피처(들)을 구성할 수 있다.

[0287] 제 2 디바이스 (예를 들어, MME) 는 제 2 디바이스 (예를 들어, MME) 에 대한 필요성 없이 하나 이상의 선택적으로 활성화된 피처들을 사용하기 위한 제 1 디바이스의 권리를 검증하여, 제 1 디바이스로부터 제 1 인가 서버에 의해 서명된, 제 1 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 제 1 디바이스에 대한 권한의 증거 (예를 들어, 인가 인증서의 형태의 인가 정보) 를 획득할 수도 있다. 제 1 디바이스에 대한 권한의 증거는 선택적으로 활성화된 피처들의 세트를 사용하기 위한 제 1 디바이스의 권리를 검증하기 위해 제 2 디바이스 (예를 들어, MME) 에 의해 필요로될 수도 있다. 대안의 양태에서, 증거는 HSS 로부터 제 2 디바이스 (예를 들어, MME) 에 의해 획득되고, 제 1 디바이스로부터의 입력 없이 네트워크에 구성될 수도 있다.
따라서, 그리고 예를 들어, 예를 들어 강화된 액세스 네트워크 질의 프로토콜 또는 서비스 질의 프로토콜을 사용하여 HSS 로부터 획득될 수도 있는, 디바이스의 능력에 관련할 수도 있는 정보의 엘리먼트 및/또는 능력 프로파일의 사용은 인가 합의를 검증 및 시행하는데 있어서 MME 의 효율성을 용이하게 하고/스피드-업하고/개선시킬 수도 있다.

[0288] 도시 및 설명된 특정 구현들은 단지 예들이며, 본원에서 다르게 지정되지 않으면 본 개시물을 구현하기 위한 유일한 방식으로서 해석되지 않아야 한다. 본 개시물의 다양한 예들이 다수의 다른 솔루션들에 의해 실시될 수도 있다는 것이 당업자에게 용이하게 명백하다.

[0289] 본원에 설명되고 도면들에 예시된 컴포넌트들, 액트들, 피처들 및/또는 기능들 중 하나 이상은 단일의 컴포넌트, 액트, 피처, 또는 기능으로 재배열 및/또는 결합될 수도 있고, 또는 여러 컴포넌트들, 액트들, 피처들, 또는 기능들에 포함될 수도 있다. 추가의 엘리먼트들, 컴포넌트들, 및/또는 기능들이 또한, 본 개시물로부터 벗어남 없이 추가될 수도 있다. 또한, 본원에서 설명된 알고리즘들은 소프트웨어에서 효율적으로 구현되고/되거나 하드웨어에 임베디드될 수도 있다.

[0290] 설명에서, 엘리먼트들, 회로들, 기능들, 및 모듈들은 불필요한 상세에서 본 개시물을 모호하게 하지 않기 위해 블록도 형태로 도시될 수도 있다. 반대로, 도시 및 설명된 특정 구현들은 단지 예시적이며, 본원에 다르게 지정되지 않으면 본 개시물을 구현하기 위한 유일한 방식으로서 해석되지 않아야 한다. 부가적으로, 블록 정의들 및 다양한 블록들 간의 로직의 파티셔닝은 특정 구현의 예이다. 대부분, 타이밍 고려사항들 등에 관련한 상세들은 생략되어 있고, 여기서 이러한 상세들은 본 개시물의 완전한 이해를 획득하는데 불필요하며 관련 기술의 당업자의 능력들 내에 있다.

[0291] 또한, 예들은 플로우차트, 흐름도, 구조도, 또는 블록도로 도시되는 프로세스로서 설명된다는 것이 주목된다.
흐름도가 순차적인 프로세스로서 동작들을 설명할 수도 있지만, 많은 동작들은 병렬로 또는 동시에 수행될 수 있다. 또한, 동작들의 순서는 재배열될 수도 있다. 프로세스는 프로세스의 동작들이 완료되는 경우 종료된다. 프로세스는 방법, 기능, 절차, 서브루틴, 서브프로그램 등에 대응할 수도 있다. 프로세스가 기능에 대응하면, 그 종료는 호출 기능 또는 메인 기능으로의 그 기능의 리턴에 대응한다.

[0292] 당업자는, 정보 및 신호들이 임의의 다양한 상이한 기술들 및 기법들을 사용하여 표현될 수도 있음을 인지할 것이다. 예를 들어, 이 설명을 통해 참조될 수도 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들, 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 입자들, 광학장들 또는 입자들, 또는 이들의 임의의 조합에 의해 표현될 수도 있다. 일부 도면들은 제시 및 설명의 명확함을 위해 단일 신호로서 신호들을 예시할 수도 있다. 이 신호는 신호들의 버스를 나타낼 수도 있다는 것이 당업자에 의해 이해될 것이고, 여기서 버스는 다양한 비트 폭들을 가질 수도 있고 본 개시물은 단일의 데이터 신호를 포함하는, 임의의 수의 데이터 신호들 상에서 구현될 수도 있다.

[0293] "제 1", "제 2" 등과 같은 지정을 사용하는 본원에서 엘리먼트에 대한 임의의 참조는, 이러한 제한이 명확하게 언급되지 않으면, 이들 엘리먼트들의 양 또는 순서를 제한하지 않는 것으로 이해되어야 한다. 차라리, 이들

지정들은 2 이상의 엘리먼트들 또는 엘리먼트의 인스턴스들 간에 구별되는 편리한 방법으로서 본원에서 사용될 수도 있다. 따라서, 제 1 및 제 2 엘리먼트들에 대한 참조는 단지 2 개의 엘리먼트들이 거기서 이용될 수 있고, 또는 제 1 엘리먼트가 임의의 방식으로 제 2 엘리먼트보다 선행되어야 한다는 것을 의미하지 않는다. 또한, 다르게 언급되지 않으면, 엘리먼트들의 세트는 하나 이상의 엘리먼트들을 포함할 수도 있다. 또한, 단수로 사용된 단어들은 복수를 포함하고 복수로 사용된 단어들은 단수를 포함하는 것으로 이해되어야 한다.

[0294] 또한, 저장 매체는, 판독 전용 메모리 (ROM), 랜덤 액세스 메모리 (RAM), 자기 디스크 저장 매체, 광학 저장 매체들, 플래시 메모리 디바이스들 및/또는 다른 머신-판독가능 매체들, 프로세서-판독가능 매체들, 프로세싱 회로 판독가능 매체들, 및/또는 정보를 저장하기 위한 프로세서-판독가능 매체들을 포함하는, 데이터를 저장하기 위한 하나 이상의 디바이스들을 나타낼 수도 있다. 용어들 "머신-판독가능 매체", "프로세서-판독가능 매체", "프로세싱 회로 판독가능 매체", 및/또는 "컴퓨터-판독가능 매체" 는 비-일시적 매체들, 예컨대 휴대용 또는 고정된 저장 디바이스들, 광학 저장 디바이스들, 및 명령(들) 및/또는 데이터를 저장, 포함, 또는 반송할 수 있는 다양한 다른 매체들을 포함할 수도 있지만, 이에 제한되지는 않는다. 따라서, 본원에 설명된 다양한 방법들은 머신-판독가능 매체, 프로세서-판독가능 매체, 프로세싱 회로 판독가능 매체, 및/또는 컴퓨터 판독가능 매체에 저장될 수도 있고, 하나 이상의 프로세서들, 프로세싱 회로들, 머신들, 및/또는 디바이스들에 의해 실행될 수도 있는 명령들 및/또는 데이터에 의해 전체적으로 또는 부분적으로 구현될 수도 있다.

[0295] 또한, 양태들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 또는 이들의 임의의 조합에 의해 구현될 수도 있다. 소프트웨어, 펌웨어, 미들웨어, 또는 마이크로코드에서 구현되는 경우, 태스크들을 수행하기 위한 프로그램 코드 또는 코드 세그먼트들은 머신-판독가능 매체, 예컨대 저장 매체 또는 다른 스토리지(들)에 저장될 수도 있다. 프로세싱 회로는 태스크들을 수행할 수도 있다. 코드 세그먼트는 프로세스, 절차, 기능, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스, 또는 명령들, 데이터 구조물들, 또는 프로그램 스테이트먼트들의 임의의 조합을 나타낼 수도 있다. 코드 세그먼트는 정보, 데이터, 아규먼트들, 파라미터들, 또는 메모리 콘텐츠를 패스, 포워딩, 또는 송신함으로써 다른 코드 세그먼트 또는 하드웨어 회로에 커플링될 수도 있다. 정보, 데이터, 아큐먼트들, 파라미터들, 또는 메모리 콘텐츠 등은 메모리 공유, 메시징 패싱, 토큰 패싱, 네트워크 송신 등을 포함하는 임의의 적합한 수단을 통해 패스, 포워딩, 또는 송신될 수도 있다.

[0296] 본원에서 개시된 예들과 연관되어 설명된 다양한 예시적인 논리 블록들, 엘리먼트들, 모듈들, 회로들, 기능부들, 및/또는 컴포넌트들은 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적 회로 (ASIC), 필드 프로그래머블 게이트 어레이 (FPGA) 또는 다른 프로그래머블 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에 설명된 기능들을 수행하도록 설계된 것들의 임의의 조합에 의해 구현 또는 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안에서 범용 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수도 있다. 프로세서는 또한, 컴퓨팅 컴포넌트들의 조합, 예를 들어 DSP 와 마이크로프로세서, 다수의 마이크로프로세서들, DSP 코어와 연계한 하나 이상의 마이크로프로세서들의 조합, 또는 임의의 다른 이러한 구성으로 구현될 수도 있다. 본원에 설명된 양태들을 실행하기 위해 구성된 범용 프로세서는 이러한 양태들을 수행하기 위한 특수-목적의 프로세서로 간주된다. 유사하게, 범용 컴퓨터는 본원에 설명된 양태들을 수행하기 위해 구성되는 경우 특수-목적의 컴퓨터로 간주된다.

[0297] 본원에 개시된 예들과 연관되어 설명된 방법들 또는 알고리즘들은 하드웨어에서, 프로세서에 의해 실행 가능한 소프트웨어 모듈에서, 또는 이 둘의 조합에서, 프로세싱 유닛, 프로그래밍 명령들, 또는 다른 지시들의 형태로 직접 포함될 수도 있고, 단일의 디바이스에 포함되거나 또는 다수의 디바이스들에 걸쳐 분산될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 착탈형 디스크, CD-ROM, 또는 당업자에 의해 인지된 임의의 다른 형태의 저장 매체 내에 상주할 수도 있다. 저장 매체는 프로세서에 커플링되어, 프로세가 저장 매체로부터 정보를 판독하거나 저장 매체에 정보를 기록하도록 할 수도 있다. 대안에서, 저장 매체는 프로세서에 통합될 수도 있다.

