(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년02월05일
(11) 등록번호 10-1229306
(24) 등록일자 2013년01월29일

(51) 국제특허분류(Int. Cl.)
H04W 12/04 (2009.01) *H04W 8/06* (2009.01)
H04W 8/26 (2009.01)
(21) 출원번호 10-2010-7018308
(22) 출원일자(국제) 2009년01월21일
심사청구일자 2010년08월20일
(85) 번역문제출일자 2010년08월18일
(65) 공개번호 10-2010-0113577
(43) 공개일자 2010년10월21일
(86) 국제출원번호 PCT/US2009/031603
(87) 국제공개번호 WO 2009/092115
국제공개일자 2009년07월23일
(30) 우선권주장
61/022,127 2008년01월18일 미국(US)
(뒷면에 계속)
(56) 선행기술조사문헌
WO2008001322 A1
US20070157022 A1
전체 청구항 수 : 총 4 항

(73) 특허권자
인터디지탈 패튼 홀딩스, 인크
미국, 델라웨어주 19809, 윌밍턴, 벨뷰 파크웨이 200, 스위트 300
(72) 발명자
차 인혁
미국 펜실베니아주 19067 야들리 사우스릿지 서클 510
샤 요겐드라 씨
미국 펜실베니아주 19341 엑스톤 리젠시 코트 10
(뒷면에 계속)
(74) 대리인
신정건, 김태훙

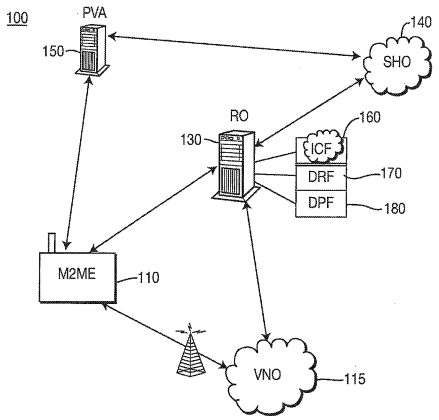
심사관 : 정필승

(54) 발명의 명칭 **M2M 통신을 인에이블하는 방법 및 장치**

(57) 요 약

보안 M2M 프로비져닝 및 통신을 수행하기 위한 방법 및 장치가 개시된다. 특히, M2ME를 고유하게 식별하기 위한 임시 비공개 식별자, 또는 임시 접속 식별정보(PCID)도 또한 개시된다. 또한, M2ME를 확인하고 인증하고 프로비져닝하는데 사용하기 위한 방법 및 장치가 또한 개시된다. 개시된 확인 절차는 자율, 반자율, 및 원격 확인을 포함한다. 프로비져닝 절차는 M2ME를 재프로비져닝하기 위한 방법을 포함한다. 소프트웨어를 업데이트하고, M2ME에 대한 조작을 검출하는 절차도 또한 개시된다.

대 표 도 - 도1



(72) 발명자

쉬미트 앤드레스 유

독일 프랑크푸르트 암 마인 65929 투토넨베르그 37

메여스테인 마이클 브이

영국 마틀샴 헤스 입스위치 1피5 3티유 메이필드 27

(30) 우선권주장

61/025,163 2008년01월31일 미국(US)

61/031,630 2008년02월26일 미국(US)

61/060,725 2008년06월11일 미국(US)

61/127,792 2008년05월14일 미국(US)

61/141,569 2008년12월30일 미국(US)

61/141,586 2008년12월30일 미국(US)

특허청구의 범위

청구항 1

신뢰 환경(trusted environment; TRE)을 갖는 M2ME(machine-to-machine equipment)에서의 방법에 있어서,

인증 절차를 개시하는 단계;

보안 시작(secure start-up)을 달성한 M2ME의 부분을 결정하는 단계;

상기 M2ME의 부분이 미리 정의된 상태의 보안 시작을 충족할 때, 상기 신뢰 환경에 의하여, 상기 M2ME가 네트워크에 어태치(attach)하도록 함으로써, 상기 네트워크에 대한 상기 M2ME의 유효성을 암시적으로 표시하는 단계;

상기 M2ME의 부분이 미리 정의된 상태의 보안 시작을 충족하지 않을 때, 상기 신뢰 환경에 의하여, 상기 M2ME가 상기 네트워크에 어태치하는 것을 방지함으로써, 상기 네트워크에 대한 상기 M2ME의 무효성을 암시적으로 표시하는 단계;

상기 신뢰 환경에 의하여, 자율 확인(autonomous validation)의 복수의 이벤트들 각각에 대하여 자율 확인 이벤트에 관한 정보를 포함하는 감사 기록(audit record)을 저장하는 단계; 및

상기 M2ME와 독립적인 엔티티로부터 하나 이상의 감사 기록에 대한 요청을 수신하는 단계

를 포함하는 M2ME에서의 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

청구항 1에 있어서, 상기 M2ME의 부분이 미리 정의된 상태의 보안 시작을 충족할 때 증명서 또는 크리덴셜을 생성하는 단계를 더 포함하는 M2ME에서의 방법.

청구항 5

삭제

청구항 6

M2ME(machine-to-machine equipment)에 있어서,

인증 절차를 개시하도록 구성되는 프로세서; 및

상기 프로세서와 통신하는 신뢰 환경을 포함하고,

상기 신뢰 환경은,

보안 시작을 달성한 M2ME의 부분을 결정하고;

상기 M2ME의 부분이 미리 정의된 상태의 보안 시작을 충족할 때, 상기 M2ME가 네트워크에 어태치(attach)하도록 함으로써, 상기 네트워크에 대한 상기 M2ME의 유효성을 암시적으로 표시하고;

상기 M2ME의 부분이 미리 정의된 상태의 보안 시작을 충족하지 않을 때, 상기 M2ME가 상기 네트워크에 어태치하는 것을 방지함으로써, 상기 네트워크에 대한 상기 M2ME의 무효성을 표시하고;

자율 확인의 복수의 이벤트들 각각에 대하여 자율 확인 이벤트에 관한 정보를 포함하는 감사 기록(audit record)을 저장하고;

상기 M2ME에 독립적인 엔티티로부터 하나 이상의 감사 기록에 대한 요청을 수신하도록 구성되는 것인

M2ME.

청구항 7

삭제

청구항 8

삭제

청구항 9

청구항 6에 있어서, 상기 신뢰 환경은 또한 상기 M2ME의 부분이 미리 정의된 상태의 보안 시작을 충족할 때 증명서 또는 크리덴셜을 생성하도록 구성되는 것인 M2ME.

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 무선 통신에 관한 것이다.

배 경 기 술

[0002] M2M(Machine-to-Machine) 통신은 배치될 경우 반드시 직접적인 사람의 상호작용을 필요로 하는 것이 아닌 엔티티들 간의 데이터 통신의 형태이다. M2M 통신의 하나의 과제로는, 배치된 장비가 어떠한 직접적인 사람의 상호작용 없이도 원격으로 관리될 수 있도록 프로토콜을 확립하는 것이다.

[0003] 기존의 M2M 방법은 예비 구성 식별자의 오버디에어(OTA; over-the-air) 보호가 없고, 장비의 인증(authentication), 등록(registration), 및 프로비져닝(provisioning)에 있어서 M2M 가능(M2M-enabled) 장비의 신뢰 상태(TS; Trusted State) 상의 정보를 이용하지 않으며, M2M 가능 장비에 대하여 가입된 오퍼레이터의 보안 변경을 보장하지 못하고, M2M 가능 장비의 예비 인증에 사용된 인증 및 키 동의(Authentication and Key Agreement) 크리덴셜(credential)이 신뢰되는 것을 보장하지 못하고, 소프트웨어 및 펌웨어의 보안 업데이트나 M2M 가능 장비의 재구성을 제공하지 못하며, M2M 가능 장비에 대한 조작(tampering)을 검출하여 반응하지 못한다. 또한, M2M 가능 장비 사용자/가입자의 역할이 정의가 없다. 따라서, M2M 성능, 보안 및 신뢰성을 개선하기 위한 방법 및 장치를 제공하는 것이 유리할 것이다.

발명의 내용

해결하려는 과제

[0004] 본 발명은 M2M 통신을 인에이블(enable)하는 방법 및 장치를 제공하고자 한다.

과제의 해결 수단

[0005] 보안 M2M 프로비져닝 및 통신을 수행하기 위한 방법 및 장치가 개시된다. 특히, M2ME(machine-to-machine equipment)를 고유하게 식별하기 위한 임시 비공개(private) 식별자, 또는 임시 접속 식별정보(PCID; provisional connectivity identification)가 또한 개시된다. 또한, M2ME를 확인(validate)하고 인증하고 프로비져닝하는데 사용하기 위한 방법 및 장치도 개시된다. 개시된 확인 방법은 자율, 반자율, 및 원격 확인을 포함한다. 프로비져닝 절차는 M2ME를 재프로비져닝(reprovisioning)하기 위한 방법을 포함한다. 소프트웨어를 업데이트하고 M2ME에 대한 조작을 검출하기 위한 절차도 또한 개시된다.

발명의 효과

[0006] 본 발명에 따르면 M2M 통신을 인에이블하는 방법 및 장치를 제공할 수 있다.

도면의 간단한 설명

[0007] 첨부 도면과 함께 예로써 주어진 다음의 상세한 설명으로부터 보다 상세한 이해가 이루어질 수 있다.

도 1은 M2M 프로비져닝 및 통신을 위한 통신 시스템의 예시적인 블록도를 도시한다.

도 2는 M2ME의 예시적인 블록도를 도시한다.

도 3은 자율 확인을 위한 절차의 예시적인 흐름도를 도시한다.

도 4는 반자율 확인을 위한 절차의 예시적인 흐름도를 도시한다.

도 5는 반자율 확인을 위한 다른 절차의 예시적인 흐름도를 도시한다.

도 6은 원격 확인을 위한 절차의 예시적인 흐름도를 도시한다.

도 7은 M2ME의 프로비져닝 또는 재프로비져닝을 위한 예시적인 절차를 도시한다.

도 8은 M2ME의 프로비져닝 또는 재프로비져닝을 위한 대안의 예시적인 절차를 도시한다.

도 9는 새로 선택된 홈 오퍼레이터를 사용하여 M2ME를 재프로비져닝하기 위한 절차의 예시적인 흐름도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0008] 이하 언급될 때, 용어 "무선 송수신 유닛(WTRU; wireless transmit/receive unit)"은 사용자 기기(UE), 이동국, 고정 또는 이동 가입자 유닛, 페이저, 셀룰러 전화, 개인 휴대정보 단말기(PDA), 컴퓨터, M2M 장비(M2ME), 홈 노드 B 또는 무선 환경에서 동작할 수 있는 임의의 기타 유형의 디바이스를 포함하지만, 이에 한정되는 것은 아니다. 이하 언급될 때, 용어 "기지국"은 노드 B, 사이트 컨트롤러, 액세스 포인트(AP), 또는 무선 환경에서 동작할 수 있는 임의의 기타 유형의 인터페이싱 디바이스를 포함하지만, 이에 한정되는 것은 아니다.

[0009] 도 1은 M2M 프로비져닝 및 통신을 위한 통신 시스템(100)의 예시적인 블록도이다. 통신 시스템(100)은 M2ME(110), 방문한 네트워크 오퍼레이터(VNO; visited network operator)(115), 등록 오퍼레이터(RO; registration operator)(130), 선택한 홈 오퍼레이터(SHO; selected home operator)(140), 플랫폼 검증 권한자(PVA; platform verification authority)(150)를 포함한다. 시스템(100)은 또한 장비 제조자/공급자(E/S; equipment manufacturer/supplier)(도시되지 않음)를 포함할 수 있다.

[0010] VNO(115)는 도 1에서 단일 네트워크 엔티티로서 나타나 있지만, USIM/ISIM 애플리케이션의 최초 등록 및 프로비져닝의 목적을 위해 액세스되는 모든 액세스 네트워크가 VNO인 것으로 간주된다. M2ME(110)가 상이한 SHO에 대하여 등록하게 되면, VNO(115)는 VNO로 남는다. M2ME(110)가 현재 VNO(115)인 SHO(140)에 등록되게 된다면, VNO(115)는 SHO가 된다.

[0011] VNO(115)는 액세스 크리덴셜 및 인증이 요구될 수 있는 경우에 M2ME(110)에 임시 네트워크 액세스를 제공하는 일을 담당한다. 이는 PCID 또는 임의의 기타 임시 비공개 ID와 같은 임시 네트워크 액세스 크리덴셜에 기초할 수 있다. 허용되는 것으로 간주되는 경우에, VNO(115)는 DRF(170)에 개방 네트워크 액세스를 제공할 수 있으며, 적어도 RO(130)의 서비스에 대한 액세스에 어떠한 크리덴셜이나 인증도 요구되지 않는다. 예를 들어, 이 기능은 VNO(115)가 등록 및 프로비져닝 이벤트 후에 고객의 SHO가 될 것일 때 적용된다. 등록 및 프로비져

닝 절차가 구현된 후에, VNO(115)는 프로비져닝된 USIM/ISIM 애플리케이션을 사용하여 전체 네트워크(및 IMS) 액세스를 제공할 것이다.

[0012] RO(130)는 도시된 바와 같이 ICF(160), 탐색 및 등록 기능부(DRF; discover and registration function)(170), 및 다운로딩 및 프로비져닝 기능부(DPF; downloading and provisioning function)(180)를 포함한다. 그러나, 당해 기술 분야에서의 숙련자라면, ICF(160), DRF(170) 및 DPF(180)는 또한 개별 엔티티에 위치될 수도 있고, 또는 하나의 엔티티로 뭉쳐질 수도 있다.

[0013] ICF(160)는 동작적 네트워크 액세스의 등록 및 프로비져닝의 목적을 위해 통신 네트워크에 대한 임시 액세스를 허용하는 크리덴셜의 검증을 담당할 기능부 또는 권한자이다. ICF(160)의 기능은 각각의 M2ME(110)에 대한 임시 네트워크 액세스 크리덴셜 및 임의의 임시 비공개 식별자의 발행을 포함한다. 이들은 USIM/ISIM 애플리케이션 프로비져닝 절차가 일어날 수 있게 할 최초 임시 네트워크 액세스를 인증하는데 사용될 수 있다. ICF(160)는 또한 아래에 상세하게 설명되는 프로비져닝 및 재프로비져닝 절차를 위해 오버디에어 다운로드 가능한 M2M 키, 구성, 및 애플리케이션으로써 M2ME(110)를 프로비져닝하도록 구성될 수 있다.

[0014] ICF(160)는 또한 ICF(160)에 의해 발행된 크리덴셜을 이용해 M2ME(110)를 사전 구성하도록(pre-configure) 단말기 공급자를 제공하도록 구성될 수 있다. 이들 크리덴셜을 제공하기 위하여, ICF(160)는 M2ME(110)에 그것들을 내장시키는(embed) 일을 담당하는 조직에의 크리덴셜의 보안 전송을 제공하도록 구성되어야 한다. ICF(160)는 또한 데이터베이스에서 크리덴셜을 등록하고, 신뢰 당사자(relying party)에 의해 요청될 때 크리덴셜의 확인을 수행하도록 구성될 수 있다. 이는 신뢰 당사자에게의 인증 벡터 및/또는 기타 관련 데이터의 보안 전송을 포함할 수 있다. M2ME(110)의 SHO(140)에의 성공적인 등록 전에 모든 액세스 네트워크가 방문 네트워크로서 간주되어야 함을 유의하여야 한다. 이는 어떠한 네트워크 변경 없이도 종래의 네트워크를 통해 SHO(140)에의 투과 접속을 허용한다.

[0015] DRF(170)는 특정 SHO(140)의 구매후 선택(after-purchase selection) 및 그 SHO(140)에의 M2ME(110)의 등록을 가능하게 하는 기능부이다. 이는 독립적인 서비스일 수 있고, 대안으로서 SHO(140)에 의해 동작될 수 있으며 이의 RO(130)가 SHO의 3GPP 네트워크를 통해서만 접촉 가능하거나 또는 인터넷을 통하여 직접 접촉 가능하고 예를 들어 M2ME(110)에서의 기능을 사용하여 탐색 가능할 수 있다.

[0016] DRF(170)는 적어도 다음의 사용(usage) 관련 기능들을 지원해야 하는데, (1) 공급자로부터 M2ME(110)의 전달 후에 고객이 SHO(140)를 선택할 수 있게 해주고, (2) 임시 인증된 네트워크 액세스나 제한된 개방 네트워크 액세스를 사용하여 M2ME(110)가 RO(130)에 대한 IP 접속을 갖게 해주고, (3) M2ME(110)가 아직 어떠한 SHO(140)와도 연관되지 않음에 따라 M2ME(110)가 방문 네트워크 오퍼레이터를 통하여 USIM/ISIM 애플리케이션 프로비져닝이 일어나도록 요청할 수 있게 해주고, (4) 프로비져닝 요청을 승인하여 M2ME(110)를 프로비져닝하도록 DPF(180)에 권한 부여하고, (5) M2ME(110)의 소유자에 의한 M2ME(110)의 등록을 지원하여야 한다.

[0017] 상기 기재한 사용 관련 기능들을 지원하기 위하여, DRF(170)는 M2ME(110)의 SHO(140)와의 연관을 지원할 수 있다. 대안으로서, DRF(170)는 VNO의 네트워크에 의해 제공된 IP 접속을 사용하여 직접 탐색 가능하고 어드레스 지정가능할 수 있다. 어떠한 경우든, DRF(170)는 M2ME(110)가 자신의 신뢰 환경(TRE; trusted environment)(230)의 진위(authenticity)의 증거로서 소유하는 크리덴셜의 PVA(150)를 통한 확인을 지원하여야 한다. DRF(170)는 또한 인가(authorization) 및 감사(audit)를 위해 DPF(180)에의 접속을 지원해야 한다. 또한, 크리덴셜의 확인 뿐만 아니라 TRE(230)가 그리 하는 것이 바람직하다면 TRE(230)와 선택적으로 전체 M2ME(110)의 확인이 있을 수 있다는 것을 유의하여야 한다. 예를 들어, 확인은 M2ME 기능부들의 신뢰(trustworthiness)를 확립하는 것을 포함할 수 있다.

[0018] DRF(180)는 또한 USIM/ISIM 크리덴셜, 파일 및 실행(executable)과 같은 M2ME(110)에 다운로드될 데이터의 패키지의 생성 또는 획득을 지원할 수 있다. DRF(180)는 또한 PS에 안전하게 이 데이터를 전송하도록 구성될 수 있다. 대안으로서, 이들 기능은 DPF(180)에 의해 제공될 수 있다.

[0019] 마지막으로 DRF(180)는 또한 M2ME(110)와 DPF(180) 사이의 보안 연관의 설정을 용이하게 할 수 있다. 이는 M2ME(110) 및 DPF(180)에의 보안 채널을 통한 보안 토큰의 생성 및 전송을 필요로 할 수 있다.

[0020] DPF(180)는 M2ME(110)에의 USIM/ISIM 크리덴셜의 원격 프로비져닝을 가능하게 한다. DPF(180)의 기능은 M2ME(110)를 프로비져닝하는데 대한 DRF(170)로부터의 인가를 수신하는 것을 포함한다. 이는 M2ME(110)와 통신하기 위한 보안 토큰을 제공하는 것을 포함할 수 있다. DPF(180)는 또한 다운로드될 애플리케이션 패키지를 DRF(170)로부터 수신하는 일을 담당한다. DPF(180)는 대안으로서 저장된 규칙들로부터 이를 생성할 수 있고

M2ME(110)로부터 다운로드된 크리덴셜을 DRF(170)에 알릴 수 있다.

[0021] DPF(180)는 또한 아래에 기재되는 바와 같이 M2ME(110)에의 USIM/ISIM 파라미터 또는 USIM/ISIM 애플리케이션의 프로비져닝을 지원하도록 구성된다. 프로비져닝 외에도, DPF(180)는 또한 M2ME(110)에의 USIM/ISIM 파라미터 또는 USIM/ISIM 애플리케이션에 대한 추후의 업데이트 및 새로운 애플리케이션의 추후의 프로비져닝을 수행하도록 구성될 수 있다. 이들 기능이 포함되면, DPF(180)는 또한 성공적이거나 성공적이지 않은 프로비져닝 이벤트를 DRF(170)에 통지하도록 구성될 수 있다.

[0022] SHO(140)는 고객 또는 M2ME(110)의 최종 사용자와의 상업적 관계를 가지며 고객에게 요금 청구하는 일을 담당하는 네트워크 오퍼레이터이다. SHO(140)는 다른 역할들, 특히 DRF(170) 및 DPF(180)의 일부 또는 전부를 동작시킬 수 있으며, 또는 이들은 전부 SHO(140)와 그리고 서로 동작적 관계를 갖는 개별 상업적 엔티티들일 수 있다.

[0023] M2ME(110)는 처음에 서비스 제공자와 함께 동작하도록 의뢰(commission)되지 않으며, 그리하여 VNO(115)와 통신하여 RO(130)에 대한 채널을 확립한다. 서비스를 프로비져닝하기 위하여, 각각의 M2ME(110)는 PCID와 같은 각자의 임시 비공개 아이덴티티를 가지며, 이는 임의의 VNO(115)가 M2ME(110)를 인식하여 자기가 제공하는 서비스에 대한 임시 액세스를 허용할 수 있게 하며, 오퍼레이터와의 서비스를 다운로드 및 프로비져닝하기 위하여, 최초 접속 메시지를 적합한 네트워크 컴포넌트로 향할 수 있게 한다.

[0024] PVA(150)는 다운로드된 USIM/ISIM 애플리케이션의 저장 및 실행에 사용되는 M2ME(110) 내의 보안 디바이스의 진위를 입증하는 크리덴셜을 담당하는 권한자이다. 이 기능은 증명서(certificate)와 키 쌍과 같은 크리덴셜을 발행하고 증명서 확인 서비스를 제공하는 하나 이상의 상업적 조직에 의해 수행될 수 있다. 보안 디바이스는 UICC, TRE, 또는 M2ME(110)에 내장된 일부 기타 형태의 보안 모듈일 수 있다. 이 기능은 보안 디바이스의 강력한 인증이 USIM/ISIM 애플리케이션의 프로비져닝을 위한 전제조건(pre-requisite)인 경우에 요구된다. PVA(150)는 또한 M2ME(110) 내의 보안 디바이스의 보안을 입증하도록 크리덴셜의 생성 및 발행과 같은 기능을 제공할 수 있다. 그러나, 이 기능이 다른 엔티티에 의해 수행될 수 있다는 것도 가능하다. PVA(150)는 또한 필요조건 프로토콜을 사용하여 신뢰 당사자에 의해 요청될 때 상기 기재한 크리덴셜의 확인과 같은 기능을 제공할 수 있다. 이는 신뢰 당사자에의 인증 벡터 및/또는 기타 관련 데이터의 보안 전송을 포함할 수 있다. PVA(150)는 또한 디바이스의 발행된 크리덴셜의 유효성(validity)에 관한 데이터의 유지와 같은 기능을 제공할 수 있다.