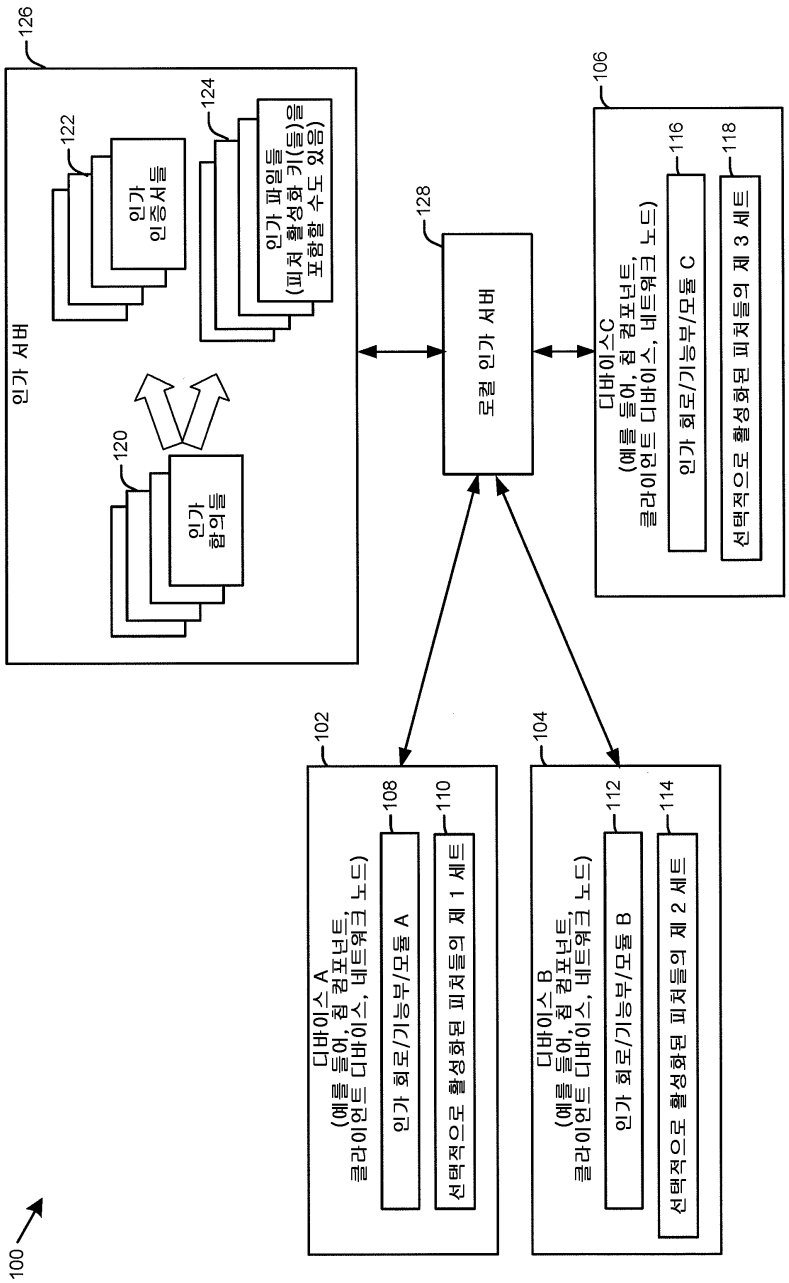
[0298] 당업자는 또한, 본원에 설명된 예들과 연관되어 설명된 다양한 예시적인 논리 블록들, 회로들, 기능들, 모듈들 및 알고리즘들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양자 모두의 조합으로서 구현될 수도 있음을 인지할 것이다. 하드웨어와 소프트웨어의 이러한 상호교환성을 명확하게 설명하기 위해, 다양한 예시적인 엘리먼트들, 컴포넌트들, 블록들, 기능들, 회로들, 모듈들 및 알고리즘들이 그들의 기능성에 대해 일반적으로 전술되었다. 이러한 기능이 하드웨어, 소프트웨어, 또는 이들의 조합으로서 구현되는지 여부는 특정 애플리케이션

및 전체 시스템에 부과되는 설계 제약들에 의존한다.

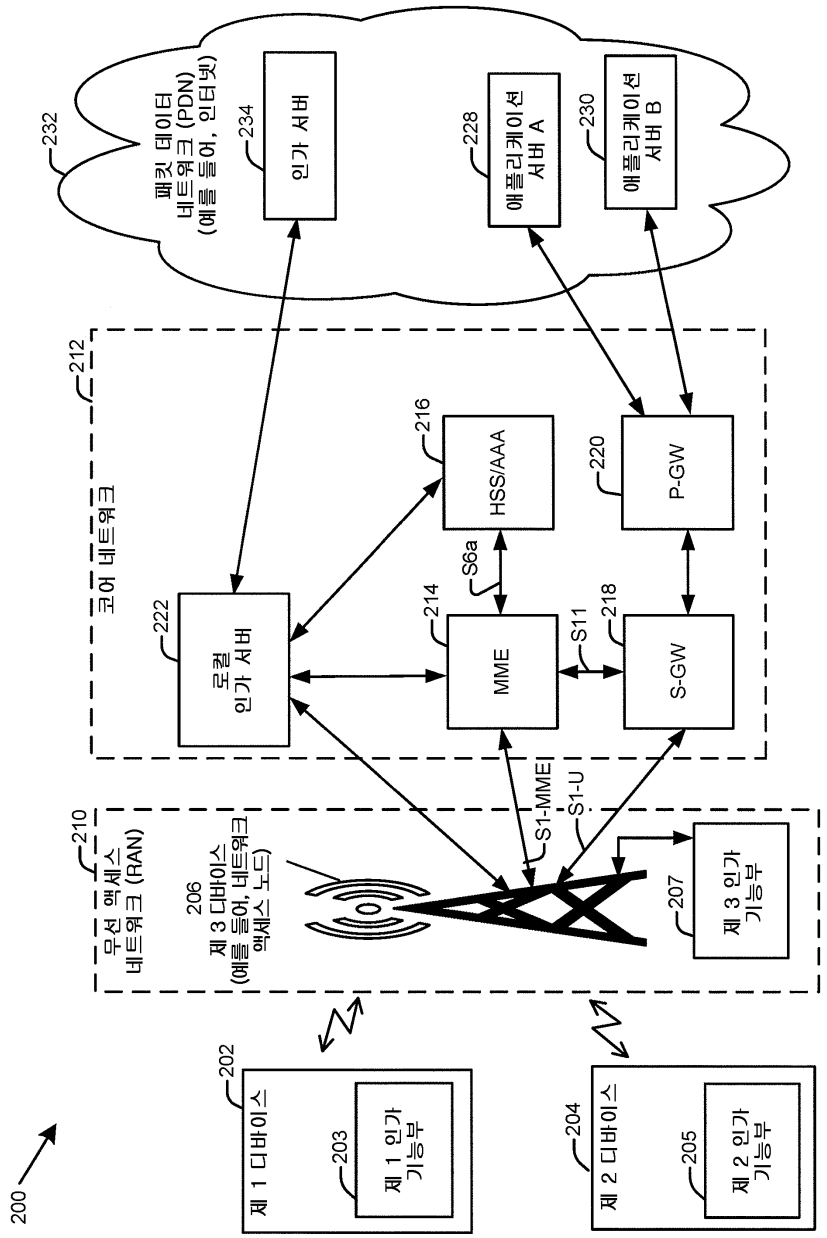
[0299] 본원에 설명된 개시물의 다양한 피처들은 본 개시물로부터 벗어남 없이 상이한 시스템들에서 구현될 수 있다. 상기의 양태들은 단지 예들이며 본 개시물을 제한하는 것으로서 해석되지 않아야 한다. 본 개시물의 교시들의 예들의 설명들은 예시적인 것으로 의도되고, 청구항의 범위를 제한하지 않는다. 이와 같이, 본 교시들은 다른 유형들의 장치들에 용이하게 적용될 수 있고, 많은 대안들, 수정들, 및 변형들이 당업자에게 명백할 것이다.