[0025] 장비 제조/공급자(E/S; manufacture/supplier)(도시되지 않음)는 또한 도 1의 통신 시스템(100)에 참여한다. 구체적으로, M2ME(110)는 임시 최초 네트워크 액세스를 위한 인증을 위해 ICF(160)로부터 크리덴셜을 안전하게 획득한다. E/S는 또한 임시 최초 네트워크 액세스를 허용하기 위하여 그들의 예비 네트워크 액세스 크리덴셜을 이용해 고객에의 전달 전에 M2ME(110)의 재구성을 지원할 수 있다. 또한, E/S는, M2ME(110)가 표준화된 보안 요건 세트에 따르는, ICF(160)를 통하여 DRF(170)에 증명하는데 사용하기 위한 크리덴셜을 PVA(150)로부터 안전하게 획득할 수 있다. 이러한 활동은 필요한 보안 기반구조를 갖는 승인된 조직에 맡겨질 수 있다.

[0026] E/S는 또한 고객에의 전달 전에 크리덴셜을 이용해 M2ME(110)의 사전구성(pre-configuration)을 담당할 수 있다. 이러한 사전구성 활동은 필요한 보안 기반구조를 갖는 승인된 조직에 맡겨질 수 있다. E/S는 또한 단말기 소유자가 원하는 DRF(170) 및 SHO(140)를 선택할 수단을 제공할 수 있거나, 또는 단말기가 액세스 네트워크(AN)에 접속될 때 이것이 자동으로 발생하도록 할 수단을 제공할 수 있다.

[0027] 도 2는 도 1의 M2ME(110)의 예시적인 도면을 도시한다. M2ME(110)는 송신기(215), 수신기(220), 프로세서(225), 신뢰 환경(TRE)(230)을 포함한다. 선택적으로, M2ME(110)는 GPS(global positioning system) 유닛(235), 가입자 아이덴티티 모듈(SIM)(240) 및 보안 시간 유닛을 포함할 수 있다.

[0028] M2ME(110)는 TRE(230)와 같은 수많은 다양한 신뢰 메커니즘, 또는 SIM(240) 또는 ISIM과 같은 임의의 기타 신뢰 프로세싱 또는 저장 메커니즘을 지원하도록 구성될 수 있다. 이들 신뢰 메커니즘은 또한, 풀(full) AKA가 발생할 수 있기 전에 그리고 인증이 확립된 후에, M2ME(110)와 네트워크 요소 사이의 임의의 통신을 보호하기 위해(PCID의 전송만은 아님), M2ME(110)에서 TRE(230)에 의해 보호된 '신뢰 상태' 정보 및/또는 임의의 키를 포함하도록 일반적인 AKA 프로토콜로 보다 완전히 통합될 수도 있다.

[0029] 선택적으로, SIM(240)은 또한 상기 기재한 동작들을 지원하도록 신뢰 프로세싱 모듈(TPM; trusted processing mudule) 또는 모바일 신뢰 모듈(MTM; mobile trusted module)의 기능을 포함하도록 강화될 수 있다. 대안으로서, SIM(240)은 원하는 기능을 달성하도록 M2ME(110) 내의 TPM 또는 MTM과 밀접하게 동작할 수 있다. SIM의 기능은 또한 TRE(230) 내에서 달성될 수 있다는 것도 유의하여야 한다. 이는 아이덴티티 관리에 있어서 보다 양

호한 융통성을 가능하게 한다.

[0030] 선택적으로, M2ME(110)는 E/S에 의해 설치되는 적어도 하나의 AKA 루트 시크릿(root secret)을 이용해 사전프로비져닝(pre-provisioning)될 수 있으며, 이 중 하나는 임의의 소정 시간에 활성이다. AKA 루트 시크릿(들)은 SIM(240)에 의해 보호될 수 있으며, 절대 변경되서는 안 된다. SIM(240)은 활성 AKA 루트 시크릿으로부터 세션 키를 유도하도록 구성될 수 있다.

[0031] M2ME(110)는 또한 ICF(160)에 신뢰 상태 정보를 제공하도록 구성될 수 있다. 그러면, 신뢰 상태 정보는 M2ME(110)가 VNO(110)에 어태치(attach)할 때 예비 인증에 사용될 수 있다. 신뢰 상태 정보는 또한 세션 키(CK 및 IK)를 유도하는데 사용될 수 있다.

[0032] TRE(230) 기능은 하나의 컴포넌트 상에서 독점적으로 구현될 수 있으며, 또는 M2ME(110) 내의 내장된 신뢰 컴포넌트들 사이에 분포될 수 있다는 것을 유의하여야 한다. 대안으로서, TRE(230) 기능은 탈착 가능한 SIM 모듈 상에서 구현될 수 있다.

[0033] 세션 키 CKn 및 IKn에 PCR 레지스터 값을 바인딩(bind)할 공식의 예는 다음과 같을 수 있으며, 여기에서 n은 CKn 및 IKn의 가장 최근의 업데이트에 대한 인덱스를 칭한다:

$$CK_n = f3_K\,(RAND \,||\, PCR0_n)$$

$$IK_n = f4_K\,(RAND \,||\, PCR0_n).$$

Equation 1

[0034]

[0035] 여기에서, $f3_K()$ 및 $f4_K()$는 공유 마스터 시크릿 K 중에 각각 암호 키 및 무결성(integrity) 키에 대한 AKA 키 유도 함수를 칭하고, RAND는 CATNA에 의해 생성되고 AKA 프로세스에서 M2ME(110)에 보내짐에 따라 공유되는 인증 벡터(AV) 내의 랜덤 넌스(random nonce)이고, PCR0n은 M2ME(110) 상의 MTME 안의 PCR0 레지스터의 가장 최근의 값을 칭한다. PCR0 레지스터의 현재 값은 M2ME(110)의 가장 최근의 부트후(post-boot) 신뢰 상태의 기술(description)을 의미함을 유의하자.

[0036] 방정식(Equation) 1에 따라, M2ME(110)의 PCR0 값이 두 번 부트들 사이에 변하는 경우 CKn과 IKn의 값이 변한다는 것을 유의하자. 이러한 방식이 작용하기 위하여, ICF(160)는 또한 M2ME(110)의 부트후 신뢰 상태의 변화가 있을 때 PCR0 값(또는 보다 일반적으로 M2MR(110)의 '신뢰 상태')의 변화를 알아야 한다. 이는 ICF(160)가 M2ME(110)의 부트후 신뢰 상태에 영향을 미치는 M2ME의 OS, 펌웨어 또는 애플리케이션의 임의의 적법한 또는 인가된 업데이트의 스케쥴 및 내용을 알게 되어 있다면 가능하게 될 수 있다. 이는 아래에 기재한 절차에서 PVA(150) 및/또는 ICF(160)를 수반함으로써 행해질 수 있다. 그러면, 적합한 절차에 이어서, M2ME(110)와 ICF(160) 사이에 공유되는 AKA 암호 및 무결성 키가 업데이트되고 세션 키가 M2ME(110)의 가장 최근의 '신뢰 상태' 값을 반영하는 방식으로 M2ME(110)의 인증에 유용하게 됨으로써, AKA 키 유도 프로세스의 신선도(freshness) 및 보안을 강화하는 것을 보장할 수 있다.

[0037] 세션 키가 M2ME(110)와 ICF(160) 사이에 동일한 방식으로 업데이트될 수 있고 M2ME(110)에서의 업데이트 절차 자체가 신뢰 컴퓨팅(Trusted Computing) 기술의 사용에 의해 제공되는 것과 같은 신뢰 실행 환경에서 수행되는 한, 방정식 1의 공식과 다른 바인딩(binding) 공식이 고려될 수 있다는 것을 유의하여야 한다.

[0038] TRE(230)는 이 분리를 위한 하드웨어 지원을 갖는 M2ME(110)에서의 논리적으로 별도의 영역이다. 이는 반드시 탈착가능한 모듈인 것은 아니며, 즉 IC 내의 기능부이거나, IC 그룹에 걸쳐 분포되어 있는 기능부들일 수 있다. TRE(230)는, TRE(230)와 직접 통신하도록 권한 부여되는 엔티티의 제어 하에서만 사용 가능한, 외부 세계에 대한 논리적 및 물리적 인터페이스를 정의한다.

[0039] TRE(230)는 다수의 관리가능한 아이덴티티(MID; manageable identity)에 대하여 그리고 MID의 프로비져닝 및 관리와 관련된 특정 기능들에 대하여 보안 저장 및 보안 실행 환경을 위한 신뢰의 루트를 제공한다. MID는 전체 보안 애플리케이션 및 그의 제휴 파라미터, 크리덴셜 등에 대한 포괄적인 용어이다. 이는 표준 USIM 애플리케이션 및 키와 같은 임의의 가입 관리 기능, 또는 ISIM 또는 보안 지불 애플리케이션과 같은 기타 보안 애플리케이션을 통합할 수 있다. 이하, MID는 관리가능한 아이덴티티, 가입 관리 아이덴티티, USIM 애플리케이션, ISIM 애플리케이션, 가상 SIM(vSIM), 또는 임의의 기타 동적인 보안 아이덴티티 솔루션을 칭하는데 사용될 수 있다.

[0040] TRE(230)는 또한 임의의 필요한 암호 키 및 기타 크리덴셜을 이용해 보안 대역외(out-of-band) 시설(facility)에서 사전프로비져닝될 수 있다. TRE(230)의 기타 보안 결정적인(security-critical) 기능이 동일한 방식으로 M2ME(110)로 사전프로비져닝된다. 부가적인 기능이 M2ME(110)가 발행된 후에 다운로드에 의해 통상적으로 프로비져닝될 수 있다.

[0041] TRE(230)는 또한 물리적 및 논리적 공격에 대항하는 어느 정도의 보호를 제공하고, 그 자신의 보안 정책을 지원하고 실시하며, UICC 또는 기타 스마트 카드 플랫폼에서만 현재 구현되는 MID의 저장 및 실행을 허용하는데 대해 충분히 안전하다. TRE(230)는 또한 TRE(230) 외부에 있는 M2ME(110) 부분에 대한 인터페이스를 갖는다.

[0042] TRE(230)는 사용될 경우에 TRE(230)에 또한 내장되는 M2ME(110)의 아이덴티티와 통상적으로 연관되는 자신의 내장된 고유 아이덴티티를 갖는다. 이러한 것으로서, TRE(230)는 표준화된 프로토콜을 사용하여 발행 권한자에 이들 아이덴티티를 안전하게 인증하도록 구성될 수 있다. 그러면, 발행 권한자는 TRE의 아이덴티티를 유효 발행된 TRE(230) 및 M2ME(110)의 아이덴티티인 것으로서 확인할 수 있다. 이들 아이덴티티의 각각은 M2ME(110)가 발행되기 전에 일어나는 물리적으로 안전한 대역외 프로세스의 일부로서 내장된다.

[0043] TRE(230)는 특정 강화된 기능을 갖는 삽입된 UICC에서 구현될 수 있으며, 또는 대안으로서 M2ME(110)에 의해 제공된 하드웨어 및 소프트웨어 컴포넌트를 이용하는 M2ME(110) 상의 통합 솔루션으로서 구현될 수 있다. TRE(230)가 강화된 UICC에서 구현된다면, TRE(230)는 여전히 MID의 다운로딩 및 원격 프로비져닝 및 관리 그리고 TRE(230) 내의 관리가능한 아이덴티티 엔진(MIDE; manageable identity engine)의 기능을 지원할 것이다.

[0044] TRE(234)가 M2ME(110)에서 통합 솔루션으로서 구현되면, M2ME(110)는 TRE 코드 베이스를 구성하는 소프트웨어 코드 및 데이터의 무결성 체크를 지원한다. TRE 코드는 M2ME(110)의 파워업(power up)/부트시에 적어도 한번 체크되어야 한다. 선택적 코드 체크는 특정 트리거/이벤트에 또는 정의된 간격으로 백그라운드 프로세스로서 M2ME(110)의 동작적 사용 동안 수행될 수 있다. 또한, 코드 체크의 커버리지는 M2ME(110)의 전체 또는 부분 체크를 커버하도록 확장될 수 있다.

[0045] 대안의 개선에서, TRE(230)는 TRE(230) 내에서 이해관계자-소유자(stakeholder-owner)가 각각 소유하는 다수의 분리된 신뢰 도메인에 대한 지원을 포함할 수 있다. 이러한 도메인들은 조작성이며 인가되지 않은 액세스에 대항하여 서로 분리될 수 있으며, 인증 및/또는 입증 기능과 같은 도메인간 서비스를 제공할 수 있다.

[0046] 일부 사용 경우에, M2ME(110)는 그의 배치 사이클의 대부분 동안 휴면(dormant) 상태에서 동작할 것이고, 산발적으로만 또는 드물게 3G 네트워크에 접속할 것이다. 이러한 경우에, TRE의 소프트웨어 코드의 실행시간(run-time) 무결성 체크는 휴면 상태 주기 동안 일어나도록 이루어질 수 있다. 이러한 방식으로, 코드 체크는 TRE(230) 또는 M2ME(110) 내의 다른 프로세스를 방해하지 않을 것이고, 코드 체크의 결과는 M2ME(110)가 SHO(140)에 재접속할 때 준비되도록 이루어질 수 있다.

[0047] 각각의 M2ME(110)에는 M2ME(110)에 고유한 임시 비공개 아이덴티티, 즉 PCID(provisional connectivity identification)이 할당되어야 한다. PCID는 각각의 M2ME를 고유하게 식별하는 임시 비공개 아이덴티티이다. 이 PCID는, 요구될 경우에, M2ME가 SHO(140)와 같은 임의의 특정 SHO와 연관되기 전에 3GPP 네트워크에 등록할 수 있게 하기 위하여 ES에 의해 M2ME(110)에 설치될 필요가 있다. PCID는 처음에 ICF(160)에 의해 발행되며, ICF(160)는 프로비져닝 관계를 갖는 ES에 PCID를 보낸다. 그러면, ES는 M2ME(110)의 TRE(230)로 PCID를 프로비져닝한다. PCID가 M2ME(110)로부터 VNO(115)로 제시될 때, VNO(115)는 표준 IMSI의 포맷을 갖는 것으로서 그것을 인식한 다음, 나중에 프로비져닝을 위한 최초 접속을 확립하도록 M2ME(110)를 RO(130)로 향하게 할 수 있다.

[0048] 하나의 실시예에서, 단일 PCID는 M2ME(110)에 의해 실시되는 제한된 기간(time span) 동안 유효할 수 있다(이하, "유효 기간(validity period)"). 유효 기간은 그의 TRE(230)에 의해 구체적으로 제어될 수 있다. 각각의 M2ME 디바이스는 PCID 및 유효 기간을 수신할 수 있다. 시간이 만료된 후에, M2ME(110)는 PCID를 삭제할 수 있다. 그러면, PCID는 동일한 PCID로써 프로비져닝되는 또 다른 M2ME(도시되지 않음)가 코어 네트워크에 어태치하려고 시도할 때 재사용될 수 있다. 그러나, 두 번째 M2ME의 PCID의 유효 기간은 일반적으로 이전의 M2ME의 PCID의 유효 기간과 중첩해서는 안된다.

[0049] 첫 번째 M2ME(110)가 PCID를 다시 사용하지 않은 후에, 통상적으로 PCID는 M2ME(110)에 대한 적합한 유효 기간의 소진까지 새로운 M2ME에 재발행되지 않을 수 있다.

[0050] 다른 실시예에서, PCID는 체계적으로 재할당될 수 있다(PCID의 동시 사용 없이). 이는 M2ME(110)의 라이프사이

클(lifecycle)을 커버할 수 있다. 한정된 수의 PCID가 M2ME(110)에 체계적으로 사전프로비져닝될 수 있다. 이는 TRE(230)의 성능을 이용하면서 최초 네트워크 접속의 자율 관리를 허용할 수 있다. M2ME는 크기 N의 그룹으로 해제(release)된다고 가정된다. j번째 배치(batch)의 M2ME는 M_i,j로 칭하며, 여기에서 j=1,...,M이다. PCID 할당은 크기 NxM의 매트릭스 (P)_{i,j}로 초기화될 수 있다. M2ME(110) M_i,1은 제조 동안 TRE(230)로 로딩된 열 P_i,*을 얻는다. M2ME가 해제될 때, 보안 타이머(secure timer) 및 단조 카운터(monotonic counter)가 초기화되고 활성화되며 TRE(230)의 제어 하에 놓인다. 배치 1의 M2ME(110), 즉 M_i,1은 초기화된 카운터 또는 시간에 기초하여 미리 결정된 횟수 또는 결정된 기간 T에 대하여 P_i,1을 사용한다. 소정 시간(유효 기간) 후에, M_i,1의 TRE는 P_i,1을 폐기하고 P_i,2를 사용한다. 사용 횟수 또는 기간은 제2 배치가 아직 해제되지 않도록 이루어져야 함을 유의하여야 한다. 제2 배치 M_i,2는, 해제될 때, 또한 이 시점에서 M_i,1에 의해 놓아지는(free) P_i,1을 사용하기를 시작한다. 이상적으로, MxT는 네트워크에 의해 지원되어야 하는 모든 M2ME의 전체 동작 시간을 커버한다.

[0051] 이 실시예는 디바이스가 라이프타임 사이클 내에 있는지 네트워크가 결정할 수 있게 해줄 수 있다. 이전의 PCID는 새로운 디바이스에 안전하게 재할당될 수 있다. 이 방식은 TRE(230)와의 M2ME 제조자의 본질적인 신뢰 관계를 활용한다. TRE(230)에 의한 시간 제한의 실시와 TRE(230) 내의 PCID 열 벡터의 처리는, PCID의 동시 사용이 막아지며 M2ME(110)가 그의 동작 시간 전반에 걸친 사용을 위한 유효 PCID를 갖는다는 것을 PLMN 오퍼레이터에 대하여 장담한다.

[0052] 그러나, 이 실시예는 네트워크 오퍼레이터에 영향을 미칠 수 있는데, 네트워크 오퍼레이터가 제조 프로세스의 특정 지점에서 제조자에게 PCID 세트를 전달하거나, 또는 해제 전에 보안 설비에서 PCID 세트를 설치할 수 있기 때문이다. 또한, M2ME는 다수의 PCID를 이용해 사전프로비져닝될 수 있다. M2ME는 PCID의 추후 배치의 재프로비져닝을 지원할 수 있다. 임의의 소정 시간에 PCID의 동일 배치를 공유하는 다수의 M2ME들은, 둘 이상의 M2ME가 동일 배치로부터 동일한 PCID를 선택하고 동시에 접속하려고 시도함에 따라 'PCID 충돌'을 초래할 수 있는 '기회(chance)' 충돌을 가질 수 있다. 배치의 크기(행의 크기, N)가 PCID의 동일 배치를 사용하는 M2ME들의 수보다 훨씬 크게 이루어진다면 그리고 M2ME가 랜덤 방식으로 사용할 PCID를 선택한다면 PCID 충돌의 기회는 더 적어질 수 있다.

[0053] 시간 제한을 갖는 PCID의 관리는 소정의 정밀도 제한 내에서 M2ME의 내부 클록의 동기화를 필요로 한다. 이는 예를 들어 단일 M2ME(110)의 파워다운(power-down) 이벤트를 커버하여야 하며, 그 후에 재동기화가 필수가 될 수 있다. 따라서, TRE(230)는 시간축을 보유하고 관리하여야 하며 네트워크에서의 신뢰 시간 소스(trusted time source)와의 동기화를 지원해야 한다. 선택적으로, TRE(230)는 도 2에 도시된 바와 같이 M2ME(110)에 위치되어진 신뢰 시간 소스에 의존할 수 있다.

[0054] M2ME(110)는 GPS(235)와 같은 자율 측위(geo-positioning) 장비를 구비할 수 있다. M2ME(110) TRE(230)는 측위 장비에 대한 보안 액세스를 갖는다.

[0055] M2ME(110)는 상이한 영역들에 분포될 수 있으며, 2개의 M2ME가 동시에 동일한 액세스 네트워크(AN) 셀 또는 기지국에 대한 무선 접속을 물리적으로 확립할 수 없도록 구성될 수 있다. 따라서, 다수의 M2ME들은 동일한 PCID 뿐만 아니라 목적지(destination) 측위위치(geo-position)(D), 및 허용 범위(tolerance)(r)를 이용해 사전프로비져닝될 수 있으며, 목적지 측위위치는 각각의 M2ME에 고유하다. 이 데이터는 TRE(230) 안에 안전하게 저장되거나 암호로 보안될 수 있으며, 그리하여 TRE(230)만이 데이터에 액세스할 수 있다.

[0056] M2ME(110)에 의한 최초 네트워크 액세스 시도 전에, TRE(230)는 현재 측위위치를 결정하고, 허용 범위 r 내의 위치 D와 일치하는지 체크한다. 그러한 경우, TRE(230)는 최초 네트워크 액세스를 위해 PCID를 해제한다. 이러한 방식으로, 어떠한 2개의 M2ME라도 동일한 PCID를 사용하여 동일한 셀을 통하여 액세스를 시도하지 않을 것임이 AN에 보장될 수 있다.

[0057] 그렇지만, 어떤 경우에, AN은 상이한 셀들로부터의 동일한 PCID를 사용하는 동시 액세스 시도를 구별할 필요가 있을 수 있다. 따라서, 최초 네트워크 접속 서비스 내의 (PCID, 셀 ID) 쌍의 기록을 유지해야 할 필요가 있을 수 있다. 그리하여 이 경우에는 코어 네트워크에 일부 영향을 미칠 수 있다.

[0058] 대안의 실시예에서, M2ME(110)에 의한 네트워크에의 액세스는 미리 결정된 네트워크 셀을 통해서만 허가된다. 미리 결정된 네트워크 셀은 M2ME의 TRE로 로딩되는 그들의 네트워크 셀 식별자에 의해 식별된다. 이들은 쌍 (D,r)을 대신한다.

[0059] 또 다른 대안의 실시예에서, M2ME는 지리학적으로 이동될 수 있다. M2ME(110)가 이동될 때 네트워크 액세스는

디스에이블된다. M2ME 이동성(mobility)을 인에이블하기 위해, M2ME(110)는 특정 PCID가 사용될 수 있는 상이한 장소들을 지정하는 트리플(triple) 세트 (PCID, D, r)로써 사전프로비져닝될 수 있다. M2ME(110)의 최초 네트워크 접속 시도 전에, TRE(230)는 현재 측위위치가 목적지 D 중 하나의 범위 r 중 하나 내에 있는지 체크하고, 성공인 경우에 대응하는 PCID를 해제한다.

[0060] 또한, (PCID, D, r) 트리플릿(triplet)에는 라이프타임, 즉 상술한 바와 같이 사용되고 실시되어지는 허용된 사용 기간이 할당될 수 있다. 크리덴셜은 퀸트플(quintuple) (PCID, D, r, t1, t2)일 것이며, 여기에서 t1 및 t2는 유효 기간의 시작 및 종료 시간을 지정한다. 이는 M2ME(110)의 허용된 이동에 대한 경로를 기술한다. 예를 들어, M2ME(110)의 이동은 자동차에서와 같은 이동 배치 시나리오에서 제어될 수 있다. M2ME의 TRE(230)가 빈번하게 재접속하거나 아니면 PCID를 사용하도록 강행될 때, 네트워크 서비스에 의해 실패가 검출될 수 있고 (시간만료의 형태로), M2ME(110)가 결정된 경로를 남기는 것으로 해석됨으로써 경보를 일으킬 수 있다.

[0061] 상술한 방법 및 장치는 그들 라이프타임 전반에 걸쳐 M2ME(110)에 대한 이동성 및/또는 PCID 관리 요건을 수용하기에 불충분할 수 있다. 따라서, 퀸트플릿(quintuplet) (PCID, D, r, t1, t2)을 관리, 즉 재프로비져닝 및 삭제할 방법이 바람직하다.

[0062] 이러한 퀸트플릿은 PCID 업데이트 서비스(PUS; PCID update service)를 사용하여 재프로비져닝될 수 있다. PUS는 업데이트하는 TRE(230)(M2ME(110)에 고유하게 대응함)를 식별할 수 있다. PUS는 CCIF 서비스의 일부일 수 있거나 네트워크에서의 별도의 컴포넌트일 수 있다. 업데이트는 하나 이상의 (PCID, D, r, t1, t2) 퀸트플릿에 대한 변경을 포함할 수 있다. TRE(230) 아이덴티티(ID)는 현재 네트워크(IP) 어드레스에 TRE ID를 연관시킬 수 있는 네트워크 서비스에 보내질 수 있다. 예를 들어, 네트워크 엔티티는 풀 네트워크 접속을 획득하는 동안 TRE(230) 및 M2ME(110)의 무결성을 확인한 PVA(150)일 수 있고, 또는 PVA(150)와 함께 작업하여 M2ME(110)의 유효성을 확인하고 새로운 PCID(들)를 발행하며 M2ME(110)에 새로운 PCID(들)를 원격 프로비져닝하는 접속 크리덴셜 발행 기능부(CCIF; Connectivity Credentials Issuing Function)일 수 있다. 원격 프로비져닝은 또한 네트워크에서 DPF(170)에 위임될 수 있다.

[0063] 재포지셔닝(repositioning) 절차는, 예를 들어 아래에 기재되고 도 3 내지 도 5에 도시된 플랫폼 확인 절차를 통하여, PUS가 목표 M2ME(110) 및 TRE(230)에 접속하고 그의 상태의 확인을 요청할 때 시작된다. 이는 TRE(230)가 구(old) 퀸트플릿 (PCID, D, r, t1, t2) (세트)을 안전하게 폐기하고 원하는 새로운 것을 설치할 것임을 PUS에 표시할 수 있다. 확인 성공시, PUS는 새로운 (PCID, D, r, t1, t2) 퀸트플릿 및 폐기될 구 퀸트플릿들의 리스트를 전달할 수 있다. TRE(230)는 자동으로 새로운 퀸트플릿을 설치하고 (계속되는 접속을 보장하기 위해) 구 퀸트플릿을 폐기한다.

[0064] 다른 실시예에서, TRE(230)는 충돌을 완화하도록 PCID와 수반될 수 있는(adjoin) (의사) 랜덤 번호를 생성할 수 있다. AN은 추가적인 정보를 추적하고 그것을 구별하게 될 수 있다.

[0065] 통신 엔티티는 M2ME(110), TRE(230), 및 네트워크 액세스 포인트(NAP)(도시되지 않음)가 있다. NAP는 예를 들어 VNO(115)와 연관된 eNodeB(eNB)일 수 있다. TRE(230)는 단일 최초 네트워크 접속 시도에 사용될 랜덤 번호(RAND)를 생성한다. TRE(230)는 RAND가 제2 파라미터, 예를 들어 필요에 따른 추가 데이터(D1), 및 PCID를 입력하는 키 해시 함수와 같은 무결성 보호 방법을 적용한다. TRE(230)는 $\mathrm{TRE} \rightarrow \mathrm{eNB}: \mathrm{RAND} \,||\, \mathrm{PCID} \,||\, \mathrm{D1} \,||\, \mathrm{M1} := \mathrm{MAC}(\mathrm{PCID} \,||\, \mathrm{D1}, \mathrm{RAND})$로서 이 데이터를 보낸다.

[0066] eNB는 메시지 인증 코드(MAC; message authentication code)를 검증하고 페이로드 데이터(D2)와 수신 데이터로부터의 반환 패키지(return package)를 $\mathrm{eNB} \rightarrow \mathrm{TRE}: \mathrm{D2} \,||\, \mathrm{M2} := \mathrm{MAC}(\mathrm{PCID} \,||\, \mathrm{D2}, \mathrm{M1}$로서 구축하고, 이를 TRE에 보낸다.

[0067] 이 방법은 최초 네트워크 접속에서 교환된 모든 후속 메시지까지 확장된다. 후속 메시지 교환은 임의의 새로운 메시지 요소를 포함하는 데이터 요소의 MAC와 직전 교환의 MAC를 포함할 것이다. eNB 및 TRE(230)는 새로운 M_n을 구축하는데 마지막 값 M_{n-1}를 사용하여 이 통신 중에 메시지들을 구별할 수 있다.

[0068] 이 통신 상의 중간자(man-in-the-middle) 유형 공격을 피하기 위해, 미리 확립되거나 협상/공유된 시크릿이 통신 당사자들의 인증을 위해 메시지에 포함될 수 있다.

[0069] MAC 값에 적합한 PCID의 포함은 선택적이지만, 해시 테이블(hash table)을 구축하고, 다른 그리고/또는 일반적

인 PCID를 이용한 다수의 M2ME들의 동시 활성 네트워크 접속 시도를 효율적으로 구별하는데 유리할 수 있다. 이는 보안 이슈일 수 있는 최초 네트워크 접속 통신의 모든 메시지에서의 PCID의 송신을 막을 수 있다(가능한 클리어 텍스트(clear text)).

[0070] eNB는 PCID를 사용하여 모든 동시 활성 네트워크 액세스 시도(이하, 채널이라 부름)의 상태를 나타내는 표를 유지할 수 있다. 각각의 채널에 대하여, 표 1에서의 정보를 포함한다.

표 1

[0071]

PCID index	Active hash value	Data history
I	M_2	RAND, D_1, D_2

[0072] 제1 열은 이 특정 채널에 속하는 PCID의 인덱스를 포함하며, 이는 모든 채널에 대하여 동시 활성인 모든 PCID의 리스트에서의 엔트리를 가리킨다 PL:= [PCID1, ...PCIDN]. 이것은 상기 표에 대해 메모리를 보관하지만, 메모리가 문제가 아니라면, 이 열은 전체 PCID를 포함할 수 있다.

[0073] eNB는 채널을 통해 제3 메시지를 수신한다:

[0074] $\text{TRE} \rightarrow \text{eNB:} \qquad D3 \,||\, M3 := MAC(PCID \,||\, D3, M2)$

[0075] i=1,...,N에 대하여 다음 절차의 성공까지, eNB는 PL로부터 $PCID_i$를 선택한다. 첫 번째 셀에서 PCID 인덱스 I를 갖는 모든 표의 행에 대하여, eNB는 $M := MAC(PCID_i \,||\, D_3, M_2)$를 계산하고, 여기에서 M_2는 행에서의 두 번째 셀로부터 취해진다. $M=M_3$인 경우, 성공 상태에 도달하고 검색 절차가 종료된다. 마지막으로 수신한 제3 메시지에 대응하는 채널의 행 번호가 반환된다. D_3이 데이터 이력에 추가되고, M_2는 선택된 표 행의 활성 해시 값(Active Hash Value) 셀에서 M_3로 교체된다. 이러한 프로세스는 모든 후속 통신 단계에 대하여 반복된다.

[0076] 대안으로서, PCID 대신에, 제1 메시지 후의 메시지는 훨씬 더 효율적으로 후속 메시지의 연관된 채널을 찾기 위해 채널의 인덱스 I를 포함할 수 있다.

[0077] 특정 메모리에서 M2ME(110) 및/또는 eNB의 리소스가 한정되는 경우에, 활성 PCID는 잠금(locked)될 수 있다. 이는 M2ME(110)가 잠금된 PCID를 사용하는 것을 막음으로써 유리할 수 있다.

[0078] 예를 들어, M2ME(110)는 PCID에 대하여 eNB와의 채널을 개방하였다. 제2 TRE(도시되지 않음)를 갖는 제2 M2ME(도시되지 않음)는 제1 채널이 여전히 개방되어 있는 동안 동일한 PCID를 사용하여 eNB에의 채널을 개방하려고 시도한다. eNB는 M_1을 전송함으로써 제2 M2ME의 TRE의 제1 메시지에 응답할 수 있다. 따라서, 제2 TRE에는 이 PCID가 현재 차지되어 있음을 통지된다. 제2 TRE는 또 다른 채널 개방 시도를 위해 설치된 PCID의 풀(pool)로부터의 다른 PCID를 사용할 수 있거나, 또는 동일한 PCID를 다시 사용하기까지 미리 결정된 기간을 기다릴 수 있다.

[0079] 대안으로서, PCID는 참여하는 엔티티에 의해 능동으로 할당 해제(deallocate)될 수 있다. M2ME의 TRE(230)는 풀 네트워크 접속을 획득하기 위해 사용되었을 때 사용된 PCID를 폐기할 수 있다(즉, 적절한 크리덴셜의 다운로드 후). 다양한 이벤트가 PCID의 폐기를 야기할 수 있다. 예를 들어, TRE(230)가 그 목적을 위한 프로토콜의 성공적인 진행에 의한 것과 같이 풀 네트워크 접속이 보장되는 상태에 도달하였다면 PCID를 폐기하는 것이 트리거될 수 있다. 유효 기간이 만료된 경우, eNB, 보안 게이트웨이, 또는 전용 PCID 관리 엔티티와 같은 네트워크 엔티티가 폐기를 강행한 경우, 또는 M2ME(110)의 제조자와 같은 네트워크 외부의 엔티티가 폐기를 강행한 경우, PCID를 폐기하는 것이 트리거될 수 있으며, 이는 M2ME(110)에 VNO(115)를 통한 보안 접속을 확립할 수 있다.

[0080] 무슨 이벤트가 폐기를 트리거하는지에 관계 없이, 이벤트에 관한 정보는 PCID를 적절하게 할당 해제하는데, 즉 다른 M2ME에 의한 재사용을 위해 PCID를 놓아주는데(free) 사용될 수 있다. 할당 해제 이벤트를 시그널링하도록 TRE(230)로부터 M2ME의 제조자에의 접속이 확립될 수 있다. 제조자는 놓아진 PCID의 진행 리스트를 업데이트할 수 있고, 그것들을 재사용하여 해제시 새로운 M2ME에 PCID를 각인할 수 있다.

[0081] 대안으로서, ES, 기존의 SHO(140), 도시되지 않은 새로운 SHO 또는 ICF(160)와 같은 네트워크 내의 엔티티는,

예를 들어 하나의 SHO로부터 다른 SHO에의 가입 변경의 개시시 추후 접속 동작을 용이하게 하기 위하여, PCID를 업데이트하도록 구성될 수 있다. M2ME(110)가 프로비져닝되었다면, 새로운 SHO로써 서비스를 프로비져닝하는 것을 돕는데 추후 사용하기 위해 최초 네트워크 액세스 크리덴셜에 대한 업데이트된 값, PCID가 M2ME(110)에 MID로서 전달될 수 있다. 크리덴셜은 M2ME(110)의 TRE(230)에서 추출되고 저장되며 독점적으로 사용될 것이다.

[0082] SHO의 변경으로 인한 크리덴셜 재프로비져닝 프로세스 전에, M2ME(110)에는 그의 기존의 최초 네트워크 액세스 크리덴셜, PCID가 만료되었다거나 막 만료되려고 한다는 것이 알려질 수 있다. M2ME(110)는 E/S, 기존의 SHO(140), 새로운 SHO 또는 ICF(160)로부터 새로운 최초 네트워크 액세스 크리덴셜을 요청하고 수신할 수 있다. 대안으로서, M2ME(110)는 E/S로부터 또는 새로운 SHO로부터 소싱된 이들 네트워크 컴포넌트들 중 하나로부터 새로운 PCID를 수신할 수 있으며, 그리하여 M2ME(110)가 원시(pristine) 상태로부터 새로운 최초 네트워크 액세스 시도를 행할 때 새로운 SHO로 M2ME(110)를 라우팅할 수 있다.

[0083] 하나의 실시예에서, M2ME(110)는 U(I)SIM 애플리케이션, PCID, 및 하나보다 많은 AKA 루트 시크릿 세트(한 번에 하나의 활성 세트가 사용될 것임)로써 사전구성될 수 있다. PCID의 변경시, M2ME(110)에는 다음 AKA 크리덴셜 세트를 사용하도록 지시되며, 그리하여 이들이 M2ME(110)에 3GPP 접속을 제공하는데 사용됨으로써 새로운 SHO에의 가입 재프로비져닝 및 오퍼레이터의 변경을 용이하게 할 수 있다.

[0084] 상기에서는 최초 네트워크 액세스 크리덴셜의 교체 및 재프로비져닝 서비스에 대하여 가능한 방법들의 몇몇만 기재한 것이다. 모든 할당 해제 프로세스에서 보안의 고려는 PCID가 할당 해제 프로세스에서 클리어 텍스트로 전달되어서는 안된다는 것을 요구함을 유의하여야 한다. 또한, 모든 할당 해제 프로세스에 대하여, 통신 파트너는 할당 해제 프로세스에서 인증되어야 한다.

[0085] TRE(230), 또는 M2ME(110) 및 연관된 데이터와 크리덴셜의 신뢰 상태의 확인 또는 인증을 수행하기 위해 3가지 기본적으로 상이한 가능성이 존재한다. 가능성은, (1) 자율 확인, (2) 반자율 확인, 및 (3) 원격 확인을 포함한다. 각각은 도 1에 도시된 아키텍처를 참조하여 아래에 보다 상세하게 설명될 것이다.

[0086] 자율 확인은 M2ME(110)의 내부 확인이 M2ME(110)가 네트워크 어태치(network attachment)를 겪을 수 있게 하기 전에 발생하였다고 가정되는 절차이다.

[0087] 반자율 확인은, M2ME(110)의 유효성이 외부 네트워크 엔티티에 의존하지 않고 M2ME(110) 자체 내에서 평가되는 절차이다. 이러한 확인의 결과 및 M2ME(110)의 유효성에 대한 TRE(230)의 인증의 바인딩의 필요한 증거가 PVA(150)와 같은 원격 엔티티에 시그널링되며, 이는 M2ME(110)로부터의 메시지의 컨텐츠에 기초하여 결정을 행한다. M2ME(110)로부터 PVA(150)에의 시그널링은 보호되어야 한다.

[0088] 원격 확인은, M2ME의 TRE(230)에 의해 생성되는 확인에 대한 증거 뿐만 아니라 TRE(230)와 M2ME(110) 사이의 바인딩의 증거를 수신한 후에 M2ME(110)의 유효성/무결성을 외부 네트워크 엔티티(예를 들어, PVA(150))가 직접 평가하는 절차로 구성된다. 원격 확인을 위해 M2ME(110)와 PVA(150) 사이에 발생하는 통신은 보호되어야 한다.

[0089] TRE(230)가 M2ME(110)의 무결성의 자율 확인을 수행하면, 확인의 어떠한 직접적인 증거도 외부 세계에 제공되지 않는다. 외부 세계는, M2ME 및 TRE가 규정되고 구현되는 방식으로 인해, 그의 내부 무결성 체크에 실패한 M2ME(110)는 그의 TRE(230)에 의해 네트워크에 자신을 어태치한다거나 원격 엔티티에의 인증된 접속을 획득할 수 없을 것임을 가정한다. 예를 들어, 보안 부트(secure boot)의 프로세스는 M2ME(110)에서 코드를 안전하게 꺼내오는 것을 용이하게 하지만, 이 목적을 충족시키는 장비에 의존하는 것이 아닌 경우 어떠한 외부 시그널링도 존재하지 않는다.

[0090] 도 3은 M2ME(110)의 무결정을 확인하도록 TRE(230)에 의해 수행된 자율 확인 절차(300)의 예를 도시한다.

[0091] 먼저, 310에서 TRE(230)는 미리 정의된 상태의 보안 시작(secure start-up)을 달성했는지 체크한다. 다음으로, 320에서, TRE(230)는 보안 시작을 필요로 하는 나머지 M2ME(110)의 미리 정의된 부분이 미리 정의된 상태의 보안 시작을 달성했는지 체크한다.

[0092] 그 다음, 330에서, TRE(230) 자체에 의해 또는 TRE(230) 외부에 있지만 TRE(230)에 의해 무결성 보호되는 M2ME(110) 내의 측정 컴포넌트에 의해 부가적인 체크가 일어날 수 있다. 이러한 후단계(later-stage) 체크에서, 나머지 M2ME(110)의 다른 컴포넌트, 구성, 또는 파라미터의 무결성은, 그것들이 로딩되거나 시작될 때, 또는 다른 미리 정의된 실행시간 이벤트에서, 이러한 것들이 측정 컴포넌트에 이용 가능하게 될 때마다 체크된다.

[0093] 마지막으로, 340에서 TRE(230)는 M2ME(110)가 요청된 인증 절차에 참여할 것을 허용한다.

[0094] 자율 확인은 필요한 외부 통신에 대해서는 가장 경제적인 방법이다. 그러나, 자율 확인은 네트워크 액세스 동안 또는 중단되지 않은 접속 단계 동안 임의의 외부 엔티티가 M2ME(110) 또는 TRE(230)의 무결성을 독립적으로 평가할 수 있게 하지 못한다. 즉, M2ME(110)의 신뢰는, 네트워크 또는 기타 통신 파트너가 볼 때, 단순한 스마트 카드 기반의 인증의 경우에서와 같이, 오로지 M2ME의 TRE(230)의 보안 특성의 기술 사양에 달려있다.

[0095] 따라서, TRE(230)는 또한 자율 확인의 매 이벤트에 응답하여(예를 들어, 네트워크 액세스 시도 전에) 확인 프로세스의 로그 및 그의 결과를 저장할 수 있다. 예를 들어, 저장된 측정 로그 및 PCR(Platform Configuration Register) 값은 신뢰 컴퓨팅 그룹 원칙을 사용하여 M2ME(110)의 무결성을 보호하는데 저장되고 사용될 수 있다.

[0096] 이 저장된 데이터는 또한 데이터가 감사 기록(audit record)을 구성하므로 외부 감사에 대하여 사용될 수 있다. 감사 데이터는 TRE(230) 내의 또는 TRE(230)에 의해 보호되는 보안 내부 아카이브(archive)에 저장되며, 그리하여 이는 이러한 조작이 검출가능하지 않고서는 변경될 수 없다. 결과적으로, 데이터의 무결성 보호가 제공된다.

[0097] 또한, 감사 데이터는 자율 확인이 호출된 특정 목적에 바인딩된다(예를 들어, 네트워크 액세스 프로토콜 실행의 특정 인스턴스). 이는 감사 데이터에 확인 목적을 고유하게 식별하는 데이터를 포함시킴으로써 달성될 수 있다.

[0098] 예를 들어, 액세스 프로토콜에서 확립되어진 공유 시크릿 또는 크리덴셜이 감사 데이터에 첨부될 수 있고, 디지털 서명이 그의 무결성을 보호하도록 생성된 데이터 세트에 TRE(230)에 의해 적용될 수 있다. 그러면, M2ME(110)에 독립적인 엔티티는 임의의 추후 시점에 감사 데이터를 요청할 수 있다. 예를 들어, 엔티티는 해당 M2ME(110)가 모든 이른 네트워크 액세스 이벤트에서 신뢰할 수 있는지 확립하도록 주기적으로 감사 데이터를 요청할 수 있다. 그 다음, 이 증거는 TRE(230) 및 M2ME(110)에 대한 아이덴티티 크리덴셜과 함께, TRE(230)의 아이덴티티 및 진위를 더 확인하고 M2ME(110)의 조작을 검출하도록, 네트워크 액세스 시도에 대한 네트워크측 프로토콜과 대항(counter-check)될 수 있다.

[0099] 도 4는 TRE(230)가 M2ME(110)의 무결성의 반자율 확인을 수행하는 절차(400)를 도시한다. 절차(400)가 시작될 때, 410에서, TRE(230)는 미리 정의된 상태의 보안 시작을 달성했는지 체크한다. 다음으로, 420에서, TRE(230)는 보안 시작을 필요로 하는 나머지 M2ME(110)의 미리 정의된 부분이 미리 정의된 상태의 보안 시작을 달성했는지 체크한다. 그 다음, 430에서, TRE(230) 자체에 의해 또는 TRE(230) 외부에 있지만 TRE(230)에 의해 무결성 보호되는 M2ME(110) 내의 측정 컴포넌트에 의해 부가적인 체크가 일어날 수 있다. 이러한 후단계 체크에서, 나머지 M2ME(110)의 다른 컴포넌트, 구성, 또는 파라미터의 무결성은, 그것들이 로딩되거나 시작될 때, 또는 측정 컴포넌트가 이용할 수 있게 되는 임의의 기타 미리 정의된 실행 시간 이벤트에 체크된다.

[0100] PVA(150)와 같은 원격 엔티티는 M2ME(110)가 반자율 확인 테스트를 통과했다는 사실을 간접적으로 알게될 수 있다. 확인 결과의 네트워크에의 명시적인 시그널링이 존재한다. 440에서, 이 시그널링은 TRE(230)로부터 발신되어야 하고, 암호로 보호되어야 한다. 또한, 시그널링은 다운로드의 목표인 M2ME(110) 컴포넌트의 무결성을 보장하도록 MID 다운로드에 필요한 M2ME(110) 인증에 앞선다. 시그널링은 또한 실제 유효성 체크에 사용된 M2ME(110)에서의 리소스와 TRE의 인증 사이의 바인딩의 증거를 포함할 수 있다. 이러한 증거는, TRE(230)와 M2ME(110)의 증명(certification)을 확립하기 위한 부가적인 정보를 제공하는, M2ME(110)로부터 네트워크로 보내진 토큰을 포함할 수 있다.

[0101] 도 5는 TRE(230)의 무결성의 반자율 확인을 위한 대안의 절차(500)를 도시한다. 510에서, 절차(500)는 PVA(150) 또는 SHO(140)가 확인을 주기적으로 수행하도록 TRE(230)에 요청할 때 시작된다. 요청은 M2ME(110)가 처음에 등록된 후에 보내질 수 있거나, 요청은 M2ME(110)가 SHO와 맨 처음에 인증될 때 한 번 보내질 수 있다.

[0102] 대안으로서, 요청은 PVA(150) 또는 SHO(140)로부터의 보호된 운영 유지보수(OAM; operation and maintenence) 메시지로서 주기적으로 보내질 수 있다. '주기적 재확인(re-validation)'의 주기는 비교적 길지만, 확인의 '신선도(freshness)'에 대하여 SHO(140)가 안전하게 느낄 정도로 충분히 짧을 수 있다.