도면

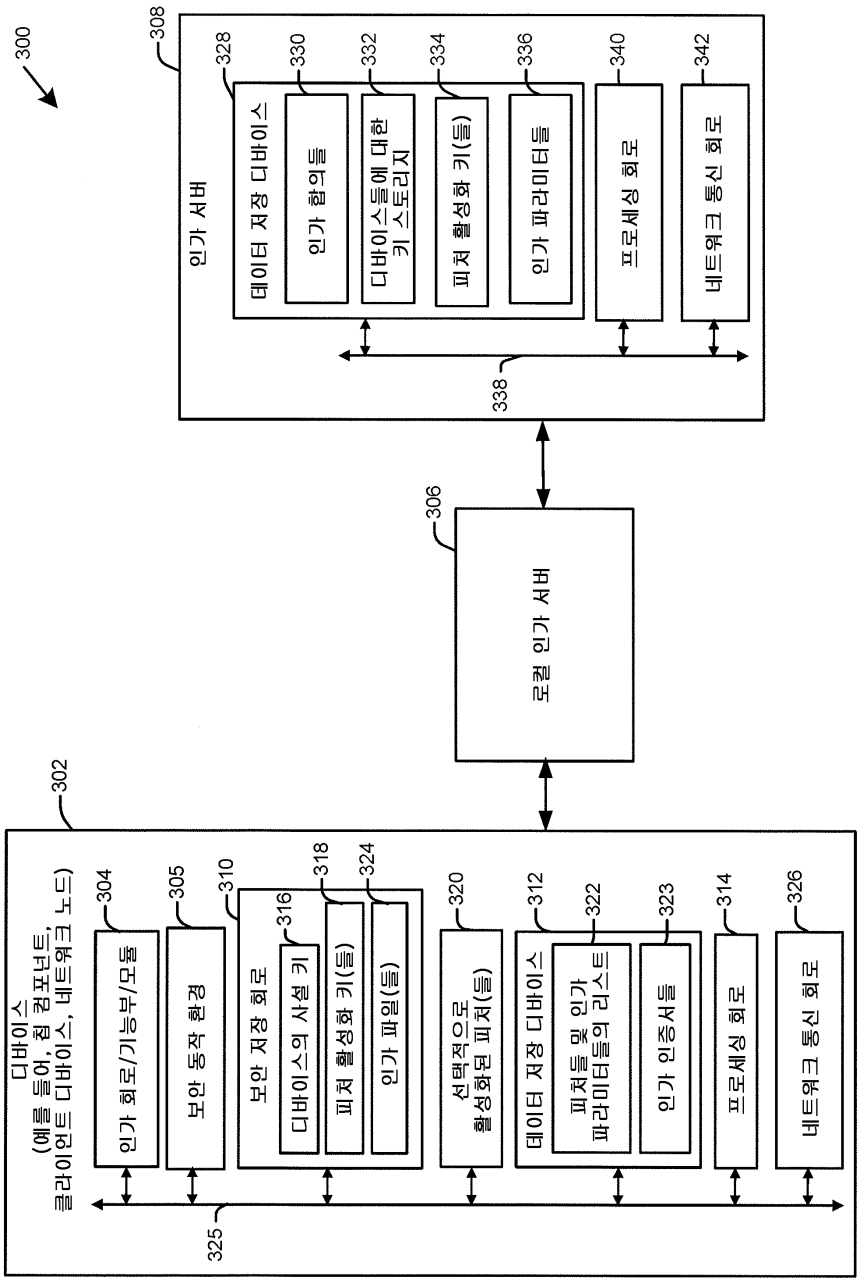
도면1



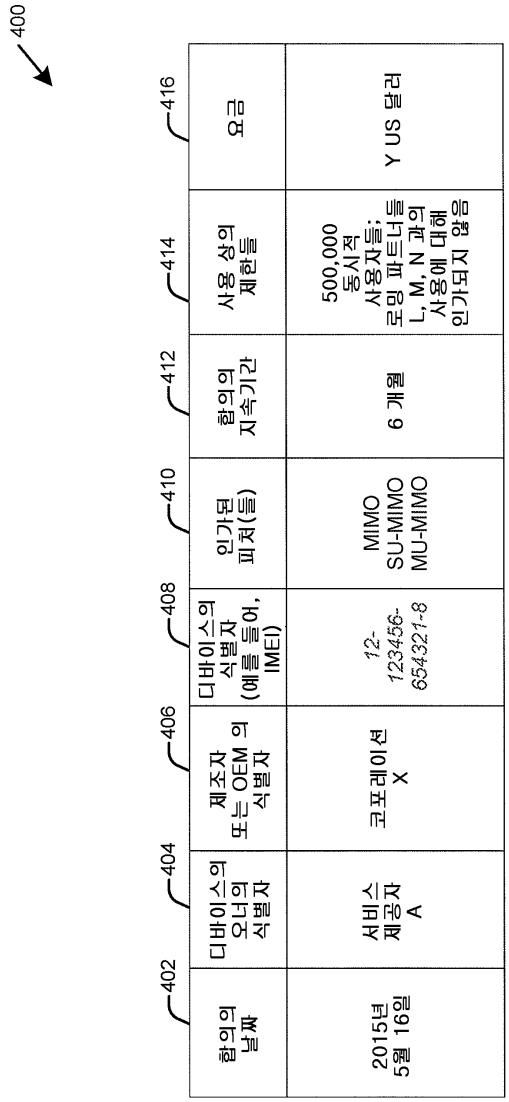
도면2


200
202
제 1 디바이스
203
제 1 인가 기능부
204
제 2 디바이스
205
제 2 인가 기능부
206
제 3 디바이스 (예를 들어, 네트워크 액세스 노드)
207
제 3 인가 기능부
210
무선 액세스 네트워크 (RAN)
212
코어 네트워크
214
MME
216
HSS/AAA
218
S-GW
220
P-GW
222
로컬 인가 서버
228
애플리케이션 서버 A
230
애플리케이션 서버 B
232
패킷 데이터 네트워크 (PDN) (예를 들어, 인터넷)
234
인가 서버
S1-MME
S1-U
S11
S6a

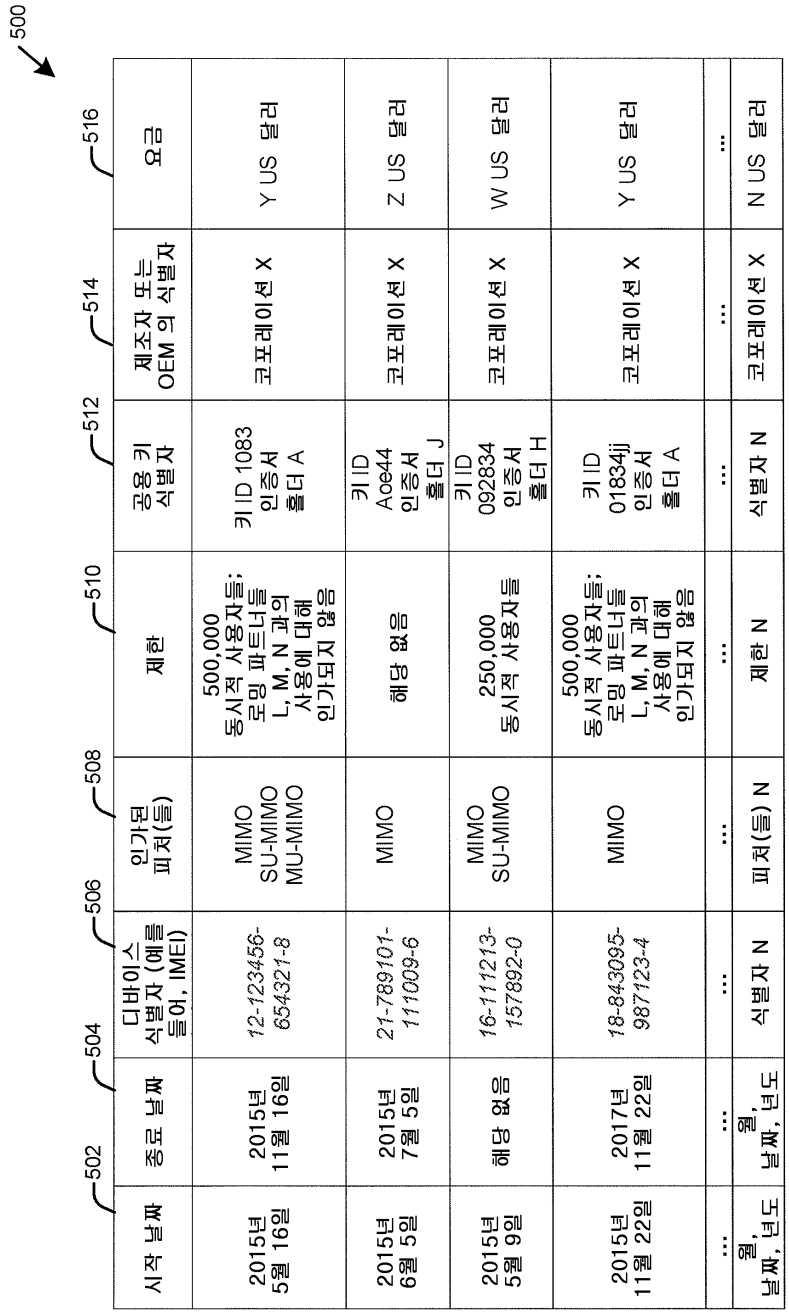
도면3


300
308
인가 서버
328
데이터 저장 디바이스
330
인가 합의들
332
디바이스들에 대한 키 스토리지
334
피처 활성화 키(들)
336
인가 파라미터들
340
프로세싱 회로
342
네트워크 통신 회로
338
306
로컬 인가 서버
302
디바이스 (예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드)
304
인가 회로/기능부/모듈
305
보안 동작 환경
310
보안 저장 회로
316
디바이스의 사설 키
318
피처 활성화 키(들)
324
인가 파일(들)
320
선택적으로 활성화된 피처(들)
312
데이터 저장 디바이스
322
피처들 및 인가 파라미터들의 리스트
323
인가 인증서들
314
프로세싱 회로
326
네트워크 통신 회로
325

도면4

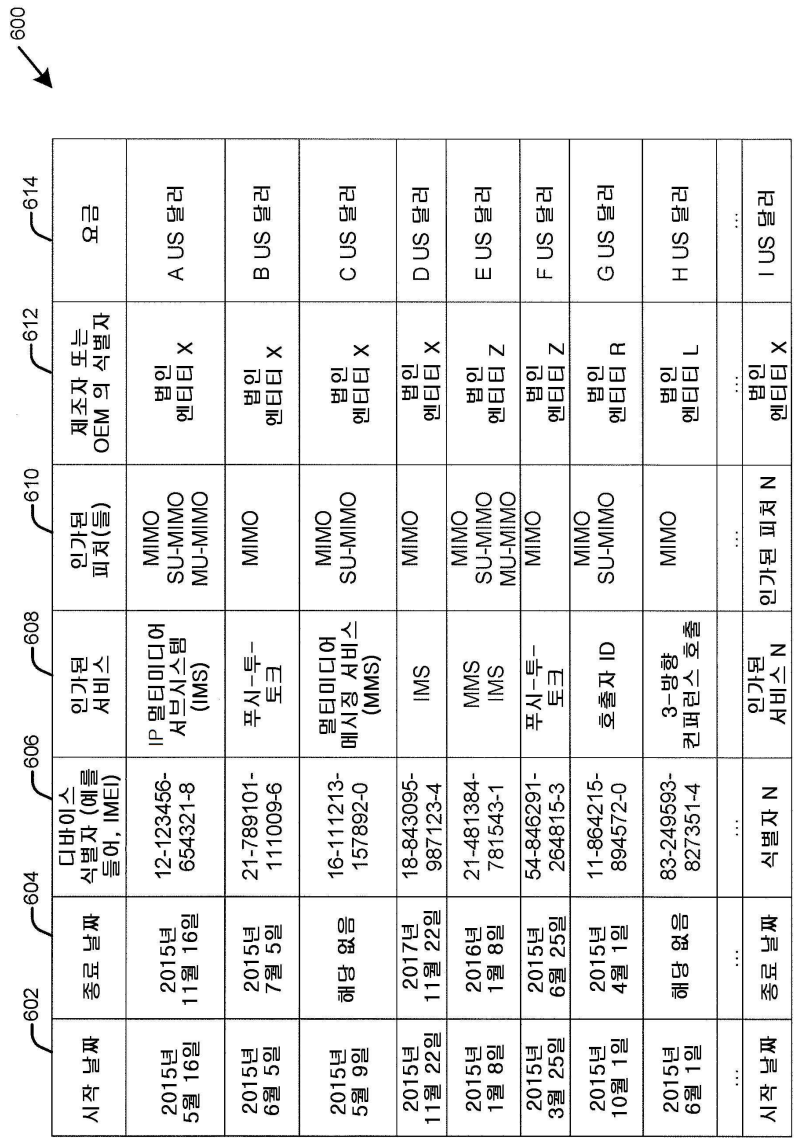

400
402
404
406
408
410
412
414
416
합의의 날짜
디바이스의 오너의 식별자
제조자 또는 OEM 의 식별자
디바이스의 식별자 (예를 들어, IMEI)
인가된 피처(들)
합의의 지속기간
사용 상의 제한들
요금
2015년 5월 16일
서비스 제공자 A
코포레이션 X
12-123456-654321-8
MIMO SU-MIMO MU-MIMO
6 개월
500,000 동시적 사용자들; 로밍 파트너들 L, M, N 과의 사용에 대해 인가되지 않음
Y US 달러

도면5



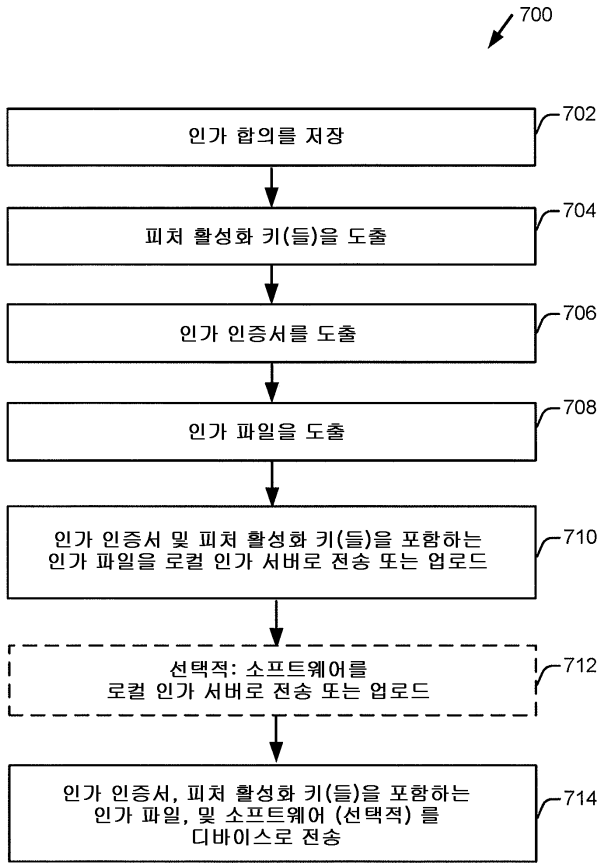
시작 날짜	종료 날짜	디바이스 식별자 (예를 들어, IMEI)	인가된 피처(들)	제한	공용 키 식별자	제조자 또는 OEM 의 식별자	요금
2015년 5월 16일	2015년 11월 16일	*12-123456-654321-8*	MIMO SU-MIMO MU-MIMO	500,000 동시적 사용자들; 로밍 파트너들 L, M, N 과의 사용에 대해 인가되지 않음	키 ID 1083 인증서 홀더 A	코포레이션 X	Y US 달러
2015년 6월 5일	2015년 7월 5일	*21-789101-111009-6*	MIMO	해당 없음	키 ID Aoe44 인증서 홀더 J	코포레이션 X	Z US 달러
2015년 5월 9일	해당 없음	*16-111213-157892-0*	MIMO SU-MIMO	250,000 동시적 사용자들	키 ID 092834 인증서 홀더 H	코포레이션 X	W US 달러
2015년 11월 22일	2017년 11월 22일	*18-843095-987123-4*	MIMO	500,000 동시적 사용자들; 로밍 파트너들 L, M, N 과의 사용에 대해 인가되지 않음	키 ID 01834jj 인증서 홀더 A	코포레이션 X	Y US 달러
...	...	...	...	...	...	...	...
월, 날짜, 년도	월, 날짜, 년도	식별자 N	피처(들) N	제한 N	식별자 N	코포레이션 X	N US 달러