[0103] 다음으로, 520에서, TRE(230)는 요청에 기초하여 확인 절차를 수행한다. 성공적인 확인시, 530에서, TRE(230)는 PVA에 확인 응답 메시지를 보내며, 이는 마지막 확인이 일어난 때를 표시하는, TRE(230)에 의해 이루어진 타임스탬프를 포함할 수 있다. 대안으로서, TRE(230)는 주기적 확인 사이클의 현재 라운드의 만료 전에 마지막

확인이 일어났다는 것을 서술하는 메시지를 보낼 수 있다.

[0104] 확인의 '결과'에 대해 어떠한 명시적인 시그널링도 없으며, 단지 규정된 주기적인 확인이 실제로 일어났다는 것을 표시하는 인증 요청의 일부로서의 일부 간접적인 표시만 있다는 것을 유의하여야 한다. 이 표시는 이것이 수행되었을 때의 날짜 또는 시간을 포함하는 것일 수 있다.

[0105] 도 6은 M2ME의 무결성을 원격으로 확인하는 절차(600)의 예이다. 절차(600)를 시작하기 위해, 610에서, M2ME(110)는 미리 정의된 보안 상태로 시작할 수 있다. 보안 상태를 달성하면, 620에서, M2ME(110)는 TRE(230)가 플랫폼 확인의 증거를 생성할 것을 요청할 수 있다. 다음으로, 630에서, TRE(230)는 나머지 M2ME(110)로부터 이러한 증거를 생성하는데 사용될 재료를 수집한다. 예를 들어, 재료는 M2ME(110)에서의 보안 결정적인(security-critical) 실행 코드, M2ME의 운영 체제(OS)에 대한 크리덴셜, 장비 ID 등을 포함할 수 있다. 그러면, 640에서, TRE(230)는 M2ME(110)의 확인을 위한 증거를 생성하고, 무결성 및/또는 비밀을 위해 그것을 암호로 보호한다. 다음으로, 650에서, TRE(230)는 M2ME(110)에 보호된 증거를 전달한다. 660에서, M2ME(110)는 PVA(150)에 보호된 증거를 전송한다.

[0106] 보호된 증거를 수신하면, 670에서, PVA(150)는 증거를 평가하고, M2ME(110)가 계속해서 디바이스 인증을 수행할 수 있고 MID의 다운로드를 허용할 만큼 충분히 신뢰성이 있는지 결정한다.

[0107] 선택적으로, 상기 기재된 절차의 요소들의 일부는 MID의 다운로드에 대하여 전제조건인 M2ME 인증에 사용된 프로세스와 통합될 수 있다. TRE(230)와 PVA(150) 사이의 통신은 보호되어야 함을 유의해야 한다.

[0108] 상기 기재한 3개 확인 절차 중 임의의 절차가 수행된 후에, M2ME 확인과 인증 사이의 바인딩은 많은 시나리오에서 바람직할 수 있다. 자율 확인의 경우에, 확인은 M2ME(110)의 보안 상태를 입증하는 M2ME(110)의 일부 증명서 또는 크리덴셜일 수 있다. 기타 확인 절차의 경우에, 확인은 M2ME(110)의 보안 상태의 증명의 보다 안전한 수단을 포함할 수 있다. M2ME의 TRE(230)는 M2ME(110)의 확인을 수행하는데 사용된 M2ME 내부 리소스의 보안 특성을 보장하는 신뢰 환경이기 때문에, 인증에 사용된 크리덴셜에 대한 확인의 결과 및/또는 크리덴셜의 바인딩이 있어야 한다.

[0109] M2ME(110)를 인증하기 위한 3가지 절차가 있다. 첫 번째로, 최초 네트워크 접속을 위한 전제조건으로서, 원시 M2ME(110)가 ICF(160)에 의해 인증될 수 있다. 두 번째로, MID의 다운로드를 위한 전제조건으로서(예를 들어, 자신의 크리덴셜을 갖는 USIM 애플리케이션), M2ME(110)는 인증된 TRE(230)를 포함하는 것을 증명하도록 DPF(180)와 같은 엔티티에 의해 인증될 수 있다. 세 번째로, 동작적 네트워크 액세스에 대하여(예를 들어, 다운로딩된 MID를 사용하여), M2ME(110)는 SHO(140)에 의해 인증될 수 있다.

[0110] 자율 확인은 상기 기재한 바와 같이 최초 네트워크 접속에 사용되는 인증 절차에 바인딩될 수 있는 유일한 유형의 확인이다. 상기 기재한 다른 2개의 확인 방법은 PVA(150)의 참여를 필요로 하지만, 어떠한 최초 접속도 없으며, M2ME(110)가 확인을 위해 PVA(150)를 관여하게 하는 것이 가능하지 않다.

[0111] 최초 네트워크 접속의 경우, 네트워크 액세스 인증에 대한 무결성/확인의 바인딩은 단지 자율 확인에 대해서 암시적일 수 있는데, 네트워크 어태치가 발생한 후까지 무결성/유효성의 어떠한 네트워크 기반 체크도 수행되지 않기 때문이다. 다른 2개 형태의 확인의 경우, M2ME(110) 내의 TRE(230)의 아이덴티티에 대해 부가적인 정보와, 따라서 TRE(230)의 보안 기능 및 M2ME(110)의 무결성을 제공하는 최초 어태치 메시지에서 (TRE(230)의 증명 및 크리덴셜을 입증하는 디지털 증명서와 같은) 토큰이 전달될 수 있다.

[0112] 동작적 접속에 대하여, 반자율 확인 뿐만 아니라 원격 확인이 있을 수 있다. 또한, 후속 인증 단계들에 대한 이러한 확인 방법의 바인딩이 있을 수 있다. 플랫폼 확인과 인증의 바인딩을 달성하기 위한 2가지 방식이 아래에서 설명된다.

[0113] 첫 번째로, 인증 크리덴셜을 M2ME(110)에 보유하는 TRE(230)의 논리적 바인딩이 있을 수 있다. 인증 동안, 디바이스 플랫폼의 무결성이 확인된다. 논리적 바인딩(예를 들어, SIM 잠금)에 대한 초기 솔루션을 빠르게 피했다는 것을 유의해야 한다. 그러나, TCG와 같이 성공적으로 적용될 수 있는 다른 더 새로운 방법들이 존재한다.

[0114] 두 번째로, M2ME(110)에 대한 TRE(230)의 물리적 바인딩이 있을 수 있다. TRE(230) 인증 동안, 디바이스 플랫폼의 무결성이 확인된다.

[0115] 상기 둘 다의 경우에, 플랫폼 리소스의 실제 확인은, M2ME(110)로 안전하게 내장된 하드웨어 보안 컴포넌트의 기능을 사용함으로써(즉, 내장된 TRE) 또는 TRE(230)의 외부에 있을 수 있지만 그의 보안 특성이 TRE(230)에 의해 보장되고 TRE(230)에의 보안 접속을 갖는 하드웨어 보안 컴포넌트를 사용함으로써, 수행되어야 한다. 3GPP

AKA 인증에 사용된 애플리케이션 및 크리덴셜은 호스팅 디바이스에서 보안 하드웨어 컴포넌트의 바인딩을 확인할 목적으로 지정되지 않는다는 것을 유의해야 한다.

[0116] 확인 및 인증의 단계들은 일반적인 프로토콜의 세션에서 결합될 수 있다. 예를 들어, 3GPP는 디바이스 및 호스팅 측에 대한 인증 단계들을 결합할 방법으로서 IKEv2를 사용한다. 동일한 프로토콜이 또한 결합된 확인/인증 절차에서의 사용을 위해 고려될 수 있다.

[0117] 도 7은 인증된 액세스의 경우 M2ME(110)에의 MID의 프로비져닝 및 재프로비져닝에 대한 제1 예시적인 절차(700)를 도시한다. 이 절차가 예시 목적으로 제공되어 있지만, 네트워크 엔티티들 간의 다른 상호작용이 마찬가지의 결과를 가지도록 가능하다. 도 7에서, 화살표들은 기능, 서비스 제공자, 및 확인 권한자들 사이의 접속을 나타낸다. 실선 화살표는 M2ME(110)로부터 VNO(115)로의 최초 네트워크 액세스를 위한 무선 인터페이스를 나타내고, 파선(dashed) 화살표는 VNO의 네트워크에 의해 제공된 무선 인터페이스를 통하여 M2ME(110)와 ICF(160) 사이의 접속을 나타내고, 점선(dotted) 화살표는 ICF(160)에 의해 제공된 IP 접속 및 VNO의 네트워크의 무선 인터페이스를 통해 DPF(170)와 PVA(150), M2ME(110)와 DPF(180) 사이의 접속을 나타낸다. ICF(160), DRF(170), 및 DPF(180)는 전부 개별 엔티티로서 도시되어 있지만, 당해 기술 분야에서의 숙련자라면, 이들이 또한 도 1에 도시된 바와 같이 하나의 단일 엔티티 내에 위치될 수 있으며, 또는 일부 기타 구성에서 본질적으로 동일한 기능을 달성한다는 것을 알 것이다.

[0118] 도 7의 절차(700)에서, M2ME(110)에의 MID의 다운로딩 및 프로비져닝은 M2ME(110)가 그의 최초 네트워크 액세스에서 3G VNO의 네트워크에 액세스할 때 발생할 수 있다. VNO(115)는 다음 절차에 따라 M2ME(110)에의 무선 인터페이스를 제공한다.

[0119] M2ME(110)는 예를 들어 네트워크 정보를 디코딩하고 어태치 메시지를 사용하여 VNO(115)의 네트워크에 어태치하는데 표준 GSM/UMTS 원리(GPRS/PS)를 사용할 수 있다. 701에서, 어태치 메시지에서, M2ME(110)는 VNO(115)에 임시 M2ME ID, 또는 PCID를 보내고, M2ME(110)는 VNO(115)에 의한 표준 UMTS AKA 절차에 의해 인증된다. PCID의 컨텐츠 및 구조는 VNO(115)가 IMSI로서 그것을 인식하도록 이루어진다.

[0120] VNO의 네트워크에 대한 최초 어태치를 위한 클라이언트 인증을 수행할 수 있기 위하여, M2ME(110)는 M2ME와 VNO(115) 전부에 의해 공유되는 Milenage 알고리즘과 같은 인증 알고리즘을 지원할 필요가 있다는 것을 유의하여야 한다.

[0121] 702에서, M2ME(110)에 대한 ID로서 PCID를 인식하는 VNO(115)는 적법한 예비 크리덴셜로서 PCID를 수락할 ICF(160)에 접촉한다. 그러면, 703에서, ICF(160)는 M2ME(110)와의 부가적인 통신을 보호하도록 예비 인증 벡터(AV)의 세트를 발행하고, M2ME(110)에 보호된 IP 접속을 제공하기 시작한다. 이 통신은 VNO의 네트워크에 의해 제공된 무선 인터페이스를 사용하여 수행된다.

[0122] 다음으로, 704에서, M2ME(110) 및 ICF(160)는 M2ME(110)에 대한 통신을 보호할 예비 AKA 키를 생성하도록 표준 AKA 프로세스를 수행한다. 나중에 그리고 M2ME(110)가 SHO의 MID 크리덴셜을 사용하여 그것들을 다운로딩 및 프로비져닝한 후에 네트워크에 접속할 때까지, M2ME(110)와 다양한 네트워크 엔티티들 간의 모든 통신은 ICF(160)에 의해 제공된 IP 접속 및 암호 보호와 VNO의 네트워크에 의해 제공된 무선 인터페이스를 통해 행해진다.

[0123] 그 다음, ICF(160)는 M2ME(110)를 DPF(180)로 재지향시킨다. 그리 함에 있어서, 705에서, ICF(160)는 DRF(170)에 PCID를 보낼 수 있다. 그러면, 706에서, DRF(170)는 M2ME(110)가 SHO(140)를 찾는 것을 돕는다. 다음으로, 707에서, DRF(170)는 SHO(140)에 접속하고, SHO의 네트워크에의 접속을 위해 M2ME(110)를 등록한다. 이에 응답하여, 708에서, SHO(140)는 M2ME(110)의 TRE(230)의 진위 및 무결성을 확인하도록 PVA(150)에 요청한다. 그 다음, 709에서, PVA(150)는 M2ME(110)의 TRE(230)의 진위 및 무결성을 확인한다. 확인 절차는 도 3 내지 도 5에 관련하여 상기 기재한 확인 절차와 유사한 방식으로 수행될 수 있다.

[0124] 확인을 완료하면, 710에서, PVA(150)는 SHO(140)에 확인 결과를 보낸다. 711에서, SHO(140)는 DPF(180)에 접촉하고 M2ME(110)에 MID(USIM/ISIM 애플리케이션)의 프로비져닝을 권한 부여한다.

[0125] 다음으로, 712에서, DPF(180)는 M2ME(110)에 MID 객체를 다운로드한다. 그 다음, 713에서, M2ME(110)는 다운로딩된 MID를 TRE(230)로 프로비져닝하고, DPF(180)에 프로비져닝의 성공/실패 상태를 보고한다. M2ME(110)는 이러한 메시지의 확인에 사용될 수 있는 토큰을 보낼 필요가 있을 수 있다. 이러한 토큰은 조작 및 리플레이(replay) 공격에 내성이 있는 형태이어야 할 필요가 있을 것이다. 마지막으로, 714에서, DPF(150)는 SHO(140)

에 프로비져닝의 성공/실패 상태를 보고한다.

[0126] 도 8은 인증된 액세스의 경우 M2ME(110)에의 MID의 프로비져닝 및 재프로비져닝에 대한 다른 절차(800)를 도시한다. 이 절차(800)에서, M2ME(110)에의 MID의 다운로딩 및 프로비져닝(110)은 M2ME(110)가 그의 최초 네트워크 액세스에서 3G VNO의 네트워크에 액세스할 때 일어날 수 있다. ICF(160)는 M2ME(110)에 임시 인증 벡터를 해제하기 전에 그리고 또한 SHO(140)가 그의 MID의 다운로딩 및 프로비져닝을 권한 부여하기에 앞서 TRE(230) 확인이 일어나게 하는 대신 M2ME(110)에의 IP 접속을 허용하기 전에 M2ME(110)의 TRE(230)를 확인하도록 PVA(150)에 요청한다.

[0127] 801에서, 절차(800)는 M2ME(110)가 예를 들어 네트워크 정보를 디코딩하고 VNO(115)의 네트워크에 어태치하는데 표준 GSM/UMTS 원리(GPRS/PS)를 사용할 때 시작된다. 어태치 메시지에서, M2ME(110)는 VNO(115)에 PCID를 보낸다. M2ME(110)는 VNO(115)에 의해 표준 UMTS AKA 절차에 의해 인증된다.

[0128] 802에서, M2ME(110)에 대하여 PCID를 인식하는 VNO(115)는 적법한 예비 크리덴셜로서 PCID를 수락할 ICF(160)에 접촉한다. 다음으로, 803에서, ICF(160)는 M2ME(110)의 TRE(230)의 진위 및 무결성을 확인하도록 PVA(150)에 요청한다. 그러면, 804에서, PVA(150)는 M2ME(110)의 TRE(230)의 진위 및 무결성을 확인한다. 확인은 앞서 언급한 확인 절차들 중 하나를 사용하여 수행될 수 있다.

[0129] 805에서, PVA(150)가 ICF(160)에 확인 결과를 보내면, 806에서, ICF는 M2ME(110)와의 부가적인 통신을 보호하도록 예비 인증 벡터(AV) 세트를 발행하고, M2ME(110)에 보호된 IP 접속을 제공하기를 시작한다. 이 통신은 VNO의 네트워크에 의해 제공된 무선 인터페이스를 통하여 행해진다.

[0130] 다음으로, 807에서, M2ME(110) 및 ICF(160)는 M2ME(110)에 대한 통신을 보호하도록 예비 AKA 키를 생성하도록 표준 AKA 프로세스를 수행한다. 나중에 그리고 M2ME(110)가 SHO의 U(I)SIM 크리덴셜을 사용하여 그것들을 다운로딩 및 프로비져닝한 후에 네트워크에 접속할 때까지, M2ME(110)와 다양한 네트워크 엔티티들 간의 모든 통신은 ICF(160)에 의해 제공된 암호 보호와 IP 접속 및 VNO의 네트워크에 의해 제공된 무선 인터페이스를 통하여 행해진다.

[0131] 그 다음, 808에서, ICF(160)는 M2ME(110)를 DRF(170)로 지향시킨다. 그리 함에 있어서, ICF(160)는 DRF(170)에 PCID 뿐만 아니라 TRE 확인 상태에 관한 정보를 보낸다. 809에서, DRF(170)는 M2ME(110)가 그의 SHO(140)를 찾는 것을 도우며, M2ME(110)를 SHO(140)로 재지향시킨다. 그러면, 810에서, DRF(170)는 SHO(140)에 접속하고, SHO(140)에의 접속을 위해 M2ME(110)를 등록한다. 그리 함에 있어서, DRF(170)는 또한 TRE 확인 상태에 관한 정보를 SHO(140)에 전달한다.

[0132] DRF(170)로부터 수신한 TRE 확인 상태 정보를 검토한 후에, 811에서, SHO(140)는 DPF(180)에 접촉하고, M2ME(110)로의 MID(USIM/ISIM 애플리케이션)의 프로비져닝을 권한 부여한다. 이에 응답하여, 812에서, DPF(180)는 M2ME(110)에 MIS(U(I)SIM 애플리케이션 및 크리덴셜) 객체를 다운로드한다.

[0133] 813에서, M2ME(110)는 TRE(230)로 다운로딩된 MID를 프로비져닝하고, DPF(180)에 프로비져닝의 성공/실패 상태를 보고한다. M2ME(110)는 이러한 메시지의 확인에 사용될 수 있는 토큰을 보낼 수 있다. 이러한 토큰은 조작 및 리플레이 공격에 내성이 있는 형태로 이루어져야 한다. 마지막으로, DPF(180)는 SHO(140)에 프로비져닝의 성공/실패 상태를 보고한다.

[0134] 도 9는 새로운 SHO(도시되지 않음)에 대하여 M2ME(110)를 재프로비져닝하기 위한 절차(900)의 예시적인 흐름도이다. 910에서, 절차(900)는 M2ME 소유자가 M2ME 파라미터를 전달하도록 새로운 SHO에 접촉할 때 시작된다. 그러면, 920에서, M2ME 소유자는 재프로비져닝 절차를 개시하도록 M2ME에 접촉한다.

[0135] 930에서, 새로운 SHO는 M2ME(110)를 확인하도록 확인 엔티티에 요청한다. 그러면, 940에서, PVA(150)는 M2ME(110)를 확인하고 새로운 SHO에 성공/실패 메시지를 보낸다. 성공의 통지를 수신하면, 950에서, 새로운 SHO는 M2ME(110)에 새로운 MID(즉, USIM 애플리케이션 및 크리덴셜)를 다운로딩/프로비져닝하도록 DPF에 요청한다.

[0136] 그 다음, 960에서, DPF(180)는 M2ME(110)에 새로운 MID 패키지를 안전하게 다운로드한다. 970에서, M2ME(110)는 구(Old) MID가 폐기된 구 SHO에 메시지를 보낸다. 그러면, 980에서, 구 SHO는 M2ME(110)에 ACK를 보내고, M2ME(110)는 이어서 DPF(180)에 그 다음 새로운 SHO에 전송한다.

[0137] 990에서, M2ME(110)는 자신의 시스템을 업데이트하고 DPF(180)의 도움으로 MID를 설치하고, DPF(180)에 성공/실패 메시지를 보낸다. 992에서, DPF(180)는 새로운 SHO에 성공/실패 메시지를 보고한다. 성공시, 998에서, 프

로비져닝 프로세스가 완료된다.

[0138] 다른 재프로비져닝 절차에서, M2ME(110)는 원시 상태에 놓일 수 있고 도 7 및 도 8에 기재된 최초 프로비져닝 절차로서 동일한 유형의 프로세스를 재개시할 수 있다.

[0139] 다른 실시예에서, PVA(150)는 M2ME(110)가 여전히 동일한 SHO(140)에 가입되어 있는 동안에 수행된 임의의 소프트웨어(SW) 또는 펌웨어(FW) 업데이트가 보안 방식으로 행해질 것을 보장하는 일을 담당한다. 이는 크리덴셜의 업데이트 또는 재구성을 포함한다.

[0140] 이는 PVA(150) 또는 DPF(180)가 SW/FW의 보안 오버디에어 다운로딩 및 M2ME(110) 및/또는 TRE(230)의 재프로비져닝과 같은 절차들을 감독해야 함을 의미한다. 따라서, PVA(150) 또는 DPF(180)는 M2ME(110)의 보안 다운로딩, FLASH 업데이트, 및/또는 디바이스 재구성에 대하여 OMA DM 및 OMA FOTA 사양에서 제공된 것들과 같은 이용 가능한 방법을 채용할 수 있다.

[0141] 또한, M2ME의 신뢰 상태 정보는 원격 SW/FW 업데이트 또는 재구성으로 인해 변할 수 있기 때문에, PVA(150) 또는 DPF(180)는 SW/FW 업데이트 또는 재구성의 완료시 M2ME(110) 또는 TRE(230)의 실행시간 신뢰상태 정보 체크 또는 새로운 검증가능한 부트를 개시하여 그 결과를 획득할 수 있어야 한다. PVA(150) 또는 DPF(180)는 또한 M2ME(110)에 관한 신뢰 상태 정보의 각자의 데이터베이스를 업데이트하여야 한다. DPF(180)가 원격 SW/FW 업데이트 또는 원격 크리덴셜 재구성을 담당하는 경우에, M2ME(110)에 관한 '신뢰 상태' 정보에 대한 업데이트/재구성의 임의의 예상되는 효과가 DPF(180)로부터 PVA(150)에 보내져야 하며, 그리하여 PVA(150)는 M2ME(110)에 대한 '신뢰 상태' 정보의 그의 데이터베이스를 업데이트할 수 있다.

[0142] 또한, M2ME(110)의 조작의 검출 및 이에 대항하는 검출후(post-detection) 치료 반응에 대한 솔루션이 개시된다. M2ME(110)를 조작 공격에 덜 취약하게 하기 위하여, 여러 솔루션들이 제안된다.