도면6

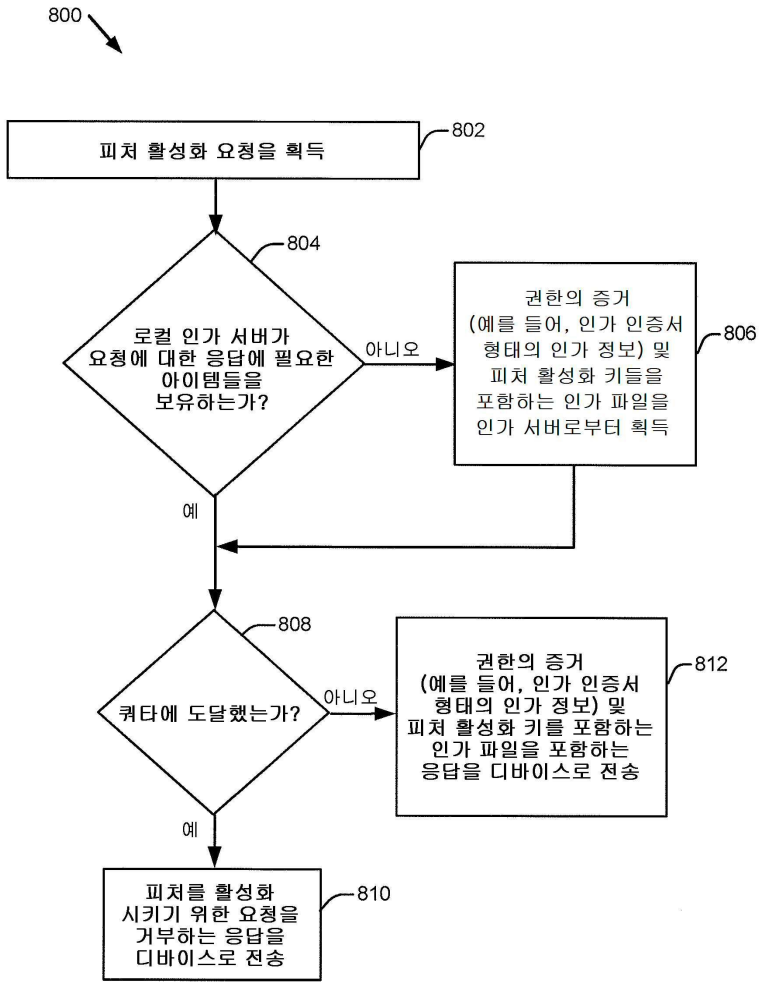


시작 날짜	종료 날짜	디바이스 식별자 (예를 들어, IMEI)	인가된 서비스	인가된 피처(들)	제조자 또는 OEM 의 식별자	요금
2015년 5월 16일	2015년 11월 16일	12-123456-654321-8	IP 멀티미디어 서브시스템 (IMS)	MIMO SU-MIMO MU-MIMO	법인 엔티티 X	A US 달러
2015년 6월 5일	2015년 7월 5일	21-789101-111009-6	푸시-투-토크	MIMO	법인 엔티티 X	B US 달러
2015년 5월 9일	해당 없음	16-111213-157892-0	멀티미디어 메시징 서비스 (MMS)	MIMO SU-MIMO	법인 엔티티 X	C US 달러
2015년 11월 22일	2017년 11월 22일	18-843095-987123-4	IMS	MIMO	법인 엔티티 X	D US 달러
2015년 1월 8일	2016년 1월 8일	21-481384-781543-1	MMS IMS	MIMO SU-MIMO MU-MIMO	법인 엔티티 Z	E US 달러
2015년 3월 25일	2015년 6월 25일	54-846291-264815-3	푸시-투-토크	MIMO	법인 엔티티 Z	F US 달러
2015년 10월 1일	2015년 4월 1일	11-864215-894572-0	호출자 ID	MIMO SU-MIMO	법인 엔티티 R	G US 달러
2015년 6월 1일	해당 없음	83-249593-827351-4	3-방향 컨퍼런스 호출	MIMO	법인 엔티티 L	H US 달러
...	...	...	...	...	...	...
시작 날짜	종료 날짜	식별자 N	인가된 서비스 N	인가된 피처 N	법인 엔티티 X	I US 달러

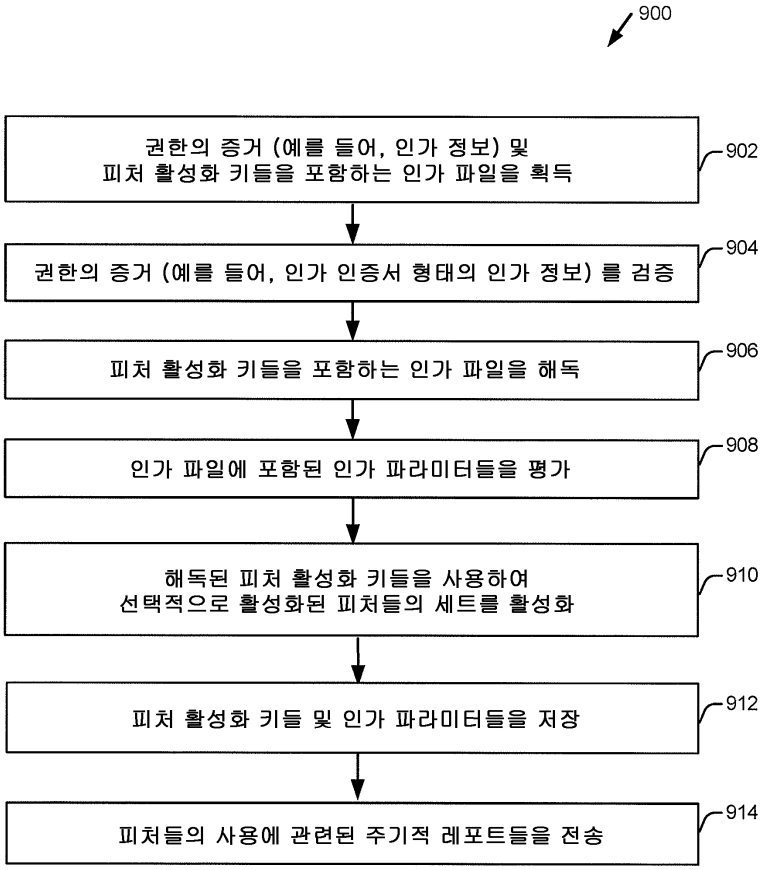
도면7


700
인가 합의를 저장
702
피처 활성화 키(들)을 도출
704
인가 인증서를 도출
706
인가 파일을 도출
708
인가 인증서 및 피처 활성화 키(들)을 포함하는
인가 파일을 로컬 인가 서버로 전송 또는 업로드
710
선택적: 소프트웨어를
로컬 인가 서버로 전송 또는 업로드
712
인가 인증서, 피처 활성화 키(들)을 포함하는
인가 파일, 및 소프트웨어 (선택적) 를
디바이스로 전송
714

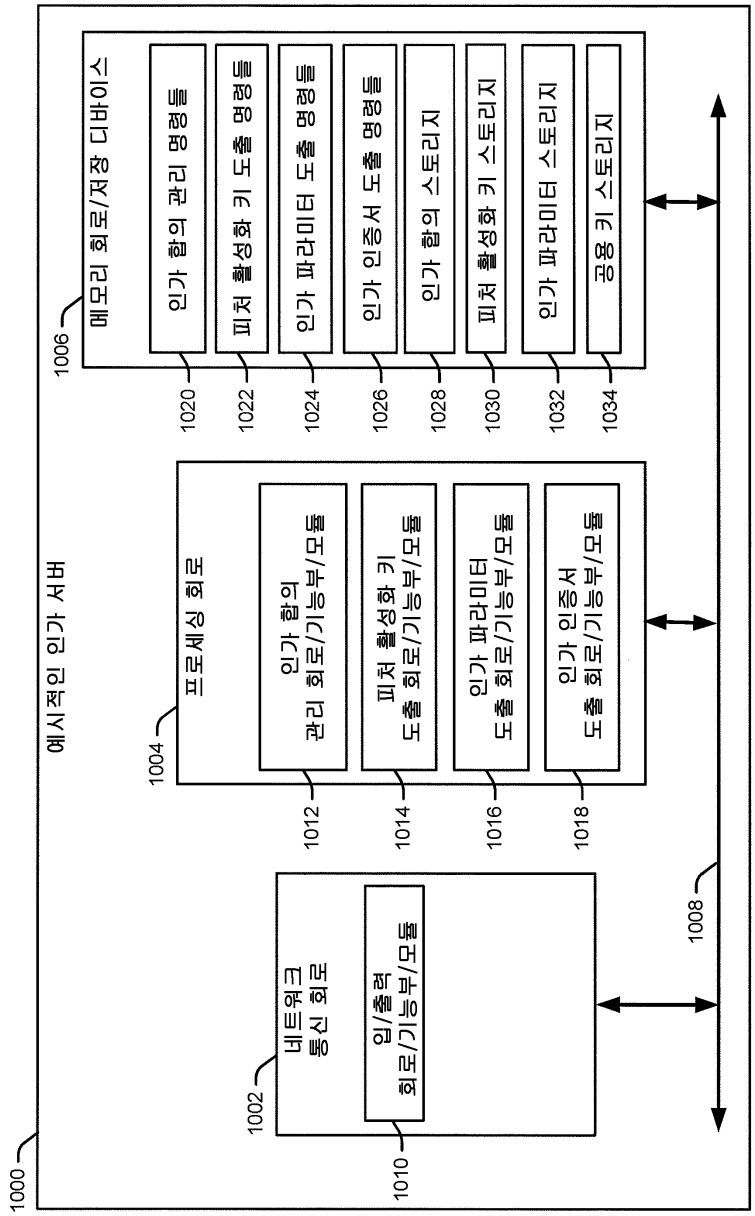
도면8


800
피처 활성화 요청을 획득
802
804
로컬 인가 서버가 요청에 대한 응답에 필요한 아이템들을 보유하는가?
아니오
권한의 증거 (예를 들어, 인가 인증서 형태의 인가 정보) 및 피처 활성화 키들을 포함하는 인가 파일을 인가 서버로부터 획득
806
예
808
큐타에 도달했는가?
아니오
권한의 증거 (예를 들어, 인가 인증서 형태의 인가 정보) 및 피처 활성화 키를 포함하는 인가 파일을 포함하는 응답을 디바이스로 전송
812
예
피처를 활성화 시키기 위한 요청을 거부하는 응답을 디바이스로 전송
810

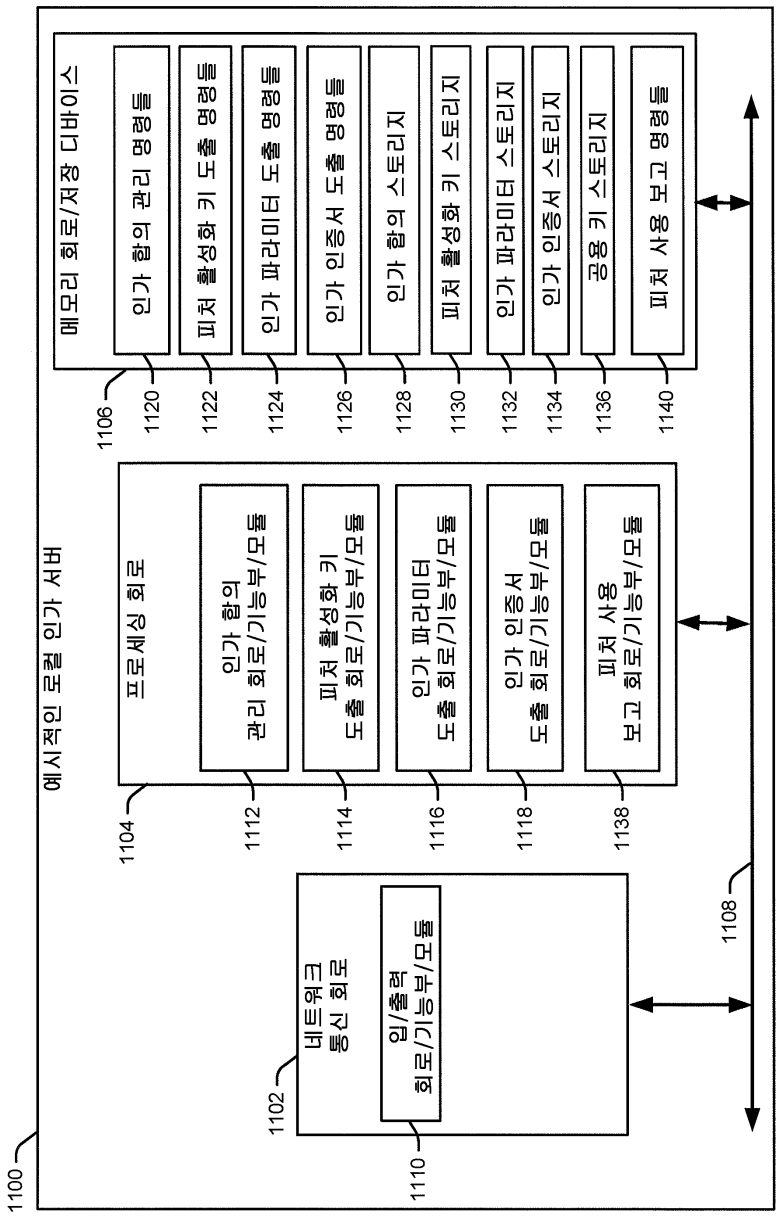
도면9


900
권한의 증거 (예를 들어, 인가 정보) 및
피처 활성화 키들을 포함하는 인가 파일을 획득
902
권한의 증거 (예를 들어, 인가 인증서 형태의 인가 정보) 를 검증
904
피처 활성화 키들을 포함하는 인가 파일을 해독
906
인가 파일에 포함된 인가 파라미터들을 평가
908
해독된 피처 활성화 키들을 사용하여
선택적으로 활성화된 피처들의 세트를 활성화
910
피처 활성화 키들 및 인가 파라미터들을 저장
912
피처들의 사용에 관련된 주기적 레포트들을 전송
914

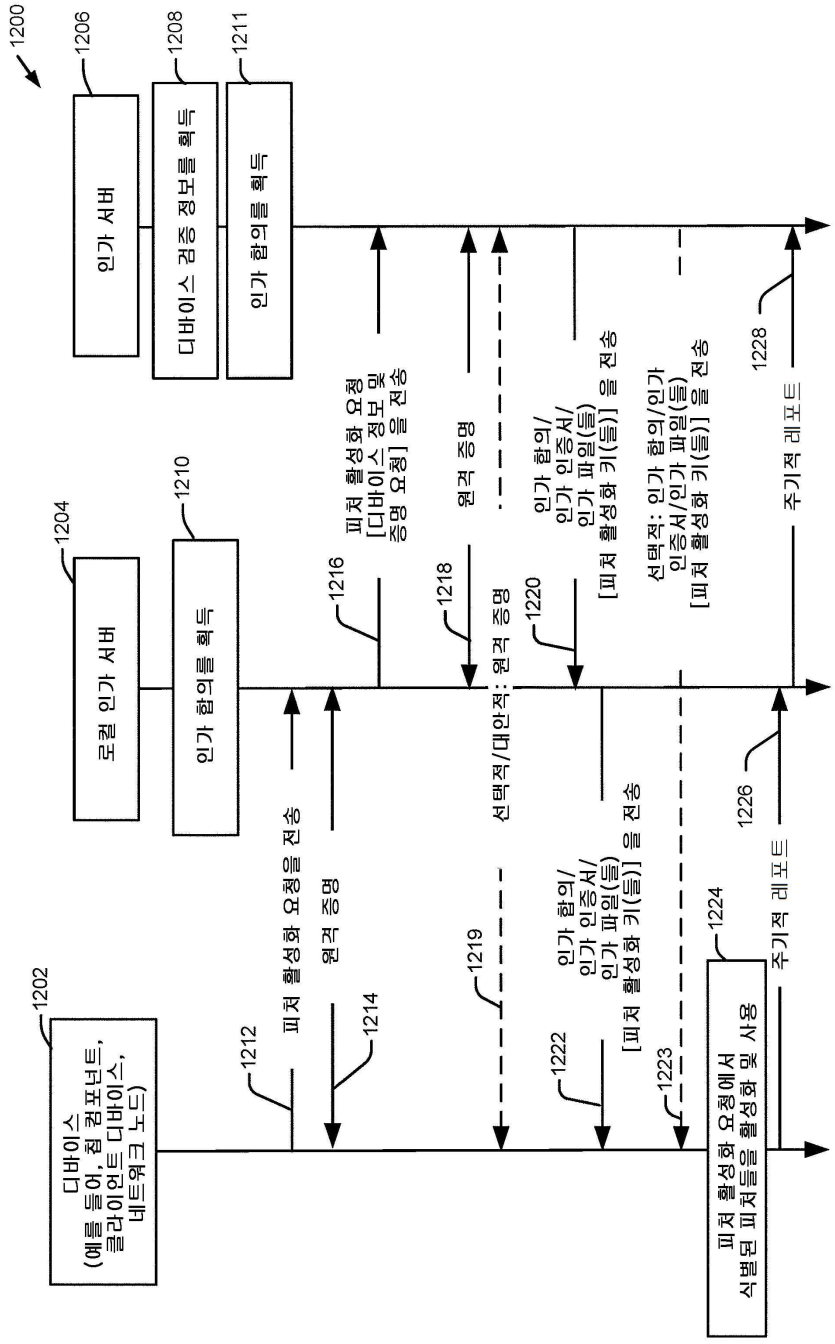
도면10


예시적인 인가 서버
1000
네트워크 통신 회로
1002
입/출력 회로/기능부/모듈
1010
프로세싱 회로
1004
인가 합의 관리 회로/기능부/모듈
1012
피처 활성화 키 도출 회로/기능부/모듈
1014
인가 파라미터 도출 회로/기능부/모듈
1016
인가 인증서 도출 회로/기능부/모듈
1018
1008
메모리 회로/저장 디바이스
1006
인가 합의 관리 명령들
1020
피처 활성화 키 도출 명령들
1022
인가 파라미터 도출 명령들
1024
인가 인증서 도출 명령들
1026
인가 합의 스토리지
1028
피처 활성화 키 스토리지
1030
인가 파라미터 스토리지
1032
공용 키 스토리지
1034

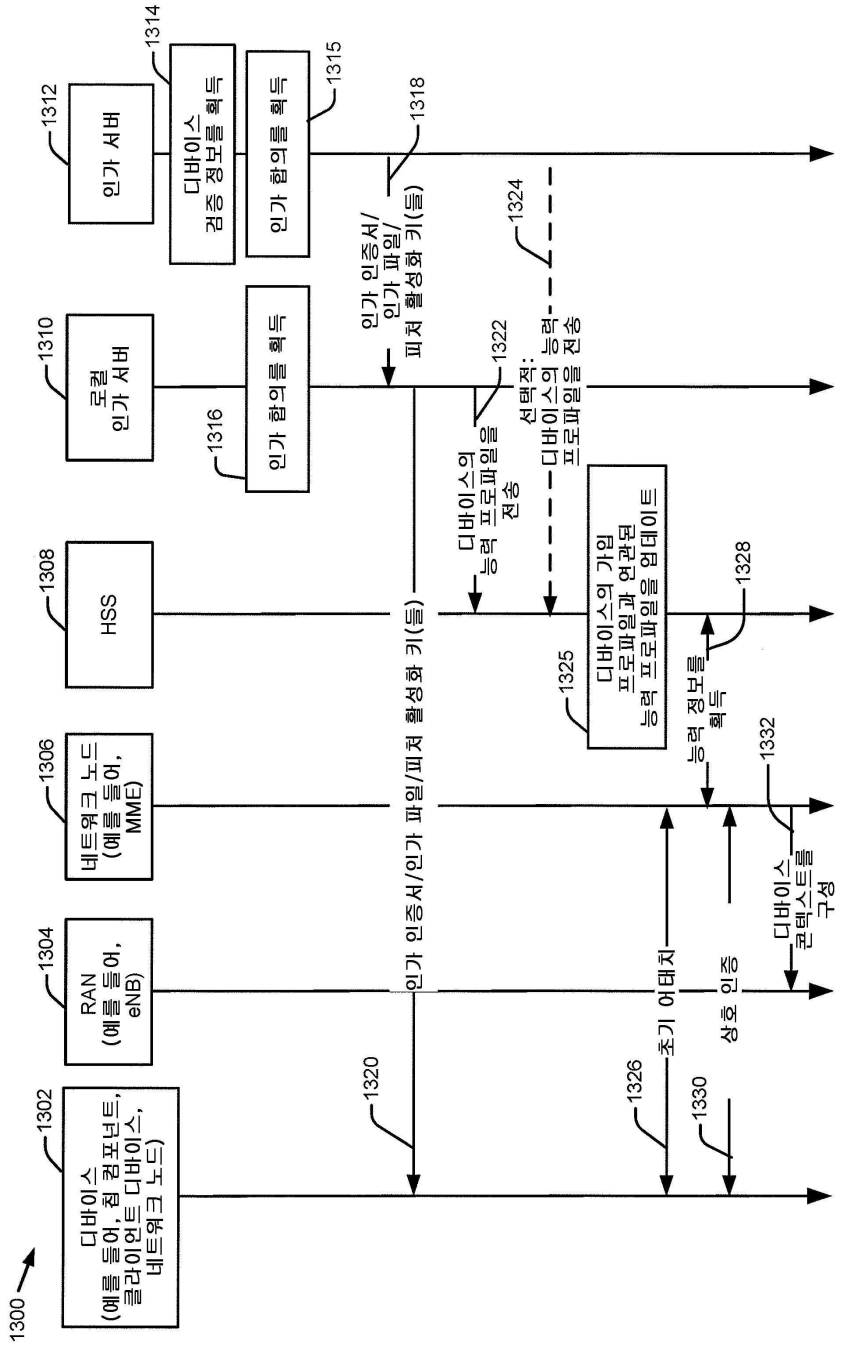
도면11


예시적인 로컬 인가 서버
1100
메모리 회로/저장 디바이스
1106
인가 합의 관리 명령들
1120
피처 활성화 키 도출 명령들
1122
인가 파라미터 도출 명령들
1124
인가 인증서 도출 명령들
1126
인가 합의 스토리지
1128
피처 활성화 키 스토리지
1130
인가 파라미터 스토리지
1132
인가 인증서 스토리지
1134
공용 키 스토리지
1136
피처 사용 보고 명령들
1140
프로세싱 회로
1104
인가 합의
관리 회로/기능부/모듈
1112
피처 활성화 키
도출 회로/기능부/모듈
1114
인가 파라미터
도출 회로/기능부/모듈
1116
인가 인증서
도출 회로/기능부/모듈
1118
피처 사용
보고 회로/기능부/모듈
1138
네트워크
통신 회로
1102
입/출력
회로/기능부/모듈
1110
1108