[0143] 첫 번째로, M2ME(110)는 충분히 빈번하고(규칙적으로 스케쥴링된 검출 시도의 경우) 그리고/또는 시기적절하게(이벤트로 구동되는 검출 시도의 경우) 그것 또는 그것 내의 임의의 서브시스템(들)에 행해진 특정 유형의 '조작'을 검출할 수 있는 기능을 갖도록 구성될 수 있다. 이러한 검출가능한 조작 이벤트의 예는, (1) 멀웨어(malware) 또는 바이러스에 의한 OS의 치료가능 및/또는 치료불가능한 중간물(compromise), (2) 버퍼 오버플로우 이벤트, (3) 무선 또는 상위 계층 접속 특성 및/또는 환경 판독(environmental readings)의 갑작스런 예상치 못하거나 인가되지 않은 변화, (4) 예비 인증, 등록, 또는 MID 프로비져닝에 대한 M2ME의 요청에 대한 신뢰 네트워크 요소에 의한 액세스 또는 서비스의 거부 및/또는 과도하게 반복되는 실패, 또는 (5) 원격 MID 관리 기능에 관련된 M2ME 서브시스템 또는 M2ME(110)의 '신뢰 상태' 의 부트후 또는 실행시간 판독의 임의의 예상치못한/인가되지 않은 변화를 포함할 수 있지만, 이에 한정되는 것은 아니다. 도 1에 기재된 PVA(150), ICF(160), 또는 임의의 기타 네트워크 요소와 같은 네트워크 요소는 또한 조작을 검출하도록 구성될 수 있다. 예를 들어, 네트워크 요소는 M2ME(110)의 기능 및/또는 각자의 기능을 사용하여 M2ME(110)에 행해진 특정 유형의 '조작'을 원격으로 검출하도록 구성될 수 있다. 또한, 네트워크 요소는 임의의 조작 검출 이벤트에 대해 보고할 것을 M2ME(110)에 요청하도록 구성될 수 있다.

[0144] 자체적으로 임의의 조작의 자가검출(self-detection)시, M2ME(110)는 그에 또는 기타 네트워크 요소에 대한 부가적인 손상을 제한할 단계들을 취해야 한다. 예를 들어, 조작의 검출시, M2ME(110)는 원격 MID 관리에 관련된 기능들을 디스에이블하도록 구성될 수 있다. M2ME(110)는 또한 SIM 및/또는 TPM/MTM과 같은 원격 MID 관리 관련 데이터, 코드, 또는 크리덴셜을 보유하는 M2ME(110)의 TRE(230) 또는 기타 부분과 같은 M2ME(110)의 미리 지정된 매우 민감한 영역에 M2ME(110)의 내부 리소스(SW 또는 OS의 특정 부분과 같은)에 의한 액세스를 디스에이블하도록 구성될 수 있다.

[0145] 조작의 자가검출시, M2ME(110)는 또한 의심되거나 검출된 조작 이벤트 뿐만 아니라 M2ME(110)가 취한 검출후(post-detection) 자가 치료 또는 재활성 동작의 이벤트의 보고를 (PVA와 같은) 지정된 네트워크 요소에 보내도록 구성될 수 있다. 이러한 이벤트 보고는 또한 이벤트의 타임스탬프 또는 M2ME(110)의 가장 최근의 GPS 판독 또는 이웃 셀들의 리스트와 같은 이벤트의 위치 정보 스탬프까지도 포함할 수 있다는 것을 유의해야 한다.

[0146] 또한 조작의 검출시, M2ME(110)는 최근의 SW 업데이트, 또는 의심되는 바이러스 또는 멀웨어 코드 또는 데이터를 삭제하거나 격리하거나 또는 언인스톨하는 것과 같은 치료 동작을 수행하도록 구성될 수 있다. M2ME(110)는 또한 일시적인(예를 들어, RAM) 및/또는 영구적인(예를 들어, NVRAM, Flash, 하드 디스크, SIM, TPM/MTM 내부 또는 암호화된 저장 영역 등) 저장장치로부터 USIM 관련 키 또는 크리덴셜과 같은 원격 MID 관리 기능에 관련된 임의의 미리 지정된 데이터 세트를 삭제하도록 구성될 수 있다.

[0147] 마지막으로, 조작의 검출시, M2ME(110)는 또한 원격 MID 관리 기능을 처리하는 단말기의 서브시스템/부분 또는 M2ME(110)를 파워다운하도록 구성될 수 있다.

[0148] PVA(150)와 같은 특정 네트워크 요소는 또한, (1) 의심되거나 검출된 조작 이벤트를 보고했거나, 또는 (2) 조작 이벤트를 경험하도록 PVA(150) 자체 또는 그와 상호작용한 기타 네트워크 요소에 의해 의심되는, M2ME(110)를 대신하여 원격 '검출후' 반응 동작을 개시하고 수행하는 일을 담당하고 이를 수행할 수 있다.

[0149] 상기 기재한 특징 및 실시예는 3G UMTS 네트워크 액세스에 대한 인증을 위해 필요한 것들이 아닌 다른 인증 프로토콜에 적용 가능하다. 이러한 프로토콜의 예로는, 비(non)3G 액세스 네트워크에 대한 GSM/UMTS 단말기의 인증에 대하여 SIM(EAP-SIM)에 기초한 확장성 인증 프로토콜 및 애플리케이션 계층 인증에 사용되는 GBA(generic bootstrapping architecture)에 따르는 것들을 포함할 수 있지만, 이에 한정되지 않는다. 예를 들어, 도 1에 기재된 네트워크 요소가 존재할 수 있고 서비스, 애플리케이션, 또는 (비3G) 네트워크 액세스에 대한 M2ME 디바이스의 인증 및 아이덴티티의 인증 및 원격 관리를 허용하기 위하여 유사하거나 동일한 기능을 수행할 수 있다.

[0150] 특징 및 구성요소가 특정 조합으로 상기에 설명되었지만, 각각의 특징 또는 구성요소는 다른 특징 및 구성요소 없이 단독으로 사용될 수 있거나, 다른 특징 및 구성요소와 함께 또는 다른 특징 및 구성요소 없이 다양한 조합으로 사용될 수 있다. 여기에 제공된 방법 또는 흐름도는 범용 컴퓨터 또는 프로세서에 의한 실행을 위해 컴퓨터 판독가능한 저장 매체에 포함된 컴퓨터 프로그램, 소프트웨어 또는 펌웨어로 구현될 수 있다. 컴퓨터 판독가능한 저장 매체의 예로는 판독 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 레지스터, 캐시 메모리, 반도체 메모리 디바이스, 내부 하드 디스크 및 이동식 디스크와 같은 자기 매체, 자기 광학 매체, 및 CD-ROM 디스크 및 DVD와 같은 광학 매체를 포함한다.

[0151] 적합한 프로세서는 예로써, 범용 프로세서, 특수 용도 프로세서, 종래 프로세서, 디지털 신호 프로세서(DSP), 복수의 마이크로프로세서, DSP 코어와 연관되는 하나 이상의 마이크로프로세서, 컨트롤러, 마이크로컨트롤러, ASIC(Application Specific Integrated Circuit), FPGA(Field Programmable Gate Array) 회로, 임의의 기타 유형의 집적 회로(IC), 및/또는 상태 머신을 포함한다.

[0152] 소프트웨어와 연관된 프로세서는 무선 송수신 유닛(WTRU), 사용자 기기(UE), 단말기, 기지국, 무선 네트워크 컨트롤러(RNC), 또는 임의의 호스트 컴퓨터에 사용하기 위한 무선 주파수 트랜시버를 구현하는데 사용될 수 있다. WTRU는 카메라, 비디오 카메라 모듈, 비디오폰, 스피커폰, 진동 장치, 스피커, 마이크로폰, 텔레비전 트랜시버, 핸즈프리 헤드셋, 키보드, 블루투스®

모듈, 주파수 변조(FM) 라디오 유닛, LCD 디스플레이 유닛, OLED 디스플레이 유닛, 디지털 뮤직 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저, 및/또는 임의의 무선 로컬 영역 네트워크(WLAN) 또는 초광대역(UWB) 모듈과 같이 하드웨어 및/또는 소프트웨어로 구현되는 모듈과 함께 사용될 수 있다.

[0153] 실시예

[0154] 1. M2M 통신을 수행하는 방법.

[0155] 2. 실시예 1에 있어서, 통신은 인증, 프로비져닝, 또는 재프로비져닝 중 하나 이상을 포함하는 것인 방법.

[0156] 3. 실시예 1 또는 2에 있어서, M2M 가능 장비(M2ME)에서 방문 네트워크 오퍼레이터(VNO)의 네트워크에 접속하는 것을 더 포함하는 방법.

[0157] 4. 실시예 1 내지 3 중 어느 하나에 있어서,

[0158] 선택 홈 오퍼레이터(SHO)의 네트워크에 접속하는데 대한 권한 부여를 수신하는 것을 더 포함하는 방법.

[0159] 5. 실시예 1 내지 4 중 어느 하나에 있어서,

[0160] SHO의 네트워크에 접속하는 것을 더 포함하는 방법.

[0161] 6. 실시예 1 내지 5 중 어느 하나에 있어서, VNO는 단일 네트워크 엔티티인 것인 방법.

[0162] 7. 실시예 1 내지 6 중 어느 하나에 있어서, VNO는 복수의 네트워크 엔티티들을 포함하는 것인 방법.

[0163] 8. 실시예 1 내지 7 중 어느 하나에 있어서, VNO는 최초 등록 및 프로비져닝의 목적을 위해 액세스되는 임의의 액세스 네트워크인 것인 방법.

[0164] 9. 실시예 1 내지 8 중 어느 하나에 있어서, 등록 및 프로비져닝은 USIM/ISIM 애플리케이션의 등록 및 프로비져

닝을 포함하는 것인 방법.

[0165] 10. 실시예 1 내지 9 중 어느 하나에 있어서,

[0166] M2ME가 VNO가 아닌 SHO에 등록하고;

[0167] VNO가 VNO로 남는 것을 더 포함하는 방법.

[0168] 11. 실시예 1 내지 10 중 어느 하나에 있어서,

[0169] M2ME가 VNO인 SHO에 등록하고;

[0170] VNO가 SHO가 되는 것을 더 포함하는 방법.

[0171] 12. 실시예 1 내지 11 중 어느 하나에 있어서, VNO는 M2ME에 임시 네트워크 액세스를 제공하는 일을 담당하는 것인 방법.

[0172] 13. 실시예 1 내지 12 중 어느 하나에 있어서, 임시 네트워크 액세스는 임시 네트워크 액세스 크리덴셜에 기초하는 것인 방법.

[0173] 14. 실시예 1 내지 13 중 어느 하나에 있어서, 임시 네트워크 액세스 크리덴셜은 PCID 또는 임의의 기타 임시 비공개 ID를 포함하는 것인 방법.

[0174] 15. 실시예 1 내지 14 중 어느 하나에 있어서,

[0175] VNO가 탐색 및 등록 기능부(DRF)에 개방 네트워크 액세스를 제공하는 것을 더 포함하는 방법.

[0176] 16. 실시예 1 내지 15 중 어느 하나에 있어서, 적어도 DRF의 서비스에 대한 액세스에 어떠한 크리덴셜 또는 인증도 요구되지 않는 것인 방법.

[0177] 17. 실시예 1 내지 16 중 어느 하나에 있어서, VNO는 VNO가 SHO가 되지 않을 것일 때 DRF에 개방 네트워크 액세스를 제공하는 것인 방법.

[0178] 18. 실시예 1 내지 17 중 어느 하나에 있어서,

[0179] VNO가 프로비져닝된 USIM/ISM 애플리케이션을 사용하여 풀 네트워크 액세스를 제공하는 것을 더 포함하는 방법.

[0180] 19. 실시예 1 내지 18 중 어느 하나에 있어서, 풀 네트워크 액세스는 IMS를 포함하는 것인 방법.

[0181] 20. 실시예 1 내지 19 중 어느 하나에 있어서, RO는 ICF, DRF, 및 다운로딩 및 프로비져닝 기능부(DPF) 중 하나 이상을 포함하는 것인 방법.

[0182] 21. 실시예 1 내지 20 중 어느 하나에 있어서, ICF, DRF, 및 DPF는 각각 개별 엔티티에 위치되는 것인 방법.

[0183] 22. 실시예 1 내지 21 중 어느 하나에 있어서, ICF는 동작적 네트워크 액세스의 등록 및 프로비져닝의 목적을 위해 통신 네트워크에 대한 임시 액세스를 허용하는 크리덴셜의 확인을 담당하는 것인 방법.

[0184] 23. 실시예 1 내지 22 중 어느 하나에 있어서,

[0185] ICF가 임시 네트워크 액세스 크리덴셜을 발행하는 것을 더 포함하는 방법.

[0186] 24. 실시예 1 내지 23 중 어느 하나에 있어서,

[0187] ICF가 M2ME에 대하여 임시 비공개 식별자를 발행하는 것을 더 포함하는 방법.

[0188] 25. 실시예 1 내지 24 중 어느 하나에 있어서, 임시 네트워크 액세스 크리덴셜 또는 임시 비공개 식별자는 인증된 최초 임시 네트워크 액세스에 사용되는 것인 방법.

[0189] 26. 실시예 1 내지 25 중 어느 하나에 있어서,

[0190] ICF가 M2M 키, 구성, 및 애플리케이션 중 하나 이상을 이용해 M2ME를 프로비져닝하는 것을 더 포함하는 방법.

[0191] 27. 실시예 1 내지 26 중 어느 하나에 있어서, 프로비져닝은 오버 디 에어 프로비져닝을 포함하는 것인 방법.

[0192] 28. 실시예 1 내지 27 중 어느 하나에 있어서,

[0193] ICF가 M2ME를 사전 구성하도록 장비 공급자(E/S)에게 크리덴셜을 제공하는 것을 더 포함하는 방법.

[0194] 29. 실시예 1 내지 28 중 어느 하나에 있어서, ICF는 M2ME로 그것들을 내장시키는 일을 담당하는 조직에 크리덴셜의 보안 전송을 제공하도록 구성되는 것인 방법.

[0195] 30. 실시예 1 내지 29 중 어느 하나에 있어서,

[0196] ICF가 데이터베이스에서 크리덴셜을 등록하는 것을 더 포함하는 방법.

[0197] 31. 실시예 1 내지 30 중 어느 하나에 있어서,

[0198] ICF가 써드파티로부터의 크리덴셜을 확인하라는 요청을 수신하고;

[0199] ICF가 크리덴셜 확인을 수행하는 것을 더 포함하는 방법.

[0200] 32. 실시예 1 내지 31 중 어느 하나에 있어서, 크리덴셜 확인은 써드파티에의 인증 벡터의 보안 전송을 포함하는 것인 방법.

[0201] 33. 실시예 1 내지 32 중 어느 하나에 있어서, 인증 벡터는 관련 데이터를 포함하는 것인 방법.

[0202] 34. 실시예 1 내지 33 중 어느 하나에 있어서, 모든 액세스 네트워크는 M2ME의 SHO에의 성공적인 등록 전에 방문 네트워크로 간주되는 것인 방법.

[0203] 35. 실시예 1 내지 34 중 어느 하나에 있어서, M2ME는 네트워크 변화 없이 종래 네트워크를 통하여 투과적으로 SHO에 접속하는 것인 방법.

[0204] 36. 실시예 1 내지 35 중 어느 하나에 있어서, DRF는 특정 SHO의 구매후 선택, 및 선택한 SHO에의 M2ME의 등록을 인에이블하는 것인 방법.

[0205] 37. 실시예 1 내지 36 중 어느 하나에 있어서, DRF는 독립 서비스인 것인 방법.

[0206] 38. 실시예 1 내지 37 중 어느 하나에 있어서, DRF는 SHO에 의해 운영되는 것인 방법.

[0207] 39. 실시예 1 내지 38 중 어느 하나에 있어서, SHO의 RO는 SHO의 3GPP 네트워크를 통하여 접촉될 수 있는 것인 방법.

[0208] 40. 실시예 1 내지 39 중 어느 하나에 있어서, SHO의 RO는 인터넷을 통하여 접촉될 수 있는 것인 방법.

[0209] 41. 실시예 1 내지 40 중 어느 하나에 있어서, SHO의 RO는 탐색 가능한 것인 방법.

[0210] 42. 실시예 1 내지 41 중 어느 하나에 있어서, SHO의 RO는 M2ME에서의 기능성을 사용하여 탐색 가능한 것인 방법.

[0211] 43. 실시예 1 내지 42 중 어느 하나에 있어서, DRF는 고객이 M2ME의 전달 후에 SHO를 선택할 수 있게 해주는 것인 방법.

[0212] 44. 실시예 1 내지 43 중 어느 하나에 있어서, DRF는 M2ME가 임시 인증된 네트워크 액세스나 제한된 개방 네트워크 액세스를 사용하여 RO에의 IP 접속을 가질 수 있게 해주는 것인 방법.

[0213] 45. 실시예 1 내지 44 중 어느 하나에 있어서, DRF는 M2ME가 VNO를 통하여 USIM/ISM 애플리케이션 프로비져닝을 요청할 수 있게 해주는 것인 방법.

[0214] 46. 실시예 1 내지 45 중 어느 하나에 있어서,

[0215] DRF가 프로비져닝 요청을 승인하고;

[0216] M2ME를 프로비져닝하도록 DPF에 권한 부여하는 것을 더 포함하는 방법.

[0217] 47. 실시예 1 내지 46 중 어느 하나에 있어서, DRF는 M2ME의 소유자에 의한 M2ME의 등록을 지원하는 것인 방법.

[0218] 48. 실시예 1 내지 47 중 어느 하나에 있어서, DRF는 M2ME의 SHO와의 연관을 지원하는 것인 방법.

[0219] 49. 실시예 1 내지 48 중 어느 하나에 있어서,

[0220] PVA를 통하여 M2ME의 크리덴셜을 사용하여 TRE의 진위를 확인하는 것을 더 포함하는 방법.

[0221] 50. 실시예 1 내지 49 중 어느 하나에 있어서,

[0222] DRF가 M2ME에 전송될 데이터의 패키지를 생성하는 것을 더 포함하는 방법.

[0223] 51. 실시예 1 내지 50 중 어느 하나에 있어서,

[0224] DRF가 M2ME에 전송될 데이터의 패키지를 획득하는 것을 더 포함하는 방법.

[0225] 52. 실시예 1 내지 51 중 어느 하나에 있어서,

[0226] DRF가 PS에 안전하게 데이터를 전송하는 것을 더 포함하는 방법.

[0227] 53. 실시예 1 내지 52 중 어느 하나에 있어서,

[0228] DPF가 M2ME에 전송될 데이터의 패키지를 생성하는 것을 더 포함하는 방법.

[0229] 54. 실시예 1 내지 53 중 어느 하나에 있어서,

[0230] DPF가 M2ME에 전송될 데이터의 패키지를 획득하는 것을 더 포함하는 방법.

[0231] 55. 실시예 1 내지 54 중 어느 하나에 있어서,

[0232] DPF가 PS에 안전하게 데이터를 전송하는 것을 더 포함하는 방법.

[0233] 56. 실시예 1 내지 55 중 어느 하나에 있어서,

[0234] DRF가 M2ME와 DPF 사이의 보안 연관의 설정을 용이하게 하는 것을 더 포함하는 방법.

[0235] 57. 실시예 1 내지 56 중 어느 하나에 있어서,

[0236] DRF가 보안 토큰을 생성하고 보안 채널을 통해 M2ME 및 DPF에 전송하는 것을 더 포함하는 방법.

[0237] 58. 실시예 1 내지 57 중 어느 하나에 있어서,

[0238] DPF가 M2ME에의 USIM/ISM 크리덴셜의 원격 프로비져닝을 인에이블하는 것인 방법.

[0239] 59. 실시예 1 내지 58 중 어느 하나에 있어서,

[0240] DPF가 M2ME를 프로비져닝하는데 대한 DRF로부터의 권한 부여를 수신하는 것을 더 포함하는 방법.

[0241] 60. 실시예 1 내지 59 중 어느 하나에 있어서, 권한 부여를 수신하는 것은 DPF가 M2ME와 통신하기 위한 보안 토큰을 수신하는 것을 포함하는 것인 방법.

[0242] 61. 실시예 1 내지 60 중 어느 하나에 있어서,

[0243] DPF가 DRF로부터 애플리케이션 패키지를 수신하는 것을 더 포함하는 방법.

[0244] 62. 실시예 1 내지 61 중 어느 하나에 있어서,

[0245] DPF가 저장된 규칙들로부터 애플리케이션 패키지를 생성하고;

[0246] DRF로 다운로딩된 크리덴셜을 DRF에 알려주는 것을 더 포함하는 방법.

[0247] 63. 실시예 1 내지 62 중 어느 하나에 있어서, DPF는 M2ME에의 USIM/ISIM 애플리케이션 또는 USIM/ISIM 파라미터의 프로비져닝을 지원하도록 구성되는 것인 방법.

[0248] 64. 실시예 1 내지 63 중 어느 하나에 있어서, DPF는 M2ME에의 USIM/ISIM 애플리케이션 또는 USIM/ISIM 파라미터에 대한 추후 업데이트를 수행하도록 구성되는 것인 방법.

[0249] 65. 실시예 1 내지 64 중 어느 하나에 있어서, DPF는 새로운 애플리케이션의 추후 프로비져닝을 수행하도록 구성되는 것인 방법.

[0250] 66. 실시예 1 내지 65 중 어느 하나에 있어서, DPF는 성공적이거나 성공적이지 않은 프로비져닝 이벤트를 DRF에 통지하도록 구성되는 것인 방법.

[0251] 67. 실시예 1 내지 66 중 어느 하나에 있어서, SHO는 M2ME의 사용자와의 상업적 관계를 갖는 네트워크 오퍼레이터인 것인 방법.

[0252] 68. 실시예 1 내지 67 중 어느 하나에 있어서, SHO는 고객에게 청구하는 일을 담당하는 것인 방법.

[0253] 69. 실시예 1 내지 68 중 어느 하나에 있어서, SHO는 DRF의 역할을 수행하는 것인 방법.

[0254] 70. 실시예 1 내지 69 중 어느 하나에 있어서, SHO는 DPF의 역할을 수행하는 것인 방법.

[0255] 71. 실시예 1 내지 70 중 어느 하나에 있어서, SHO는 다른 역할을 수행하는 것인 방법.

[0256] 72. 실시예 1 내지 71 중 어느 하나에 있어서, SHO는 DRF 및 DPF와 동작적 관계를 갖는 것인 방법.

[0257] 73. 실시예 1 내지 72 중 어느 하나에 있어서, DRF 및 DPF는 서로 동작적 관계를 갖는 것인 방법.

[0258] 74. 실시예 1 내지 73 중 어느 하나에 있어서, M2ME는 처음에 서비스 제공자와 함께 동작하도록 위임되지 않는 것인 방법.

[0259] 75. 실시예 1 내지 74 중 어느 하나에 있어서, M2ME는 VNO와 통신하여 RO에의 채널을 확립하는 것인 방법.

[0260] 76. 실시예 1 내지 75 중 어느 하나에 있어서, M2ME는 비공개 아이덴티티를 갖는 것인 방법.

[0261] 77. 실시예 1 내지 76 중 어느 하나에 있어서, PCID는 비공개 아이덴티티인 것인 방법.

[0262] 78. 실시예 1 내지 77 중 어느 하나에 있어서, 비공개 아이덴티티는 임의의 VNO가 M2ME를 인식하고 VNO의 서비스에 대한 임시 액세스를 허용하고 오퍼레이터와의 서비스를 다운로딩 및 프로비져닝하기 위하여 적합한 네트워크 컴포넌트로 최초 접속 메시지를 향하게 할 수 있게 하는 것인 방법.

[0263] 79. 실시예 1 내지 78 중 어느 하나에 있어서, PVA는 다운로딩된 USIM/ISIM 애플리케이션의 저장 및 실행에 사용되는 M2ME 내의 보안 디바이스의 진위를 입증하는 크리덴셜을 담당하는 것인 방법.