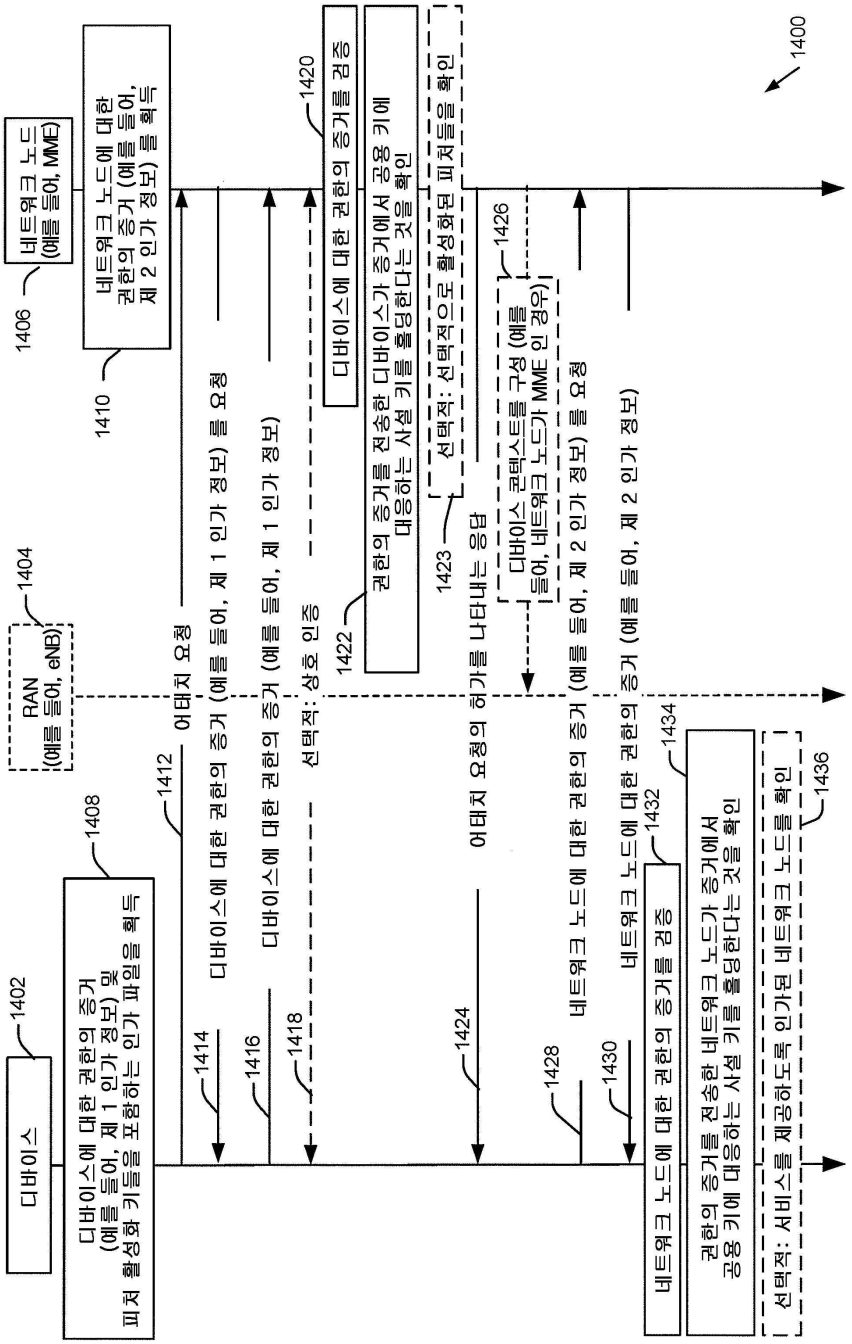
도면12


1200
1206
인가 서버
1208
디바이스 검증 정보를 획득
1211
인가 합의를 획득
1204
로컬 인가 서버
1210
인가 합의를 획득
1216
피처 활성화 요청
[디바이스 정보 및
증명 요청] 을 전송
1218
원격 증명
1220
인가 합의/
인가 인증서/
인가 파일(들)
[피처 활성화 키(들)] 을 전송
선택적: 인가 합의/인가
인증서/인가 파일(들)
[피처 활성화 키(들)] 을 전송
1228
주기적 레포트
1202
디바이스
(예를 들어, 칩 컴포넌트,
클라이언트 디바이스,
네트워크 노드)
1212
피처 활성화 요청을 전송
1214
원격 증명
1219
선택적/대안적: 원격 증명
1222
인가 합의/
인가 인증서/
인가 파일(들)
[피처 활성화 키(들)] 을 전송
1223
1226
주기적 레포트
1224
피처 활성화 요청에서
식별된 피처들을 활성화 및 사용

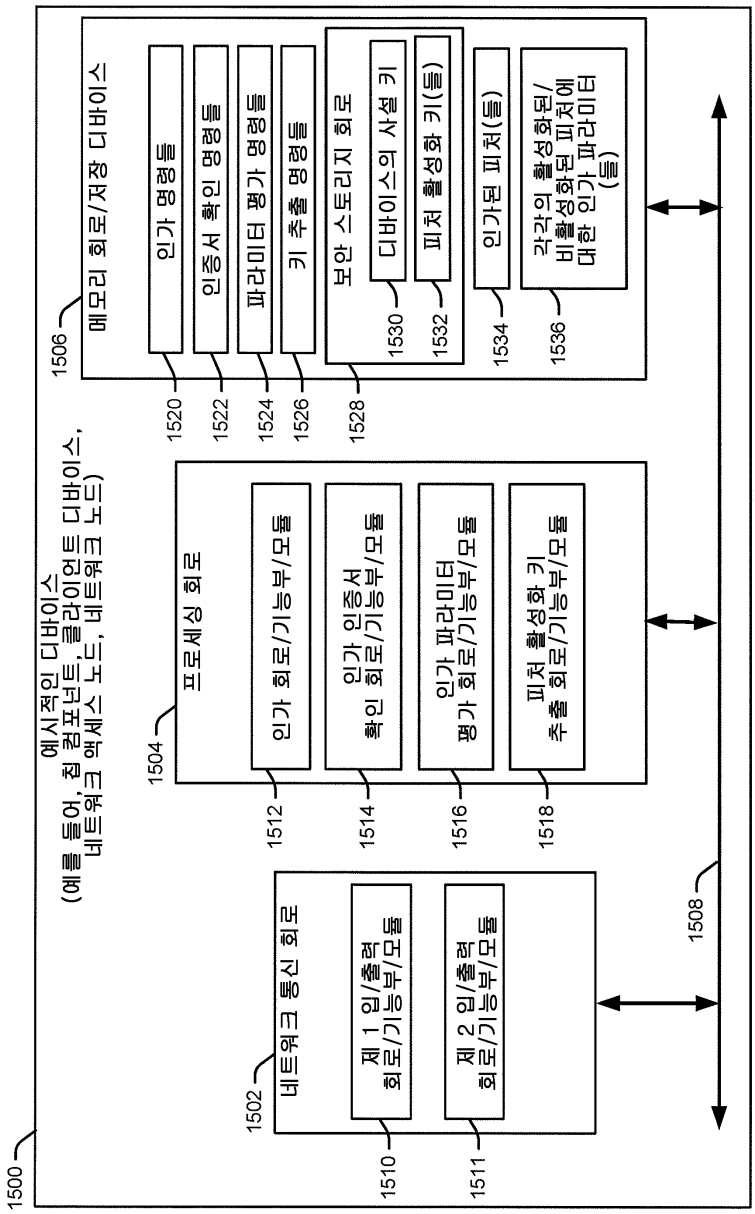
도면13


1300
디바이스
(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 노드)
1302
RAN
(예를 들어, eNB)
1304
네트워크 노드
(예를 들어, MME)
1306
HSS
1308
로컬
인가 서버
1310
인가 서버
1312
디바이스
검증 정보를 획득
1314
인가 합의를 획득
1315
인가 합의를 획득
1316
인가 인증서/
인가 파일/
피처 활성화 키(들)
1318
디바이스의
능력 프로파일을
전송
1322
선택적:
디바이스의 능력
프로파일을 전송
1324
디바이스의 가입
프로파일과 연관된
능력 프로파일을 업데이트
1325
능력 정보를
획득
1328
디바이스
콘텍스트를
구성
1332
인가 인증서/인가 파일/피처 활성화 키(들)
1320
초기 어태치
상호 인증
1326
1330

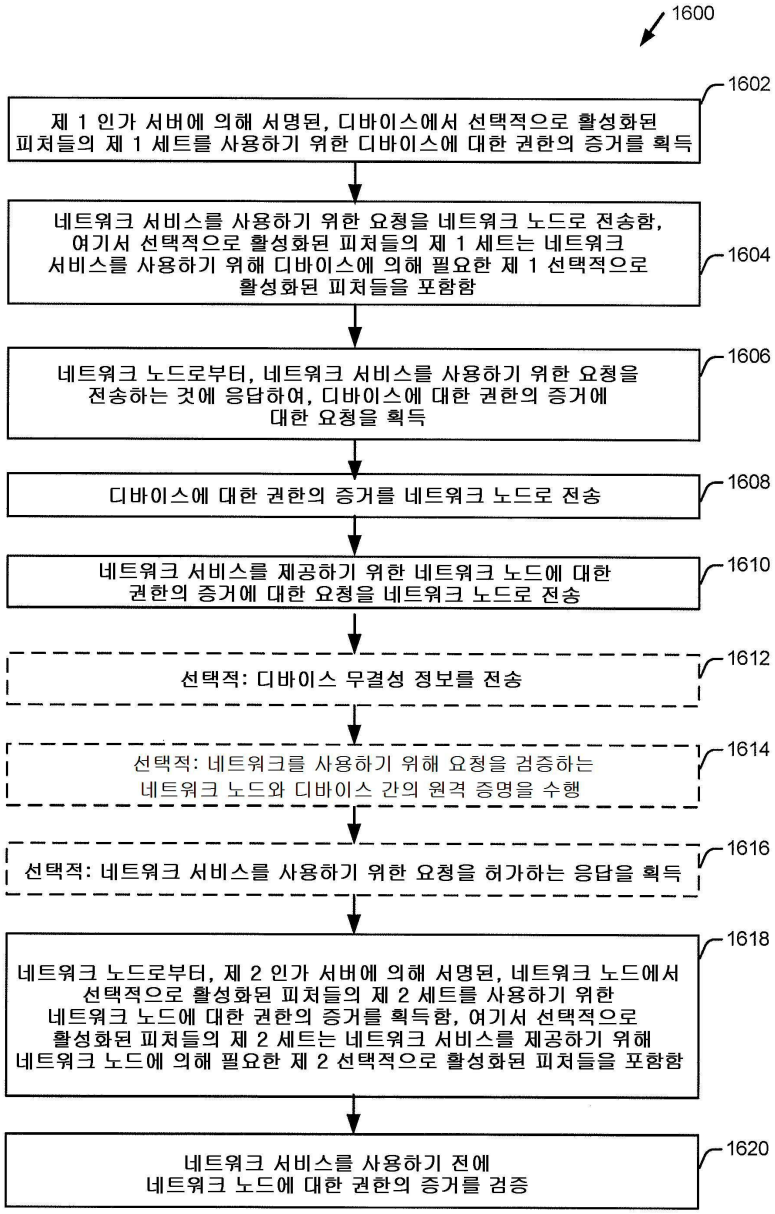
도면14


1400
디바이스
1402
디바이스에 대한 권한의 증거
(예를 들어, 제 1 인가 정보) 및
피처 활성화 키들을 포함하는 인가 파일을 획득
1408
RAN
(예를 들어, eNB)
1404
네트워크 노드
(예를 들어, MME)
1406
네트워크 노드에 대한
권한의 증거 (예를 들어,
제 2 인가 정보) 를 획득
1410
어태치 요청
1412
디바이스에 대한 권한의 증거 (예를 들어, 제 1 인가 정보) 를 요청
1414
디바이스에 대한 권한의 증거 (예를 들어, 제 1 인가 정보)
1416
선택적: 상호 인증
1418
디바이스에 대한 권한의 증거를 검증
1420
권한의 증거를 전송한 디바이스가 증거에서 공용 키에
대응하는 사설 키를 홀딩한다는 것을 확인
1422
선택적: 선택적으로 활성화된 피처들을 확인
1423
어태치 요청의 허가를 나타내는 응답
1424
디바이스 콘텍스트를 구성 (예를
들어, 네트워크 노드가 MME 인 경우)
1426
네트워크 노드에 대한 권한의 증거 (예를 들어, 제 2 인가 정보) 를 요청
1428
네트워크 노드에 대한 권한의 증거 (예를 들어, 제 2 인가 정보)
1430
네트워크 노드에 대한 권한의 증거를 검증
1432
권한의 증거를 전송한 네트워크 노드가 증거에서
공용 키에 대응하는 사설 키를 홀딩한다는 것을 확인
1434
선택적: 서비스를 제공하도록 인가된 네트워크 노드를 확인
1436

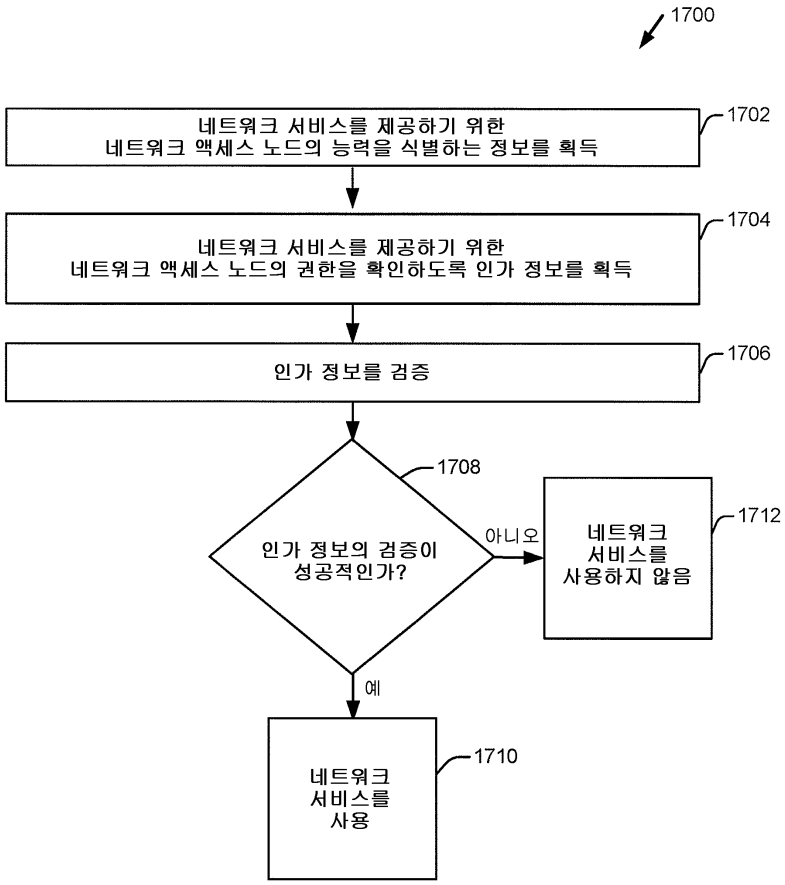
도면15


1500
예시적인 디바이스
(예를 들어, 칩 컴포넌트, 클라이언트 디바이스, 네트워크 액세스 노드, 네트워크 노드)
1502
네트워크 통신 회로
1510
제 1 입/출력 회로/기능부/모듈
1511
제 2 입/출력 회로/기능부/모듈
1504
프로세싱 회로
1512
인가 회로/기능부/모듈
1514
인가 인증서 확인 회로/기능부/모듈
1516
인가 파라미터 평가 회로/기능부/모듈
1518
피처 활성화 키 추출 회로/기능부/모듈
1508
1506
메모리 회로/저장 디바이스
1520
인가 명령들
1522
인증서 확인 명령들
1524
파라미터 평가 명령들
1526
키 추출 명령들
1528
보안 스토리지 회로
1530
디바이스의 사설 키
1532
피처 활성화 키(들)
1534
인가된 피처(들)
1536
각각의 활성화된/비활성화된 피처에 대한 인가 파라미터(들)

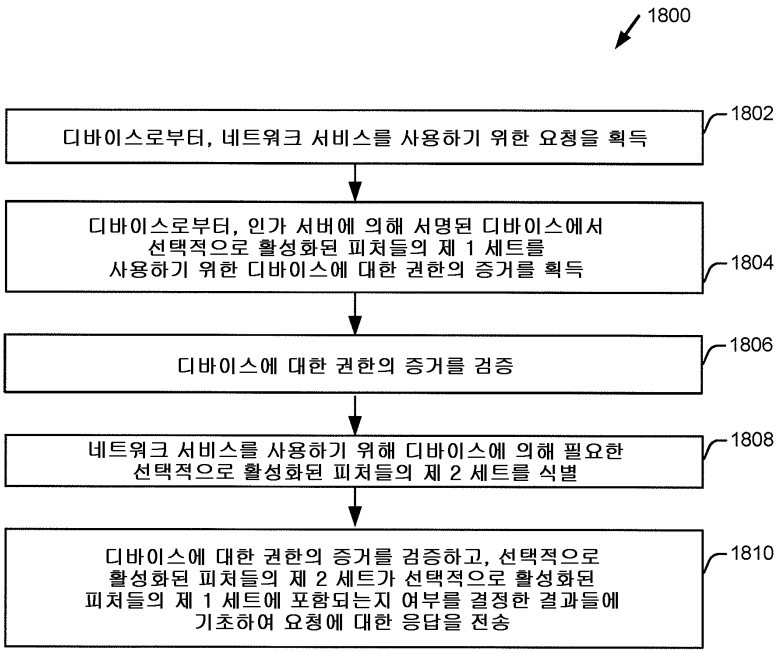
도면16


1600
1602
제 1 인가 서버에 의해 서명된, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 획득
1604
네트워크 서비스를 사용하기 위한 요청을 네트워크 노드로 전송함, 여기서 선택적으로 활성화된 피처들의 제 1 세트는 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 제 1 선택적으로 활성화된 피처들을 포함함
1606
네트워크 노드로부터, 네트워크 서비스를 사용하기 위한 요청을 전송하는 것에 응답하여, 디바이스에 대한 권한의 증거에 대한 요청을 획득
1608
디바이스에 대한 권한의 증거를 네트워크 노드로 전송
1610
네트워크 서비스를 제공하기 위한 네트워크 노드에 대한 권한의 증거에 대한 요청을 네트워크 노드로 전송
1612
선택적: 디바이스 무결성 정보를 전송
1614
선택적: 네트워크를 사용하기 위해 요청을 검증하는 네트워크 노드와 디바이스 간의 원격 증명을 수행
1616
선택적: 네트워크 서비스를 사용하기 위한 요청을 허가하는 응답을 획득
1618
네트워크 노드로부터, 제 2 인가 서버에 의해 서명된, 네트워크 노드에서 선택적으로 활성화된 피처들의 제 2 세트를 사용하기 위한 네트워크 노드에 대한 권한의 증거를 획득함, 여기서 선택적으로 활성화된 피처들의 제 2 세트는 네트워크 서비스를 제공하기 위해 네트워크 노드에 의해 필요한 제 2 선택적으로 활성화된 피처들을 포함함
1620
네트워크 서비스를 사용하기 전에 네트워크 노드에 대한 권한의 증거를 검증

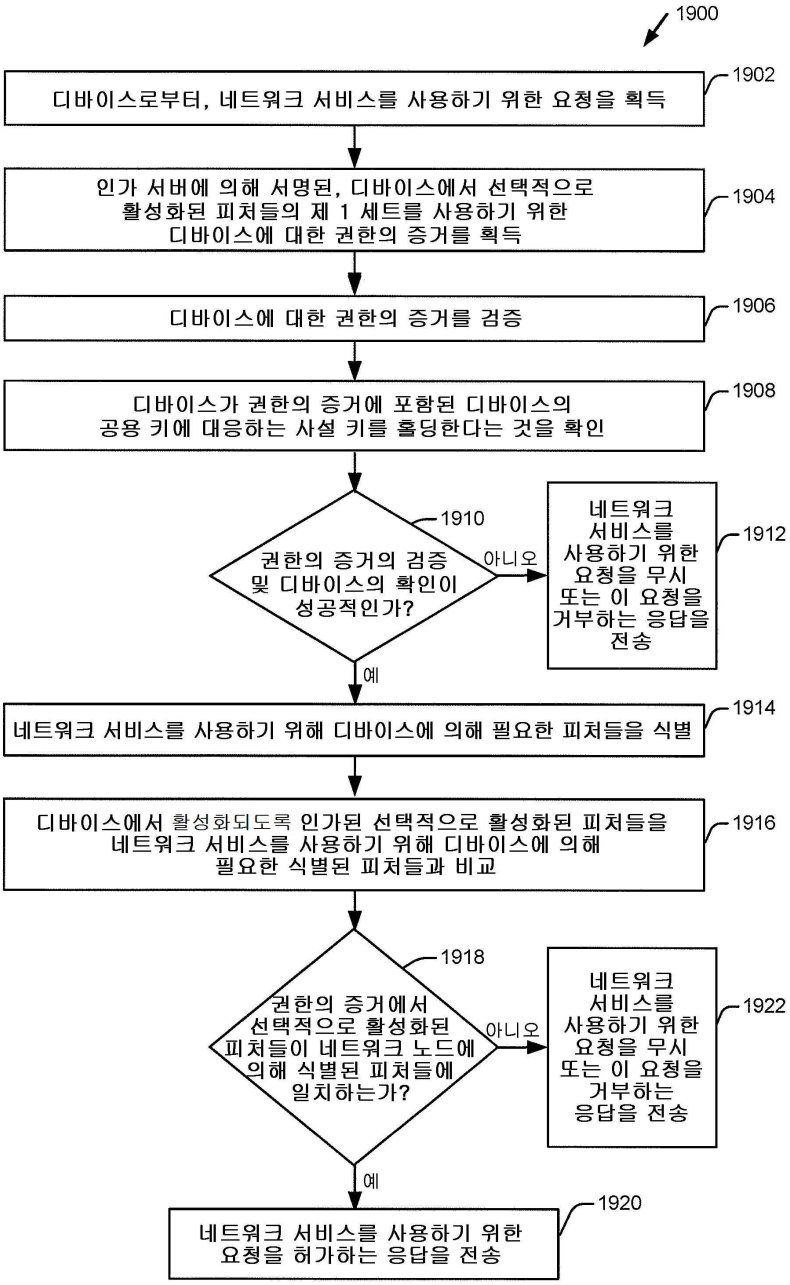
도면17


1700
네트워크 서비스를 제공하기 위한
네트워크 액세스 노드의 능력을 식별하는 정보를 획득
1702
네트워크 서비스를 제공하기 위한
네트워크 액세스 노드의 권한을 확인하도록 인가 정보를 획득
1704
인가 정보를 검증
1706
1708
인가 정보의 검증이
성공적인가?
아니오
네트워크
서비스를
사용하지 않음
1712
예
네트워크
서비스를
사용
1710