[0264] 80. 실시예 1 내지 79 중 어느 하나에 있어서, PVA는 크리덴셜을 발행하고 크리덴셜 확인 서비스를 제공하는 하나 이상의 상업적 조직을 포함하는 것인 방법.

[0265] 81. 실시예 1 내지 80 중 어느 하나에 있어서, 크리덴셜은 증명서와 키 쌍을 포함하는 것인 방법.

[0266] 82. 실시예 1 내지 81 중 어느 하나에 있어서, M2ME 내의 보안 디바이스는 UICC, TRE, 또는 일부 기타 보안 모듈 중 하나 이상인 것인 방법.

[0267] 83. 실시예 1 내지 82 중 어느 하나에 있어서, 보안 디바이스의 강한 인증이 USIM/ISIM 애플리케이션의 프로비져닝에 대한 전제 조건인 경우에 PVA 기능이 요구되는 것인 방법.

[0268] 84. 실시예 1 내지 83 중 어느 하나에 있어서,

[0269] M2ME 내의 보안 디바이스의 보안성을 입증하도록 크리덴셜을 생성하고 발행하는 것을 더 포함하는 방법.

[0270] 85. 실시예 1 내지 84 중 어느 하나에 있어서, M2ME 내의 보안 디바이스의 보안성을 입증하도록 크리덴셜을 생성하고 발행하는 것은 PVA에 의해 수행되는 것인 방법.

[0271] 86. 실시예 1 내지 85 중 어느 하나에 있어서, PVA는 M2ME 내의 보안 디바이스에 대한 크리덴셜의 확인을 제공하도록 구성되는 것인 방법.

[0272] 87. 실시예 1 내지 86 중 어느 하나에 있어서, PVA는 발행된 크리덴셜의 유효성에 관한 데이터의 유지를 제공하도록 구성되는 것인 방법.

[0273] 88. 실시예 1 내지 87 중 어느 하나에 있어서, 장비 공급자(E/S)는 임시 최초 네트워크 액세스에 대한 인증을 위해 ICF로부터 크리덴셜을 안전하게 획득하는 것인 방법.

[0274] 89. 실시예 1 내지 88 중 어느 하나에 있어서, E/S는 M2ME의 재구성을 지원하도록 구성되는 것인 방법.

[0275] 90. 실시예 1 내지 89 중 어느 하나에 있어서, 재구성은 예비 네트워크 액세스 크리덴셜을 이용해 M2ME를 프로비져닝하는 것을 포함하는 것인 방법.

[0276] 91. 실시예 1 내지 90 중 어느 하나에 있어서, E/S는 M2ME가 표준화된 보안 요건 세트에 따른다는 것을 ICF(160)를 통하여 DRF(170)에 증명하는데 사용하기 위한 크리덴셜을 PVA(150)로부터 안전하게 획득하도록 구성되는 것인 방법.

[0277] 92. 실시예 1 내지 91 중 어느 하나에 있어서, E/S는 크리덴셜을 이용해 M2ME를 구성하도록 구성되는 것인 방법.

[0278] 93. 실시예 1 내지 92 중 어느 하나에 있어서, E/S는 M2ME 소유자가 원하는 DRF 및 SHO를 선택할 수단을 제공하

도록 구성되는 것인 방법.

[0279] 94. 실시예 1 내지 93 중 어느 하나에 있어서, E/S는 M2ME가 액세스 네트워크에 접속될 때 발생할 자동 DRF 및 SHO 선택을 제공하도록 구성되는 것인 방법.

[0280] 95. 실시예 1 내지 94 중 어느 하나에 있어서, M2ME는 송신기, 수신기, 프로세서, TRE, GPS, SIM, 및 보안 시간 유닛 중 하나 이상을 포함하는 것인 방법.

[0281] 96. 실시예 1 내지 95 중 어느 하나에 있어서, M2ME는 많은 다양한 신뢰 메커니즘을 지원하도록 구성되는 것인 방법.

[0282] 97. 실시예 1 내지 96 중 어느 하나에 있어서, M2ME는 TRE, SIM, 또는 ISIM 중 하나 이상을 지원하도록 구성되는 것인 방법.

[0283] 98. 실시예 1 내지 97 중 어느 하나에 있어서, 신뢰 메커니즘은 공통 AKA 프로토콜로 완전히 통합되는 것인 방법.

[0284] 99. 실시예 1 내지 98 중 어느 하나에 있어서, 공통 AKA 프로토콜은 TRE에 의해 보호되는 키, 또는 신뢰 상태 정보 중 하나 이상을 포함하는 것인 방법.

[0285] 100. 실시예 1 내지 99 중 어느 하나에 있어서, AKA 프로토콜은 전체 AKA가 일어날 수 있기 전에 그리고 인증이 확립된 후에 M2ME와 네트워크 요소 사이의 임의의 통신을 보호하는 것인 방법.

[0286] 101. 실시예 1 내지 100 중 어느 하나에 있어서, SIM은 신뢰 프로세싱 모듈(TPM) 또는 이동 신뢰 모듈(MTM)의 기능을 포함하도록 강화되는 것인 방법.

[0287] 102. 실시예 1 내지 101 중 어느 하나에 있어서, SIM은 TPM 또는 MTM과 밀접하게 동작하도록 구성되는 것인 방법.

[0288] 103. 실시예 1 내지 102 중 어느 하나에 있어서, TRE는 SIM의 기능성을 수행하도록 구성되는 것인 방법.

[0289] 104. 실시예 1 내지 103 중 어느 하나에 있어서, M2ME는 AKA 루트 시크릿을 이용해 프로비져닝되는 것인 방법.

[0290] 105. 실시예 1 내지 104 중 어느 하나에 있어서, 루트 시크릿은 E/S에 의해 프로비져닝되는 것인 방법.

[0291] 106. 실시예 1 내지 105 중 어느 하나에 있어서, 루트 시크릿은 USIM에 의해 보호되는 것인 방법.

[0292] 107. 실시예 1 내지 106 중 어느 하나에 있어서, 루트 시크릿은 절대 변하지 않는 것인 방법.

[0293] 108. 실시예 1 내지 107 중 어느 하나에 있어서, 프로세서는 AKA 루트 시크릿으로부터 세션 키를 유도하도록 구성되는 것인 방법.

[0294] 109. 실시예 1 내지 108 중 어느 하나에 있어서, M2ME는 ICF에 신뢰 상태 정보를 제공하도록 구성되는 것인 방법.

[0295] 110. 실시예 1 내지 109 중 어느 하나에 있어서, 신뢰 상태 정보는 M2ME가 VNO에 어태치할 때 예비 인증에 사용될 수 있는 것인 방법.

[0296] 111. 실시예 1 내지 110 중 어느 하나에 있어서, 신뢰 상태 정보는 세션 키를 유도하는데 사용되는 것인 방법.

[0297] 112. 실시예 1 내지 111 중 어느 하나에 있어서, n은 세션 키 CKn 및 IKn의 가장 최근의 업데이트에 대한 인덱스를 칭하며, $\mathbf{CKn = f3K\,(RAND\,||\,PCR0n)}$, $\mathbf{IKn = f4K\,(RAND\,||\,PCR0\,n)}$ 이고, 여기에서 $f3_K()$ 및 $f4_K()$는 공유 마스터 시크릿 K 중에 암호 키와 무결성 키에 대한 AKA 키 유도 함수를 각각 칭하고, RAND는 CATNA에 의해 생성되고 AKA 프로세스에서 M2ME(110)에 보내짐에 따라 공유되는 인증 벡터(AV) 내의 랜덤 넌스이고, $PCR0_n$은 M2ME(110) 상의 MTME 안의 PCR0 레지스터의 가장 최근의 값을 칭하는 것인 방법.

[0298] 113. 실시예 1 내지 112 중 어느 하나에 있어서, PCR0 레지스터의 현재 값은 M2ME의 가장 최근의 부트후 신뢰 상태의 기술을 의미하는 것인 방법.

[0299] 114. 실시예 1 내지 113 중 어느 하나에 있어서, CKn 및 IKn의 값은 PCR0의 값이 부트들 사이에 변할 때 변하는 것인 방법.

[0300] 115. 실시예 1 내지 114 중 어느 하나에 있어서, ICF는 M2ME의 신뢰 상태에 대한 변화를 아는 것인 방법.

[0301] 116. 실시예 1 내지 115 중 어느 하나에 있어서, M2ME의 신뢰 상태에 대한 변화는 PCR0의 값에 대한 변화를 포함하는 것인 방법.

[0302] 117. 실시예 1 내지 116 중 어느 하나에 있어서, ICF에는 M2ME의 OS, 펌웨어, 또는 애플리케이션에 대한 스케쥴 및 내용이 통지되는 것인 방법.

[0303] 118. 실시예 1 내지 117 중 어느 하나에 있어서, ICF에는 M2ME의 신뢰 상태에 영향을 미치는 M2ME에 대한 임의의 변화가 통지되는 것인 방법.

[0304] 119. 실시예 1 내지 118 중 어느 하나에 있어서, M2ME와 ICF 사이에 공유되는 AKA 암호 및 무결성 키는 업데이트되고 M2ME의 인증에 유용하게 되는 것인 방법.

[0305] 120. 실시예 1 내지 119 중 어느 하나에 있어서, 세션 키는 M2ME의 가장 최근의 신뢰 상태 값을 반영하는 것인 방법.

[0306] 121. 실시예 1 내지 120 중 어느 하나에 있어서, 세션 키는 AKA 키 유도 프로세스의 보안성을 강화하는 것인 방법.

[0307] 122. 실시예 1 내지 121 중 어느 하나에 있어서, TRE는 M2ME에서의 논리적으로 분리된 영역인 것인 방법.

[0308] 123. 실시예 1 내지 122 중 어느 하나에 있어서, TRE의 논리적 분리에 대한 하드웨어 지원이 존재하는 것인 방법.

[0309] 124. 실시예 1 내지 123 중 어느 하나에 있어서, TRE는 탈착가능한 모듈인 것인 방법.

[0310] 125. 실시예 1 내지 124 중 어느 하나에 있어서, TRE는 비탈착가능한 모듈인 것인 방법.

[0311] 126. 실시예 1 내지 125 중 어느 하나에 있어서, TRE는 집적 회로(IC)와 함께 기능하는 것인 방법.

[0312] 127. 실시예 1 내지 126 중 어느 하나에 있어서, TRE 기능은 복수의 IC에 걸쳐 분포되는 것인 방법.

[0313] 128. 실시예 1 내지 127 중 어느 하나에 있어서, TRE는 외부 세계에 대한 논리적 및 물리적 인터페이스를 정의하는 것인 방법.

[0314] 129. 실시예 1 내지 128 중 어느 하나에 있어서, TRE에 의해 노출된 인터페이스는 권한 부여된 엔티티의 제어하에 사용 가능한 것인 방법.

[0315] 130. 실시예 1 내지 129 중 어느 하나에 있어서, TRE는 다수의 관리 아이덴티티(MID)에 대하여 보안 저장 및 보안 실행 환경을 위해 신뢰 루트를 제공하는 것인 방법.

[0316] 131. 실시예 1 내지 130 중 어느 하나에 있어서, TRE는 MID를 프로비져닝 및 관리하는 것을 제공하는 것인 방법.

[0317] 132. 실시예 1 내지 131 중 어느 하나에 있어서, MID는 보안 애플리케이션인 것인 방법.

[0318] 133. 실시예 1 내지 132 중 어느 하나에 있어서, MID는 가입 관리 기능, 보안 지불 애플리케이션, 가입 관리 아이덴티티, USIM 애플리케이션, ISIM 애플리케이션, 가상 SIM(vSIM), 또는 동적 보안 아이덴티티 솔루션 중 하나 이상을 포함하는 것인 방법.

[0319] 134. 실시예 1 내지 133 중 어느 하나에 있어서, TRE는 임의의 필요한 암호 키 및 기타 크리덴셜을 이용해 보안 대역외 설비에서 프로비져닝되는 것인 방법.

[0320] 135. 실시예 1 내지 134 중 어느 하나에 있어서, TRE는 물리적 및 논리적 공격에 대항하여 보호를 제공하는 것인 방법.

[0321] 136. 실시예 1 내지 135 중 어느 하나에 있어서, TRE는 자신의 보안 정책을 실시하는 것인 방법.

[0322] 137. 실시예 1 내지 136 중 어느 하나에 있어서, TRE는 MID의 저장 및 실행을 허용하도록 충분히 안전한 것인 방법.

[0323] 138. 실시예 1 내지 137 중 어느 하나에 있어서, TRE는 TRE 외부의 M2ME의 부분에 대한 인터페이스를 갖는 것인 방법.

[0324] 139. 실시예 1 내지 138 중 어느 하나에 있어서, TRE는 내장된 고유 아이덴티티를 갖는 것인 방법.

[0325] 140. 실시예 1 내지 139 중 어느 하나에 있어서, TRE의 아이덴티티는 M2ME의 아이덴티티와 연관되는 것인 방법.

[0326] 141. 실시예 1 내지 140 중 어느 하나에 있어서, TRE는 표준 프로토콜을 사용하여 발행 권한에 자신의 아이덴티티를 안전하게 인증하도록 구성되는 것인 방법.

[0327] 142. 실시예 1 내지 141 중 어느 하나에 있어서, TRE는 UICC에서 구현되는 것인 방법.

[0328] 143. 실시예 1 내지 142 중 어느 하나에 있어서, TRE는 M2ME에 의해 제공된 하드웨어 및 소프트웨어 컴포넌트를 사용하여 M2ME 상의 통합 솔루션으로서 구현되는 것인 방법.

[0329] 144. 실시예 1 내지 143 중 어느 하나에 있어서, TRE는 MID의 다운로딩 및 원격 프로비져닝 및 관리를 지원하는 것인 방법.

[0330] 145. 실시예 1 내지 144 중 어느 하나에 있어서, TRE는 관리 아이덴티티 실행(MIDE)의 기능성을 지원하는 것인 방법.

[0331] 146. 실시예 1 내지 145 중 어느 하나에 있어서, M2ME는 TRE 코드 베이스를 구성하는 소프트웨어 코드 및 데이터의 무결성 체크를 지원하는 것인 방법.

[0332] 147. 실시예 1 내지 146 중 어느 하나에 있어서, TRE는 M2ME의 파워업/부트시에 체크되는 것인 방법.

[0333] 148. 실시예 1 내지 147 중 어느 하나에 있어서, 코드 체크는 M2ME의 동작 사용 동안 수행되는 것인 방법.

[0334] 149. 실시예 1 내지 148 중 어느 하나에 있어서, 코드 체크는 정의된 간격으로 또는 특정 트리거에서 백그라운드 프로세스로서 수행되는 것인 방법.

[0335] 150. 실시예 1 내지 149 중 어느 하나에 있어서, 코드 체크는 M2ME의 부분적 또는 전체 체크를 커버하는 것인 방법.

[0336] 151. 실시예 1 내지 150 중 어느 하나에 있어서, TRE는 다수의 분리된 신뢰 도메인에 대한 지원을 포함하는 것인 방법.

[0337] 152. 실시예 1 내지 151 중 어느 하나에 있어서, 각각의 도메인은 이해관계자-소유자에 의해 소유되는 것인 방법.

[0338] 153. 실시예 1 내지 152 중 어느 하나에 있어서, 각각의 도메인은 다른 도메인과 분리되는 것인 방법.

[0339] 154. 실시예 1 내지 153 중 어느 하나에 있어서, 각각의 도메인은 조작 및 권한 부여되지 않은 액세스에 대항하여 보호되는 것인 방법.

[0340] 155. 실시예 1 내지 154 중 어느 하나에 있어서, TRE는 도메인간 서비스를 제공하는 것인 방법.

[0341] 156. 실시예 1 내지 155 중 어느 하나에 있어서, 도메인간 서비스는 인증 및 입증 기능성 중 하나 이상을 포함하는 것인 방법.

[0342] 157. 실시예 1 내지 156 중 어느 하나에 있어서, M2ME는 네트워크에 산발적으로 또는 드물게 접속하는 것인 방법.

[0343] 158. 실시예 1 내지 157 중 어느 하나에 있어서, M2ME는 휴면 상태에서 동작하는 것인 방법.

[0344] 159. 실시예 1 내지 158 중 어느 하나에 있어서, TRE의 소프트웨어 코드의 실행시간 무결성 체크는 M2ME가 휴면 상태에서 동작하는 동안에 일어나도록 구성되는 것인 방법.

[0345] 160. 실시예 1 내지 159 중 어느 하나에 있어서, 무결성 체크는 다른 M2ME 또는 TRE 프로세스를 방해하지 않는 것인 방법.

[0346] 161. 실시예 1 내지 160 중 어느 하나에 있어서, 무결성 체크의 상태는 M2ME가 SHO에 접속할 때 준비되는 것인 방법.

[0347] 162. 실시예 1 내지 161 중 어느 하나에 있어서, M2ME에는 M2ME에 고유한 임시 비공개 아이덴티티가 할당되는 것인 방법.

[0348] 163. 실시예 1 내지 162 중 어느 하나에 있어서, PCID는 시간 한정된 유효 기간 동안 유효한 것인 방법.

[0349] 164. 실시예 1 내지 163 중 어느 하나에 있어서, 유효 기간은 M2ME에 의해 실시되는 것인 방법.

[0350] 165. 실시예 1 내지 164 중 어느 하나에 있어서, 유효 기간은 TRE에 의해 제어되는 것인 방법.

[0351] 166. 실시예 1 내지 165 중 어느 하나에 있어서,

[0352] PCID를 제거하는 것을 더 포함하는 방법.

[0353] 167. 실시예 1 내지 166 중 어느 하나에 있어서, PCID는 동시에는 아니지만 하나보다 많은 수의 M2ME에 의해 사용될 수 있는 것인 방법.

[0354] 168. 실시예 1 내지 167 중 어느 하나에 있어서, PCID는 체계적으로 재할당되는 것인 방법.

[0355] 169. 실시예 1 내지 168 중 어느 하나에 있어서, 복수의 PCID가 M2ME에 프로비져닝되는 것인 방법.

[0356] 170. 실시예 1 내지 169 중 어느 하나에 있어서, M2ME는 크기 N의 그룹에 해제되는 것인 방법.

[0357] 171. 실시예 1 내지 170 중 어느 하나에 있어서, j번째 배치의 M2ME는 M_i,j라 칭하며, 여기에서 j=1,...,M인 것인 방법.

[0358] 172. 실시예 1 내지 171 중 어느 하나에 있어서, PCID 할당은 크기 NxM의 행렬 (P)_{i,j}로써 초기화될 수 있는 것인 방법.

[0359] 173. 실시예 1 내지 172 중 어느 하나에 있어서, M2ME M_i,1은 제조 동안 TRE로 로딩된 열 P_i,*을 얻는 것인 방법.

[0360] 174. 실시예 1 내지 173 중 어느 하나에 있어서, 보안 타이머 또는 단조 카운터가 초기화되고 활성화되며 TRE의 제어 하에 놓이는 것인 방법.

[0361] 175. 실시예 1 내지 174 중 어느 하나에 있어서, M2ME M_i,1은 초기화된 카운터 또는 시간에 기초하여 미리 결정된 횟수 또는 결정된 기간 T에 대하여 P_i,1을 사용하는 것인 방법.

[0362] 176. 실시예 1 내지 175 중 어느 하나에 있어서, TRE는 P_i,1을 폐기하고 P_i,2를 사용하는 것인 방법.

[0363] 177. 실시예 1 내지 176 중 어느 하나에 있어서, 네트워크는 디바이스가 라이프타임 사이클 내에 있는지 결정하도록 구성되는 것인 방법.

[0364] 178. 실시예 1 내지 177 중 어느 하나에 있어서, TRE에 의한 시간 제한의 실시 및 TRE로써 PCID 열 벡터를 처리하는 것은 PCID의 동시 사용을 막고 그의 동작 시간 전반에 걸쳐 M2ME가 유효한 PCID를 가짐을 보장하는 것인 방법.

[0365] 179. 실시예 1 내지 178 중 어느 하나에 있어서, M2ME는 PCID를 재프로비져닝하도록 구성되는 것인 방법.

[0366] 180. 실시예 1 내지 179 중 어느 하나에 있어서, 적어도 둘의 M2ME는 동시에 동일한 PCID를 사용하려고 시도하는 것인 방법.

[0367] 181. 실시예 1 내지 180 중 어느 하나에 있어서, PCID의 수는 배치 내의 M2ME의 수보다 더 큰 것인 방법.

[0368] 182. 실시예 1 내지 181 중 어느 하나에 있어서, PCID는 랜덤으로서 선택되는 것인 방법.

[0369] 183. 실시예 1 내지 182 중 어느 하나에 있어서, 복수의 M2ME의 클록이 동기화되는 것인 방법.

[0370] 184. 실시예 1 내지 183 중 어느 하나에 있어서, M2ME의 클록은 복수의 M2ME와 재동기화되는 것인 방법.

[0371] 185. 실시예 1 내지 184 중 어느 하나에 있어서, TRE는 시간 베이스를 보유하고 관리하도록 구성되는 것인 방법.

[0372] 186. 실시예 1 내지 185 중 어느 하나에 있어서, TRE는 신뢰된 시간 소스와의 동기화를 지원하도록 구성되는 것인 방법.

[0373] 187. 실시예 1 내지 186 중 어느 하나에 있어서, TRE는 M2ME에 위치된 신뢰된 시간 유닛에 의존하는 것인 방법.

[0374] 188. 실시예 1 내지 187 중 어느 하나에 있어서, M2ME는 자율 측위 장비를 포함하는 것인 방법.

[0375] 189. 실시예 1 내지 188 중 어느 하나에 있어서, TRE는 측위 장비에 대한 보안 액세스를 갖는 것인 방법.

[0376] 190. 실시예 1 내지 189 중 어느 하나에 있어서, 어떠한 두개의 M2ME도 동시에 동일한 액세스 네트워크 셀에의 무선 접속을 물리적으로 확립하지 않는 것인 방법.

[0377] 191. 실시예 1 내지 190 중 어느 하나에 있어서, M2ME는 목적지 측위점(D), 및 허용 범위(R)로써 프로비져닝되는 것인 방법.

[0378] 192. 실시예 1 내지 191 중 어느 하나에 있어서, D 및 R의 값은 TRE에 저장되는 것인 방법.

[0379] 193. 실시예 1 내지 192 중 어느 하나에 있어서, D 및 R의 값은 TRE만 데이터에 액세스할 수 있도록 암호로 보안되는 것인 방법.

[0380] 194. 실시예 1 내지 193 중 어느 하나에 있어서,

[0381] TRE가 그의 현재 측위 위치를 결정하고;

[0382] 현재 측위 위치를 R 내의 D와 비교하고;

[0383] 네트워크 액세스에 대하여 PCID를 해제하는 것을 더 포함하는 방법.

[0384] 195. 실시예 1 내지 194 중 어느 하나에 있어서, 액세스 네트워크는 PCID, 셀 ID 쌍의 기록을 유지하는 것인 방법.

[0385] 196. 실시예 1 내지 195 중 어느 하나에 있어서, M2ME에 의한 네트워크에의 액세스는 미리 결정된 복수의 셀에서 허가되는 것인 방법.

[0386] 197. 실시예 1 내지 196 중 어느 하나에 있어서, M2ME는 복수의 네트워크 셀 식별자로써 구성되는 것인 방법.

[0387] 198. 실시예 1 내지 197 중 어느 하나에 있어서, M2ME는 지리학적으로 이동되는 것인 방법.

[0388] 199. 실시예 1 내지 198 중 어느 하나에 있어서, 네트워크 액세스는 M2ME가 이동될 때 디스에이블되는 것인 방법.

[0389] 200. 실시예 1 내지 199 중 어느 하나에 있어서, M2ME는 PCID가 사용될 수 있는 장소를 지정하는 복수의 트리플로써 프로비져닝되는 것인 방법.

[0390] 201. 실시예 1 내지 200 중 어느 하나에 있어서, 트리플은 PCID, D, 및 R을 포함하는 것인 방법.

[0391] 202. 실시예 1 내지 201 중 어느 하나에 있어서,

[0392] TRE의 현재 측위 위치를 결정하고;

[0393] 현재 측위 위치를 복수의 트리플과 비교하고;

[0394] 현재 측위 위치와 연관된 PCID를 해제하는 것을 더 포함하는 방법.

[0395] 203. 실시예 1 내지 202 중 어느 하나에 있어서, M2ME는 복수의 퀸트플로써 프로비져닝되는 것인 방법.

[0396] 204. 실시예 1 내지 203 중 어느 하나에 있어서, 퀸트플은 PCID, D, R, t1, 및 t2를 포함하며, t1은 시작 시간을 지정하고 t2는 유효 기간의 종료 시간을 지정하는 것인 방법.

[0397] 205. 실시예 1 내지 204 중 어느 하나에 있어서, 퀸트플은 M2ME에 대한 경로를 기술하는 것인 방법.

[0398] 206. 실시예 1 내지 205 중 어느 하나에 있어서, 미리 결정된 시간에 네트워크에 접속하는데 대한 M2ME의 실패는 경보를 트리거하는 것인 방법.

[0399] 207. 실시예 1 내지 206 중 어느 하나에 있어서, 퀸트플은 재프로비져닝될 수 있는 것인 방법.

[0400] 208. 실시예 1 내지 207 중 어느 하나에 있어서, 퀸트플은 PCID 업데이트 서비스(PUS)를 사용하여 재프로비져닝될 수 있는 것인 방법.

[0401] 209. 실시예 1 내지 208 중 어느 하나에 있어서, PUS는 TRE를 식별하도록 구성되는 것인 방법.

[0402] 210. 실시예 1 내지 209 중 어느 하나에 있어서, ICF는 PUS를 포함하는 것인 방법.

[0403] 211. 실시예 1 내지 210 중 어느 하나에 있어서, PUS는 별도의 네트워크 컴포넌트인 것인 방법.

[0404] 212. 실시예 1 내지 211 중 어느 하나에 있어서, 퀸트플 재프로비져닝은 하나 이상의 퀸트플에 대한 변경을 포함하는 것인 방법.

[0405] 213. 실시예 1 내지 212 중 어느 하나에 있어서, TRE의 아이덴티티는 TRE를 현재 네트워크 IP 어드레스와 연관시킬 수 있는 네트워크 서버에 보내지는 것인 방법.

[0406] 214. 실시예 1 내지 213 중 어느 하나에 있어서, 원격 프로비져닝은 DPF에 위임되는 것인 방법.

[0407] 215. 실시예 1 내지 214 중 어느 하나에 있어서,

[0408] PUS가 M2ME 및 TRE에 접속하고;

[0409] PUS가 TRE의 확인을 요청하고;

[0410] PUS가 새로운 복수의 퀸트플 및 폐기될 구 퀸트플의 리스트를 전달하고;

[0411] TRE가 새로운 퀸트플을 설치하고 구 퀸트플을 폐기하는 것을 더 포함하는 방법.

[0412] 216. 실시예 1 내지 215 중 어느 하나에 있어서, TRE는 PCID와 수반될 수 있는 의사랜덤 번호를 생성하도록 구성되는 것인 방법.

[0413] 217. 실시예 1 내지 216 중 어느 하나에 있어서, 액세스 네트워크는 의사랜덤 번호를 추적하고 이들을 구별하도록 구성되는 것인 방법.

[0414] 218. 실시예 1 내지 217 중 어느 하나에 있어서, 통신하는 엔티티들은 M2ME, TRE, 및 네트워크 액세스 포인트(NAP)인 것인 방법.

[0415] 219. 실시예 1 내지 218 중 어느 하나에 있어서, NAP는 VNO와 연관된 enodeB인 것인 방법.

[0416] 220. 실시예 1 내지 219 중 어느 하나에 있어서, TRE는 단일 최초 네트워크 접속에 사용될 랜덤 번호(RAND)를 생성하도록 구성되는 것인 방법.

[0417] 221. 실시예 1 내지 220 중 어느 하나에 있어서,

[0418] TRE가 무결성 보호 방법을 적용하는 것을 더 포함하는 방법.

[0419] 222. 실시예 1 내지 221 중 어느 하나에 있어서, 무결성 보호 방법은 RAND가 제2 파라미터, 필요에 따라 추가 데이터(D1), 및 PCID를 입력하는 키 해쉬 함수인 것인 방법.

[0420] 223. 실시예 1 내지 222 중 어느 하나에 있어서,

[0421] TRE가 eNB에 $\mathrm{TRE} \rightarrow \mathrm{eNB}\text{: } \mathrm{RAND} \,||\, \mathrm{PCID} \,||\, \mathrm{D1} \,||\, \mathrm{M1} := \mathrm{MAC}(\mathrm{PCID} \,||\, \mathrm{D1}, \mathrm{RAND})$를 보내고;

[0422] eNB가 메시지 인증 코드(MAC)를 검증하고;

[0423] eNB가 페이로드 데이터 D2, M1 중에 반환 패키지를 구축하고;

[0424] eNB가 $\mathrm{eNB} \rightarrow \mathrm{TRE}\text{: } \mathrm{D2} \,||\, \mathrm{M2} := \mathrm{MAC}(\mathrm{PCID} \,||\, \mathrm{D2}, \mathrm{M1}$로서 TRE에 반환 패키지를 보내는 것을 더 포함하는 방법.

[0425] 224. 실시예 1 내지 223 중 어느 하나에 있어서, 후속 메시지 교환은 임의의 새로운 메시지 요소를 포함하는 데이터 요소의 MAC 및 직전 교환의 MAC를 포함하는 것인 방법.

[0426] 225. 실시예 1 내지 224 중 어느 하나에 있어서, eNB와 TRE는 새로운 M_n을 구축하는데 마지막 값 M_{n-1}를 사용하여 통신 동안 메시지를 구별할 수 있는 것인 방법.

[0427] 226. 실시예 1 내지 225 중 어느 하나에 있어서, 중간자 공격이 피해지는 것인 방법.

[0428] 227. 실시예 1 내지 226 중 어느 하나에 있어서, 공유 시크릿은 통신하는 당사자들의 인증을 위해 메시지에 포함되는 것인 방법.

[0429] 228. 실시예 1 내지 227 중 어느 하나에 있어서, 공유 시크릿은 협상된 시크릿인 것인 방법.

[0430] 229. 실시예 1 내지 228 중 어느 하나에 있어서, MAC 값은 PCID를 포함하는 것인 방법.

[0431] 230. 실시예 1 내지 229 중 어느 하나에 있어서, eNB는 PCID를 사용하여 모든 동시 활성 네트워크 액세스 시도(채널)의 상태를 나타내는 표를 유지하는 것인 방법.

[0432] 231. 실시예 1 내지 230 중 어느 하나에 있어서, 표에서의 첫 번째 열은 채널에 속하는 PCID의 인덱스를 포함하는 것인 방법.

[0433] 232. 실시예 1 내지 231 중 어느 하나에 있어서, 인덱스는 모든 채널에 대하여 현재 활성인 모든 PCID의 리스트에서의 엔트리를 가리키는 것인 방법.

[0434] 233. 실시예 1 내지 232 중 어느 하나에 있어서, 인덱스는 PCID 값인 것인 방법.

[0435] 234. 실시예 1 내지 233 중 어느 하나에 있어서,

[0436] eNB가 $\mathrm{TRE} \rightarrow \mathrm{eNB}: \quad \mathrm{D3} \;||\; \mathrm{M3} := \mathrm{MAC}(\mathrm{PCID} \;||\; \mathrm{D3}, \mathrm{M2})$로서 채널을 통해 메시지를 수신하는 것을 더 포함하는 방법.

[0437] 235. 실시예 1 내지 234 중 어느 하나에 있어서,

[0438] eNB가 i-1 내지 N에 대하여 PL로부터 PCID_i를 선택하는 것을 더 포함하는 방법.

[0439] 236. 실시예 1 내지 235 중 어느 하나에 있어서,

[0440] 첫 번째 셀에서 PCID 인덱스 I를 갖는 모든 표의 행에 대하여, eNB가 $\mathrm{M} := \mathrm{MAC}(\mathrm{PCID}_i \;||\; \mathrm{D}_3, \mathrm{M}_2)$를 계산하는 것을 더 포함하며, M_2는 행에서 두 번째 셀로부터 취해지는 것인 방법.

[0441] 237. 실시예 1 내지 236 중 어느 하나에 있어서,

[0442] 성공 상태에 도달하고 검색 절차가 종료되는 것을 더 포함하는 방법.

[0443] 238. 실시예 1 내지 237 중 어느 하나에 있어서, 마지막 수신한 세 번째 메시지에 대응하는 채널의 행 번호가 반환되는 것인 방법.

[0444] 239. 실시예 1 내지 238 중 어느 하나에 있어서, D_3이 데이터 이력에 추가되고 M_2는 선택된 표 행의 활성 해시 값 셀에서 M_3으로 교체되는 것인 방법.

[0445] 240. 실시예 1 내지 239 중 어느 하나에 있어서, 메시지는 후속 메시지의 연관된 채널을 찾도록 채널의 인덱스 I를 포함하는 것인 방법.

[0446] 241. 실시예 1 내지 240 중 어느 하나에 있어서, 활성 PCID가 잠금되는 것인 방법.

[0447] 242. 실시예 1 내지 241 중 어느 하나에 있어서, PCID는 능동적으로 할당 해제되는 것인 방법.

[0448] 243. 실시예 1 내지 242 중 어느 하나에 있어서, TRE는 풀 네트워크 접속을 획득하는데 사용되었을 때 사용된 PCID를 폐기하는 것인 방법.

[0449] 244. 실시예 1 내지 243 중 어느 하나에 있어서, PCID는 유효 기간이 만료된 후에 폐기되는 것인 방법.

[0450] 245. 실시예 1 내지 244 중 어느 하나에 있어서, PCID는 요청에 응답하여 폐기되는 것인 방법.

[0451] 246. 실시예 1 내지 245 중 어느 하나에 있어서, 폐기된 PCID는 상이한 M2ME에 의해 사용되는 것인 방법.

[0452] 247. 실시예 1 내지 246 중 어느 하나에 있어서, 할당 해제 이벤트를 시그널링하도록 접속이 TRE로부터 E/S로 확립되는 것인 방법.

[0453] 248. 실시예 1 내지 247 중 어느 하나에 있어서, E/S는 할당 해제된 PCID의 리스트를 유지하는 것인 방법.

[0454] 249. 실시예 1 내지 248 중 어느 하나에 있어서, PCID는 할당 해제 프로세스 동안 클리어 텍스트로 전달되지 않는 것인 방법.

[0455] 250. 실시예 1 내지 249 중 어느 하나에 있어서, 확인은 자율적으로 수행되는 것인 방법.

[0456] 251. 실시예 1 내지 250 중 어느 하나에 있어서, 확인은 반자율적으로 수행되는 것인 방법.

[0457] 252. 실시예 1 내지 251 중 어느 하나에 있어서, 확인은 원격으로 수행되는 것인 방법.

[0458] 253. 실시예 1 내지 252 중 어느 하나에 있어서, 자율 확인은 M2ME가 자체적으로 네트워크 어태치를 겪을 수 있게 하기 전에 수행되는 것인 방법.

[0459] 254. 실시예 1 내지 253 중 어느 하나에 있어서, 반자율 확인은 외부 네트워크 엔티티에 의존하지 않고 M2ME의 유효성을 평가하는 것을 포함하는 것인 방법.

[0460] 255. 실시예 1 내지 254 중 어느 하나에 있어서, 반자율 확인의 결과는 원격 엔티티에 보고되는 것인 방법.

[0461] 256. 실시예 1 내지 255 중 어느 하나에 있어서, 결과는 TRE의 M2ME에의 인증의 바인딩의 증거를 포함하는 것인 방법.

[0462] 257. 실시예 1 내지 256 중 어느 하나에 있어서, 원격 엔티티는 PVA인 것인 방법.

[0463] 258. 실시예 1 내지 257 중 어느 하나에 있어서, M2ME와 원격 엔티티 간의 시그널링은 보호되는 것인 방법.

[0464] 259. 실시예 1 내지 258 중 어느 하나에 있어서, 원격 확인은 TRE에 의해 생성된 확인에 대한 증거 및 TRE와 M2ME 사이의 바인딩의 증거를 수신한 후에 M2ME의 무결성 및 유효성을 직접 평가하는 외부 네트워크 엔티티를 포함하는 것인 방법.

[0465] 260. 실시예 1 내지 259 중 어느 하나에 있어서, 외부 네트워크 엔티티는 PVA인 것인 방법.

[0466] 261. 실시예 1 내지 260 중 어느 하나에 있어서, M2ME와 외부 네트워크 엔티티 사이의 통신은 보호되는 것인 방법.

[0467] 262. 실시예 1 내지 261 중 어느 하나에 있어서, 자율 확인이 수행되고 확인의 어떠한 직접적인 증거도 외부 세계에 제공되지 않는 것인 방법.

[0468] 263. 실시예 1 내지 262 중 어느 하나에 있어서, M2ME가 확인을 실패하고 TRE는 그것이 네트워크에 어태치하거나 원격 엔티티에의 인증된 접속을 획득하는 것을 막는 것인 방법.

[0469] 264. 실시예 1 내지 263 중 어느 하나에 있어서,

[0470] TRE가 미리 정의된 상태의 보안 시작을 달성했는지 여부를 체크하는 것을 더 포함하는 방법.

[0471] 265. 실시예 1 내지 264 중 어느 하나에 있어서,

[0472] 보안 시작을 필요로 하는 나머지 M2ME의 미리 정의된 부분이 미리 정의된 상태의 보안 시작을 달성했는지 여부를 체크하는 것을 더 포함하는 방법.

[0473] 267. 실시예 1 내지 266 중 어느 하나에 있어서, 부가적인 체크가 TRE에 의해 수행되는 것인 방법.

[0474] 268. 실시예 1 내지 267 중 어느 하나에 있어서, TRE 외부에 있지만 TRE에 의해 무결성이 보호되는 M2ME 내의 측정 컴포넌트에 의해 부가적인 체크가 수행되는 것인 방법.

[0475] 269. 실시예 1 내지 268 중 어느 하나에 있어서, TRE는 M2ME가 요청된 인증 절차에 참여할 수 있게 하는 것인 방법.

[0476] 270. 실시예 1 내지 269 중 어느 하나에 있어서, 자율 확인은 요구되는 외부 통신에 대하여 가장 경제적인 방법인 것인 방법.

[0477] 271. 실시예 1 내지 270 중 어느 하나에 있어서, 자율 확인은 어떠한 외부 엔티티라도 네트워크 액세스 동안 또는 중단되지 않는 접속 단계 동안 TRE의 무결정을 독립적으로 평가할 수 있게 하지 않는 것인 방법.

[0478] 272. 실시예 1 내지 271 중 어느 하나에 있어서, TRE는 확인 프로세스의 로그 및 그의 결과를 저장하는 것인 방법.

[0479] 273. 실시예 1 내지 272 중 어느 하나에 있어서, 로그는 오디트 기록을 구성하는 것인 방법.

[0480] 274. 실시예 1 내지 273 중 어느 하나에 있어서, 오디트 데이터는 보안 내부 아카이브에 저장되는 것인 방법.

[0481] 275. 실시예 1 내지 274 중 어느 하나에 있어서, 보안 내부 아카이브는 TRE 내에 있는 것인 방법.

[0482] 276. 실시예 1 내지 275 중 어느 하나에 있어서, 보안 내부 아카이브는 TRE에 의해 보호되는 것인 방법.

[0483] 277. 실시예 1 내지 276 중 어느 하나에 있어서, 보안 내부 아카이브의 조작이 검출되는 것인 방법.

[0484] 278. 실시예 1 내지 277 중 어느 하나에 있어서, 데이터의 무결성 보호가 제공되는 것인 방법.

[0485] 279. 실시예 1 내지 278 중 어느 하나에 있어서, 오디트 데이터는 자율 확인이 호출되는 특정 목적에 묶이는 것인 방법.

[0486] 280. 실시예 1 내지 279 중 어느 하나에 있어서, 데이터는 확인의 목적을 포함하는 것인 방법.

[0487] 281. 실시예 1 내지 280 중 어느 하나에 있어서, 액세스 프로토콜에서 확립된 공유 시크릿 또는 크리덴셜은 오디트 데이터에 첨부되고, 디지털 서명은 그의 무결성을 보호하도록 생성된 데이터에 TRE에 의해 적용되는 것인 방법.

[0488] 282. 실시예 1 내지 281 중 어느 하나에 있어서, M2ME와는 독립적인 엔티티는 M2ME가 모든 이른 네트워크 액세스에서 신뢰할 수 있는지 여부를 주기적으로 확립하도록 오디트 데이터를 요청하는 것인 방법.

[0489] 283. 실시예 1 내지 282 중 어느 하나에 있어서, 데이터는 조작을 검출하려는 네트워크 액세스 시도에 대한 네트워크측 프로토콜로써 대항되는 것인 방법.

[0490] 284. 실시예 1 내지 283 중 어느 하나에 있어서, 나머지 M2ME의 기타 컴포넌트, 구성, 또는 파라미터의 무결성은 그것들이 로딩되거나 시작될 때 또는 측정 컴포넌트가 이용할 수 있는 임의의 기타 미리 정의된 실행 시간 이벤트에서 체크되는 것인 방법.

[0491] 285. 실시예 1 내지 284 중 어느 하나에 있어서, 원격 엔티티는 M2ME가 반자율 확인 테스트를 통과했음을 간접적으로 알게 되는 것인 방법.

[0492] 286. 실시예 1 내지 285 중 어느 하나에 있어서, 반자율 확인의 결과의 네트워크에의 명시적인 시그널링이 존재하는 것인 방법.

[0493] 287. 실시예 1 내지 286 중 어느 하나에 있어서, 시그널링은 암호로 보호되는 것인 방법.

[0494] 288. 실시예 1 내지 287 중 어느 하나에 있어서, 시그널링은 MID 다운로드에 요구되는 M2ME 인증에 앞서는 것인 방법.

[0495] 289. 실시예 1 내지 288 중 어느 하나에 있어서, 시그널링은 유효성 체크에 사용된 M2ME에서의 리소스 및 TRE의 인증 간의 바인딩의 증거를 포함하는 것인 방법.

[0496] 290. 실시예 1 내지 289 중 어느 하나에 있어서, 증거는 TRE 및 M2ME의 증명을 확립하기 위한 부가적인 정보를 제공하는, M2ME로부터 네트워크에 보내진 토큰을 포함하는 것인 방법.

[0497] 291. 실시예 1 내지 290 중 어느 하나에 있어서, PVA 또는 SHO는 주기적으로 확인을 수행하도록 TRE에 요청하는 것인 방법.

[0498] 292. 실시예 1 내지 291 중 어느 하나에 있어서, 보안 게이트웨이(SeGW)는 확인을 요청하는 것인 방법.

[0499] 293. 실시예 1 내지 292 중 어느 하나에 있어서, 요청은 M2ME가 등록된 후에 보내지는 것인 방법.

[0500] 294. 실시예 1 내지 293 중 어느 하나에 있어서, 요청은 SeGW에 의해 맨 처음에 홈 eNodeB(H(e)NB)가 인증되면 보내지는 것인 방법.

[0501] 295. 실시예 1 내지 294 중 어느 하나에 있어서, 요청은 PVA, SHO, SeGW 중 하나 이상으로부터의 보호된 OAM 메시지로서 주기적으로 보내지는 것인 방법.

[0502] 296. 실시예 1 내지 295 중 어느 하나에 있어서, 주기적 재확인의 주기는 비교적 길지만 확인의 신선도에 대해 SHO가 안전하게 느낄 정도로 충분히 짧은 것인 방법.

[0503] 297. 실시예 1 내지 296 중 어느 하나에 있어서, TRE는 요청에 기초하여 확인 절차를 수행하는 것인 방법.

[0504] 298. 실시예 1 내지 297 중 어느 하나에 있어서, TRE는 마지막 성공적인 확인을 나타내는 타임스탬프를 생성하는 것인 방법.

[0505] 299. 실시예 1 내지 298 중 어느 하나에 있어서, TRE는 마지막 확인이 주기적 확인의 현재 라운드의 만료 전에

발생하였음을 나타내는 메시지를 보내는 것인 방법.

[0506] 300. 실시예 1 내지 299 중 어느 하나에 있어서, 확인의 결과에 대한 어떠한 명시적인 시그널링도 없는 것인 방법.

[0507] 301. 실시예 1 내지 300 중 어느 하나에 있어서, M2ME는 미리 정의된 보안 상태로 시작하는 것인 방법.

[0508] 302. 실시예 1 내지 301 중 어느 하나에 있어서, M2ME는 TRE가 플랫폼 유효성의 증거를 생성하도록 요청하는 것인 방법.

[0509] 303. 실시예 1 내지 302 중 어느 하나에 있어서, TRE는 나머지 M2ME로부터 플랫폼 유효성의 증거를 생성하는데 사용될 재료를 수집하는 것인 방법.

[0510] 304. 실시예 1 내지 303 중 어느 하나에 있어서, 증거는 보안 결정적인 실행 코드, M2ME의 운영 체제에 대한 크리덴셜, 및 장비 id를 포함하는 것인 방법.

[0511] 305. 실시예 1 내지 304 중 어느 하나에 있어서, TRE는 M2ME의 확인을 위한 증거를 생성하고 무결성 및 비밀을 위해 그것을 암호로 보호하는 것인 방법.

[0512] 306. 실시예 1 내지 305 중 어느 하나에 있어서, M2ME는 PVA에 보호된 증거를 전송하는 것인 방법.

[0513] 307. 실시예 1 내지 306 중 어느 하나에 있어서, PVA는 보호된 증거를 수신하고, M2ME가 계속해서 인증을 수행하고 MID를 다운로딩하기에 충분히 신뢰할 수 있는지 여부를 결정하도록 증거를 평가하는 것인 방법.