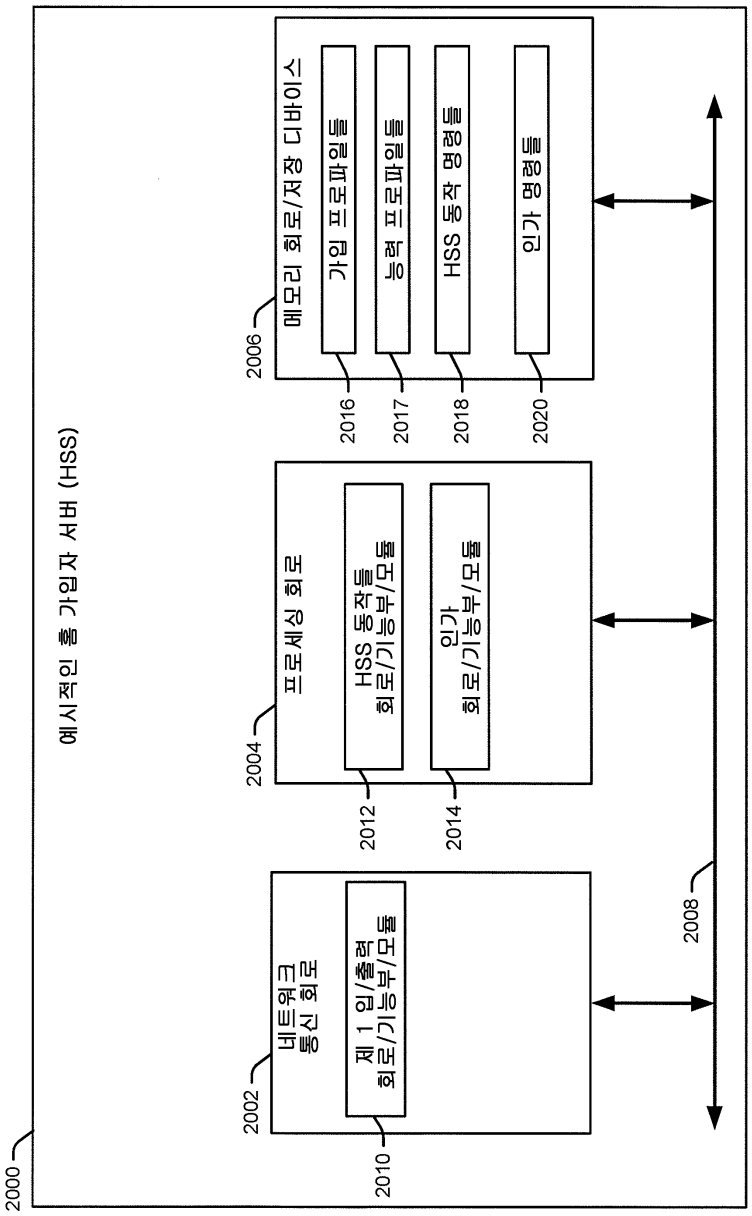
도면18


1800
디바이스로부터, 네트워크 서비스를 사용하기 위한 요청을 획득
1802
디바이스로부터, 인가 서버에 의해 서명된 디바이스에서
선택적으로 활성화된 피처들의 제 1 세트를
사용하기 위한 디바이스에 대한 권한의 증거를 획득
1804
디바이스에 대한 권한의 증거를 검증
1806
네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한
선택적으로 활성화된 피처들의 제 2 세트를 식별
1808
디바이스에 대한 권한의 증거를 검증하고, 선택적으로
활성화된 피처들의 제 2 세트가 선택적으로 활성화된
피처들의 제 1 세트에 포함되는지 여부를 결정한 결과들에
기초하여 요청에 대한 응답을 전송
1810

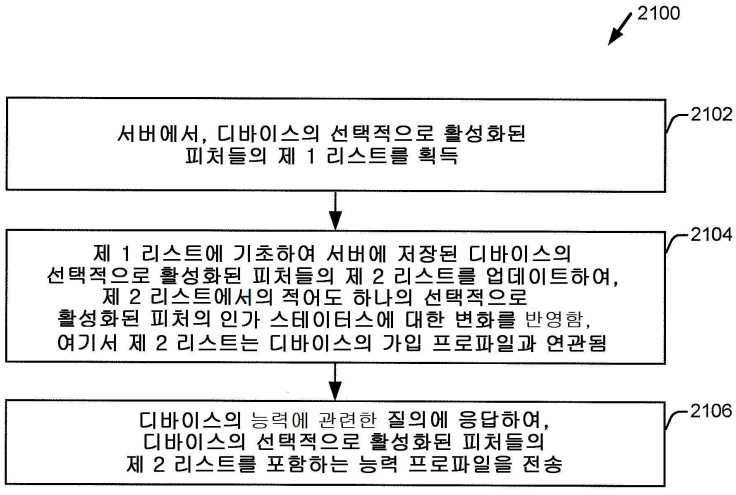
도면19


1900
디바이스로부터, 네트워크 서비스를 사용하기 위한 요청을 획득
1902
인가 서버에 의해 서명된, 디바이스에서 선택적으로 활성화된 피처들의 제 1 세트를 사용하기 위한 디바이스에 대한 권한의 증거를 획득
1904
디바이스에 대한 권한의 증거를 검증
1906
디바이스가 권한의 증거에 포함된 디바이스의 공용 키에 대응하는 사설 키를 홀딩한다는 것을 확인
1908
권한의 증거의 검증 및 디바이스의 확인이 성공적인가?
1910
아니오
네트워크 서비스를 사용하기 위한 요청을 무시 또는 이 요청을 거부하는 응답을 전송
1912
예
네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 피처들을 식별
1914
디바이스에서 활성화되도록 인가된 선택적으로 활성화된 피처들을 네트워크 서비스를 사용하기 위해 디바이스에 의해 필요한 식별된 피처들과 비교
1916
권한의 증거에서 선택적으로 활성화된 피처들이 네트워크 노드에 의해 식별된 피처들에 일치하는가?
1918
아니오
네트워크 서비스를 사용하기 위한 요청을 무시 또는 이 요청을 거부하는 응답을 전송
1922
예
네트워크 서비스를 사용하기 위한 요청을 허가하는 응답을 전송
1920

도면20


예시적인 홈 가입자 서버 (HSS)
2000
네트워크 통신 회로
2002
제 1 입/출력 회로/기능부/모듈
2010
프로세싱 회로
2004
HSS 동작들 회로/기능부/모듈
2012
인가 회로/기능부/모듈
2014
메모리 회로/저장 디바이스
2006
가입 프로파일들
2016
능력 프로파일들
2017
HSS 동작 명령들
2018
인가 명령들
2020
2008

도면21


2100
서버에서, 디바이스의 선택적으로 활성화된 피처들의 제 1 리스트를 획득
2102
제 1 리스트에 기초하여 서버에 저장된 디바이스의 선택적으로 활성화된 피처들의 제 2 리스트를 업데이트하여, 제 2 리스트에서의 적어도 하나의 선택적으로 활성화된 피처의 인가 스테이터스에 대한 변화를 반영함, 여기서 제 2 리스트는 디바이스의 가입 프로파일과 연관됨
2104
디바이스의 능력에 관련한 질의에 응답하여, 디바이스의 선택적으로 활성화된 피처들의 제 2 리스트를 포함하는 능력 프로파일을 전송
2106

【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 1

【변경전】

디바이스에서, 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 제공된 피처들의 제 1 세트의 리스팅을 네트워크 노드로부터 획득하는 단계;

상기 네트워크 서비스를 사용하기 위한 요청을 상기 네트워크 노드로 전송하는 단계;

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 권한의 증거에 대한 요청을 상기 네트워크 노드로 전송하는 단계;

인가 서버에 의해 서명된, 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 제 2 세트의 리스팅을 포함하는, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 상기 권한의 증거를 상기 네트워크 노드로부터 획득하는 단계;

상기 네트워크 노드에 대한 상기 권한의 증거를 검증하는 단계;

상기 네트워크 노드가 상기 네트워크 서비스를 제공하기 위해 피처들의 상기 제 2 세트를 사용하도록 유효하게 인가된 것을 확인하기 위해, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 제공된 피처들의 상기 제 1 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트에 포함되는 것을 확인하는 단계;

상기 디바이스에 의해, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 필요한 피처들의 제 3 세트의 리스팅을 식별하는 단계; 및

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 필요한 피처들의 상기 제 3 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트에 포함되는지 여부를 결정하는 것에 기초하여 상기 네트워크 서비스를 사용하는 단계를 포함하는, 방법.

【변경후】

디바이스에서, 네트워크 서비스를 제공하기 위해 네트워크 노드에 의해 제공된 피처들의 제 1 세트의 리스팅을 네트워크 노드로부터 획득하는 단계;

상기 네트워크 서비스를 사용하기 위한 요청을 상기 네트워크 노드로 전송하는 단계;

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 권한의 증거에 대한 요청을 상기 네트워크 노드로 전송하는 단계;

인가 서버에 의해 서명된, 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 제 2 세트의 리스팅을 포함하는, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 대한 상기 권한의 증거를 상기 네트워크 노드로부터 획득하는 단계;

상기 네트워크 노드에 대한 상기 권한의 증거를 검증하는 단계;

상기 네트워크 노드가 상기 네트워크 서비스를 제공하기 위해 피처들의 상기 제 2 세트를 사용하도록 유효하게 인가된 것을 확인하기 위해, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 제공된 피처들의 상기 제 1 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트에 포함되는 것을 확인하는 단계;

상기 디바이스에 의해, 상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 필요한 피처들의 제 3 세트의 리스팅을 식별하는 단계; 및

상기 네트워크 서비스를 제공하기 위해 상기 네트워크 노드에 의해 필요한 피처들의 상기 제 3 세트가 상기 네트워크 노드에서 활성화되도록 인가된 피처들의 상기 제 2 세트에 포함되는지 여부를 결정하는 것에 기초하여 상기 네트워크 서비스를 사용하는 단계를 포함하는, 방법.