[0514] 308. 실시예 1 내지 307 중 어느 하나에 있어서, M2ME 확인과 인증 사이의 바인딩이 수행되는 것인 방법.

[0515] 309. 실시예 1 내지 308 중 어느 하나에 있어서, 바인딩은 M2ME의 보안 상태를 입증하는 M2ME의 크리덴셜 또는 증명서를 포함하는 것인 방법.

[0516] 310. 실시예 1 내지 309 중 어느 하나에 있어서, 바인딩은 증명의 보다 안전한 수단을 포함하는 것인 방법.

[0517] 311. 실시예 1 내지 310 중 어느 하나에 있어서, M2ME는 최초 네트워크 접속을 위한 전제조건으로서 ICF에 의해 인증되는 것인 방법.

[0518] 312. 실시예 1 내지 311 중 어느 하나에 있어서, M2ME는 MID를 다운로드하기 전에 인증된 TRE를 포함하는 것을 증명하도록 DPF에 의해 인증되는 것인 방법.

[0519] 313. 실시예 1 내지 312 중 어느 하나에 있어서, M2ME는 동작적 네트워크 액세스 전에 SHO에 의해 인증되는 것인 방법.

[0520] 314. 실시예 1 내지 313 중 어느 하나에 있어서, 네트워크 액세스 인증에 대한 유효성의 바인딩은 자율 확인에 대하여 암시적인 것인 방법.

[0521] 315. 실시예 1 내지 314 중 어느 하나에 있어서, TRE의 아이덴티티에 대해 부가적인 정보를 제공하는 토큰이 최초 첨부 메시지에서 전달되는 것인 방법.

[0522] 316. 실시예 1 내지 315 중 어느 하나에 있어서, M2ME에의 인증 크리덴셜을 보유하는 TRE의 논리적 바인딩이 존재하는 것인 방법.

[0523] 317. 실시예 1 내지 316 중 어느 하나에 있어서, 디바이스 플랫폼의 무결성이 인증 동안 확인되는 것인 방법.

[0524] 318. 실시예 1 내지 317 중 어느 하나에 있어서, TRE의 M2ME에의 물리적 바인딩이 존재하는 것인 방법.

[0525] 319. 실시예 1 내지 318 중 어느 하나에 있어서, 디바이스 플랫폼의 무결성이 TRE 인증 동안 확인되는 것인 방법.

[0526] 320. 실시예 1 내지 319 중 어느 하나에 있어서, 플랫폼 리소스의 실제 확인은 M2ME로 안전하게 내장된 하드웨어 보안 컴포넌트의 기능성을 사용함으로써 수행되는 것인 방법.

[0527] 321. 실시예 1 내지 320 중 어느 하나에 있어서, 플랫폼 리소스의 실제 확인은 TRE 외부에 있지만 그의 보안 특성이 TRE에 의해 보장되고 TRE에의 보안 접속을 갖는 하드웨어 보안 컴포넌트를 사용함으로써 수행되는 것인 방법.

[0528] 322. 실시예 1 내지 321 중 어느 하나에 있어서, 확인 및 인증은 공통 프로토콜의 세션에서 조합되는 것인

방법.

[0529] 323. 실시예 1 내지 322 중 어느 하나에 있어서, IKEv2는 조합된 확인 및 인증 절차에서 사용되는 것인 방법.

[0530] 324. 실시예 1 내지 323 중 어느 하나에 있어서, ICF, DRF, 및 DPF는 개별 엔티티들인 것인 방법.

[0531] 325. 실시예 1 내지 324 중 어느 하나에 있어서, ICF, DRF, 및 DPF는 조합되는 것인 방법.

[0532] 326. 실시예 1 내지 325 중 어느 하나에 있어서, MID의 M2ME에의 다운로딩 및 프로비져닝은 M2ME가 최초 네트워크 액세스를 위해 3G VNO의 네트워크에 액세스할 때 발생하는 것인 방법.

[0533] 327. 실시예 1 내지 326 중 어느 하나에 있어서, VNO는 M2ME에 무선 인터페이스를 제공하는 것인 방법.

[0534] 328. 실시예 1 내지 327 중 어느 하나에 있어서, M2ME는 네트워크 정보를 디코딩하고 어태치 메시지를 사용하여 VNO의 네트워크에 어태치하는데 표준 GSM/UMTS 원리를 사용하는 것인 방법.

[0535] 329. 실시예 1 내지 328 중 어느 하나에 있어서, 어태치 메시지는 임시 M2ME ID(PCID)를 포함하는 것인 방법.

[0536] 330. 실시예 1 내지 329 중 어느 하나에 있어서, M2ME는 VNO에 의해 표준 UMTS AKA 절차를 사용하여 인증되는 것인 방법.

[0537] 331. 실시예 1 내지 330 중 어느 하나에 있어서, VNO는 그의 컨텐츠 및 구조에 기초하여 IMSI로서 PCID를 인식하는 것인 방법.

[0538] 332. 실시예 1 내지 331 중 어느 하나에 있어서, M2ME 및 VNO는 공통 인증 알고리즘을 지원하는 것인 방법.

[0539] 333. 실시예 1 내지 332 중 어느 하나에 있어서, 공통 인증 알고리즘은 Milenage인 것인 방법.

[0540] 334. 실시예 1 내지 333 중 어느 하나에 있어서, M2ME에 대한 ID로서 PCID를 인식하는 VNO는 적법한 예비 크리덴셜로서 PCID를 수락할 ICF에 접촉하는 것인 방법.

[0541] 335. 실시예 1 내지 334 중 어느 하나에 있어서, ICF는 M2ME와의 부가적인 통신을 보호하도록 예비 AV 세트를 발행하고, M2ME에 보호된 IP 접속을 제공하기를 시작하는 것인 방법.

[0542] 336. 실시예 1 내지 335 중 어느 하나에 있어서, M2ME 및 ICF는 M2ME와의 통신을 보호할 예비 AKA 키를 생성하도록 표준 AKA 프로세스를 수행하는 것인 방법.

[0543] 337. 실시예 1 내지 336 중 어느 하나에 있어서, ICF는 M2ME를 DPF에 재지향시키는 것인 방법.

[0544] 338. 실시예 1 내지 337 중 어느 하나에 있어서, ICF는 DRF에 PCID를 보내는 것인 방법.

[0545] 339. 실시예 1 내지 338 중 어느 하나에 있어서, DRF는 M2ME가 SHO를 찾는 것을 돕는 것인 방법.

[0546] 340. 실시예 1 내지 339 중 어느 하나에 있어서, DRF는 SHO에 접속하고 SHO의 네트워크에의 접속을 위해 M2ME를 등록하는 것인 방법.

[0547] 341. 실시예 1 내지 340 중 어느 하나에 있어서, SHO는 TRE의 진위 및 무결성을 확인하도록 PVA에 요청하는 것인 방법.

[0548] 342. 실시예 1 내지 341 중 어느 하나에 있어서, PVA는 TRE의 진위 및 무결성을 확인하는 것인 방법.

[0549] 343. 실시예 1 내지 342 중 어느 하나에 있어서, PVA는 SHO에 확인 결과를 보내는 것인 방법.

[0550] 344. 실시예 1 내지 343 중 어느 하나에 있어서, SHO는 DPF에 접촉하고 MID의 M2ME에의 프로비져닝을 권한 부여하는 것인 방법.

[0551] 345. 실시예 1 내지 344 중 어느 하나에 있어서, DPF는 M2ME로 MID를 다운로딩하는 것인 방법.

[0552] 346. 실시예 1 내지 345 중 어느 하나에 있어서, M2ME는 다운로딩된 MID를 TRE로 프로비져닝하고 DPF에 프로비져닝의 상태를 보고하는 것인 방법.

[0553] 347. 실시예 1 내지 346 중 어느 하나에 있어서, M2ME는 상태 메시지의 확인을 위한 토큰을 보내는 것인 방법.

[0554] 348. 실시예 1 내지 347 중 어느 하나에 있어서, 토큰은 조작 및 리플레이 공격에 내성이 있는 것인 방법.

[0555] 349. 실시예 1 내지 348 중 어느 하나에 있어서, DPF는 SHO에의 프로비져닝의 상태를 보고하는 것인 방법.

[0556] 350. 실시예 1 내지 349 중 어느 하나에 있어서, M2ME로의 MID의 다운로딩 및 프로비져닝은 M2ME가 최초 네트워크 액세스를 위해 3G VNO의 네트워크에 액세스할 때 발생하는 것인 방법.

[0557] 351. 실시예 1 내지 350 중 어느 하나에 있어서, ICF는 M2ME에 임시 인증 벡터를 해제하기 전에 그리고 M2ME에의 IP 접속을 허용하기 전에 TRE를 확인하도록 PVA에 요청하는 것인 방법.

[0558] 352. 실시예 1 내지 351 중 어느 하나에 있어서, M2ME 소유자는 M2ME 파라미터를 전달하도록 새로운 SHO에 접촉하는 것인 방법.

[0559] 353. 실시예 1 내지 352 중 어느 하나에 있어서, M2ME 소유자는 재프로비져닝을 개시하도록 M2ME에 접촉하는 것인 방법.

[0560] 354. 실시예 1 내지 353 중 어느 하나에 있어서, 새로운 SHO는 M2ME를 확인하도록 확인 엔티티에 요청하는 것인 방법.

[0561] 355. 실시예 1 내지 354 중 어느 하나에 있어서, 확인 엔티티는 M2ME를 확인하고 새로운 SHO에 결과를 보내는 것인 방법.

[0562] 356. 실시예 1 내지 355 중 어느 하나에 있어서, 새로운 SHO는 M2ME에 새로운 MID를 다운로딩하고 프로비져닝하도록 DPF에 요청하는 것인 방법.

[0563] 357. 실시예 1 내지 356 중 어느 하나에 있어서, DPF는 M2ME로 새로운 MID 패키지를 안전하게 다운로딩하는 것인 방법.

[0564] 358. 실시예 1 내지 357 중 어느 하나에 있어서, M2ME는 구 SHO에 구 MID가 폐기되어야 한다는 메시지를 보내는 것인 방법.

[0565] 359. 실시예 1 내지 358 중 어느 하나에 있어서, 구 SHO는 M2ME에 ACK를 보내는 것인 방법.

[0566] 360. 실시예 1 내지 359 중 어느 하나에 있어서, M2ME는 DPF 및 새로운 SHO에 ACK를 전송하는 것인 방법.

[0567] 361. 실시예 1 내지 360 중 어느 하나에 있어서, M2ME는 자신의 시스템을 업데이트하고 DPF의 도움으로 MID를 설치하는 것인 방법.

[0568] 362. 실시예 1 내지 361 중 어느 하나에 있어서, M2ME는 DPF에 상태를 보내는 것인 방법.

[0569] 363. 실시예 1 내지 362 중 어느 하나에 있어서, DPF는 새로운 SHO에 상태를 보고하는 것인 방법.

[0570] 364. 실시예 1 내지 363 중 어느 하나에 있어서, M2ME는 휴면 상태에 놓이고 최초 프로비져닝 절차를 실행하는 것인 방법.

[0571] 365. 실시예 1 내지 364 중 어느 하나에 있어서, PVA는 M2ME가 여전히 동일한 SHO에 가입되어 있는 동안에 수행된 임의의 소프트웨어 또는 펌웨어(SW/FW) 업데이트가 보안 방식으로 행해짐을 보장하는 일을 담당하는 것인 방법.

[0572] 366. 실시예 1 내지 365 중 어느 하나에 있어서, PVA 또는 DPF는 SW/FW의 보안 온에어 또는 온와이어 다운로딩 및 M2ME 또는 TRE의 재프로비져닝과 같은 절차를 감독하는 것인 방법.

[0573] 367. 실시예 1 내지 366 중 어느 하나에 있어서, PVA 또는 DPF는 OMA DM 및 OMA FOTA 절차를 채용하는 것인 방법.

[0574] 368. 실시예 1 내지 367 중 어느 하나에 있어서, M2ME의 신뢰 상태 정보는 원격 SW/FW 업데이트 또는 재구성으로 인해 변경되는 것인 방법.

[0575] 369. 실시예 1 내지 368 중 어느 하나에 있어서, PVA 또는 DPF는 M2ME 또는 TRE의 새로 검증가능한 부트 또는 실행시간 신뢰 상태 정보 체크를 개시하고 그의 결과를 획득하도록 구성되는 것인 방법.

[0576] 370. 실시예 1 내지 369 중 어느 하나에 있어서, M2ME는 조작을 검출하도록 구성되는 것인 방법.

[0577] 371. 실시예 1 내지 370 중 어느 하나에 있어서, 조작을 검출하는 것은 임의의 서브시스템에 대한 조작을 포함하는 것인 방법.

[0578] 372. 실시예 1 내지 371 중 어느 하나에 있어서, 조작 검출은 빈번하게 수행되는 것인 방법.

[0579] 373. 실시예 1 내지 372 중 어느 하나에 있어서, 조작 이벤트는, 멀웨어 또는 바이러스에 의한 OS의 치료가능 및/또는 치료불가능한 중간물, 무선 또는 상위 계층 접속 특성 및/또는 환경 판독에서의 갑작스런 예상치못하거나 인가되지 않은 변경, 예비 인증, 등록, 또는 MID 프로비져닝에 대한 M2ME의 요청에 대한 신뢰 네트워크 요소에 의한 액세스 또는 서비스의 거부 및/또는 과도하게 반복된 실패, 또는 원격 MID 관리 기능성에 관한 M2ME 또는 M2ME 서브시스템의 신뢰 상태의 부트후 또는 실행시 판독에 있어서의 임의의 예상치못한/인가되지 않은 변경 중 하나 이상을 포함하는 것인 방법.

[0580] 374. 실시예 1 내지 373 중 어느 하나에 있어서, 다른 네트워크 요소는 조작을 검출하도록 구성되는 것인 방법.

[0581] 375. 실시예 1 내지 374 중 어느 하나에 있어서, M2ME는 조작 검출에 응답하여 손상을 제한하도록 조취를 취하는 것인 방법.

[0582] 376. 실시예 1 내지 375 중 어느 하나에 있어서, M2ME는 원격 MID 관리를 디스에이블하도록 구성되는 것인 방법.

[0583] 378. 실시예 1 내지 377 중 어느 하나에 있어서, M2ME는 지정된 네트워크 요소에 조작 이벤트를 보고하도록 구성되는 것인 방법.

[0584] 379. 실시예 1 내지 378 중 어느 하나에 있어서, M2ME는 최근 소프트웨어 업데이트 또는 의심되는 바이러스나 멀웨어 코드 또는 데이터를 삭제하거나 격리하거나 언인스톨하는 것과 같은 치료 동작을 수행하도록 구성되는 것인 방법.

[0585] 380. 실시예 1 내지 379 중 어느 하나에 있어서, M2ME는 원격 MID 관리 기능에 관련된 임의의 미리 지정된 데이터 세트를 삭제하도록 구성되는 것인 방법.

[0586] 381. 실시예 1 내지 380 중 어느 하나에 있어서, M2ME는 M2ME 또는 M2ME의 일부나 서브시스템을 파워다운하도록 구성되는 것인 방법.

[0587] 382. 실시예 1 내지 381 중 어느 하나에 있어서, 네트워크 요소는 조작후 치료 측정을 수행하도록 구성되는 것인 방법.

[0588] 383. 실시예 1 내지 382 중 어느 하나의 방법의 적어도 일부를 수행하도록 구성된 무선 송수신 유닛(WTRU).

[0589] 384. 실시예 1 내지 382 중 어느 하나의 방법의 적어도 일부를 수행하도록 구성되는 M2M 장비.

[0590] 385. 실시예 1 내지 382 중 어느 하나의 방법의 적어도 일부를 수행하도록 구성되는 네트워크 엔티티.

부호의 설명

[0591] 110: M2ME(machine-to-machine equipment)

115: VNO(visited network operator)

130: RO(registration operator)

140: SHO(selected home operator)

150: PVA(platform verification authority)

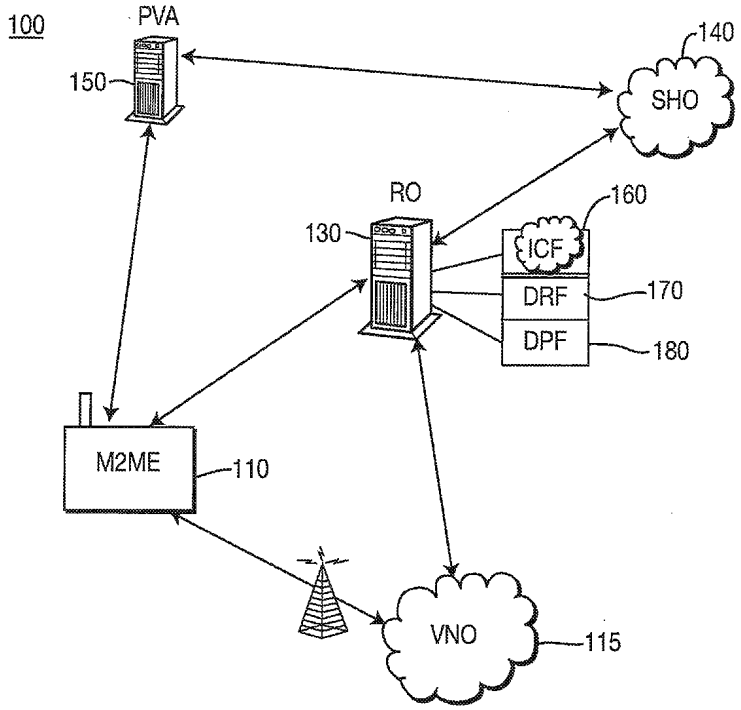
160: ICF

170: DRF(discover and registration function)

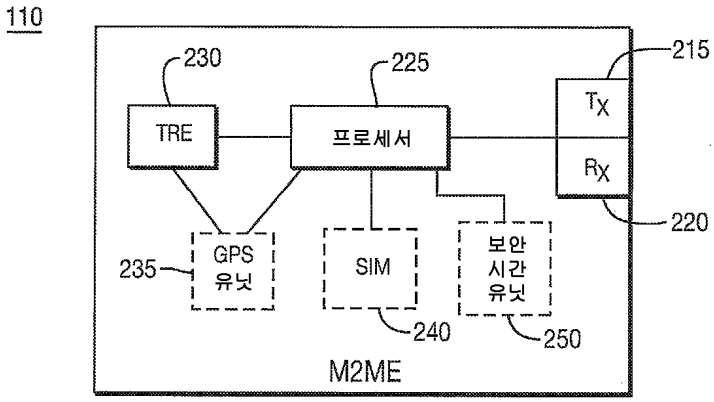
180: DPF(downloading and provisioning function)

도면

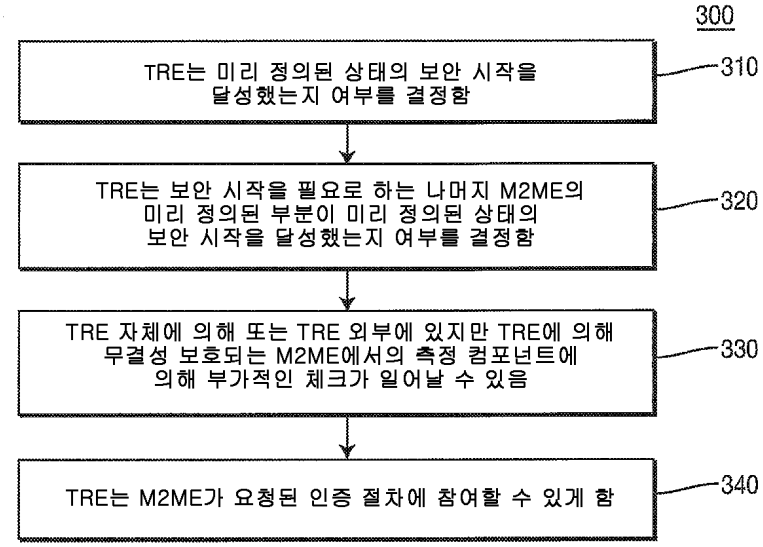
도면1


100
PVA
150
140
SHO
RO
130
160
ICF
DRF
170
DPF
180
M2ME
110
VNO
115

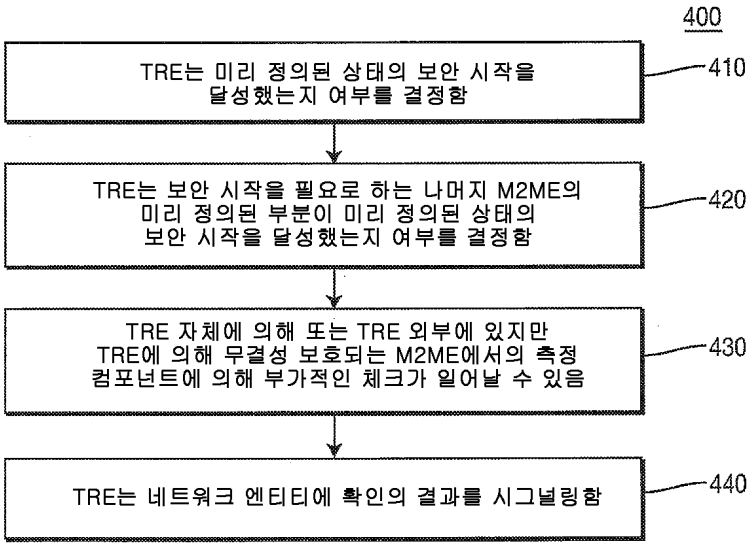
도면2


110
230
225
215
TRE
프로세서
Tx
Rx
220
235
GPS 유닛
SIM
보안 시간 유닛
240
250
M2ME

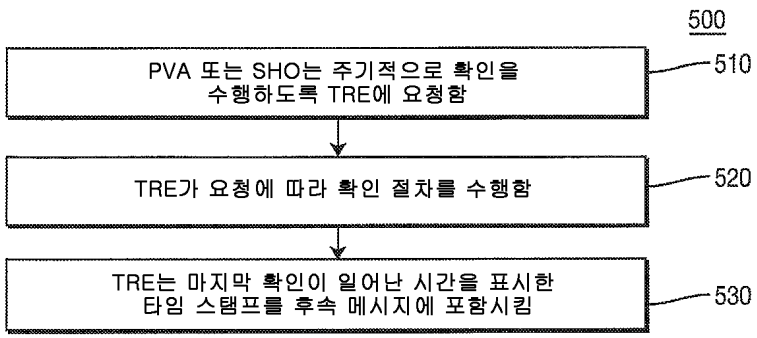
도면3


300
TRE는 미리 정의된 상태의 보안 시작을 달성했는지 여부를 결정함
310
TRE는 보안 시작을 필요로 하는 나머지 M2ME의 미리 정의된 부분이 미리 정의된 상태의 보안 시작을 달성했는지 여부를 결정함
320
TRE 자체에 의해 또는 TRE 외부에 있지만 TRE에 의해 무결성 보호되는 M2ME에서의 측정 컴포넌트에 의해 부가적인 체크가 일어날 수 있음
330
TRE는 M2ME가 요청된 인증 절차에 참여할 수 있게 함
340

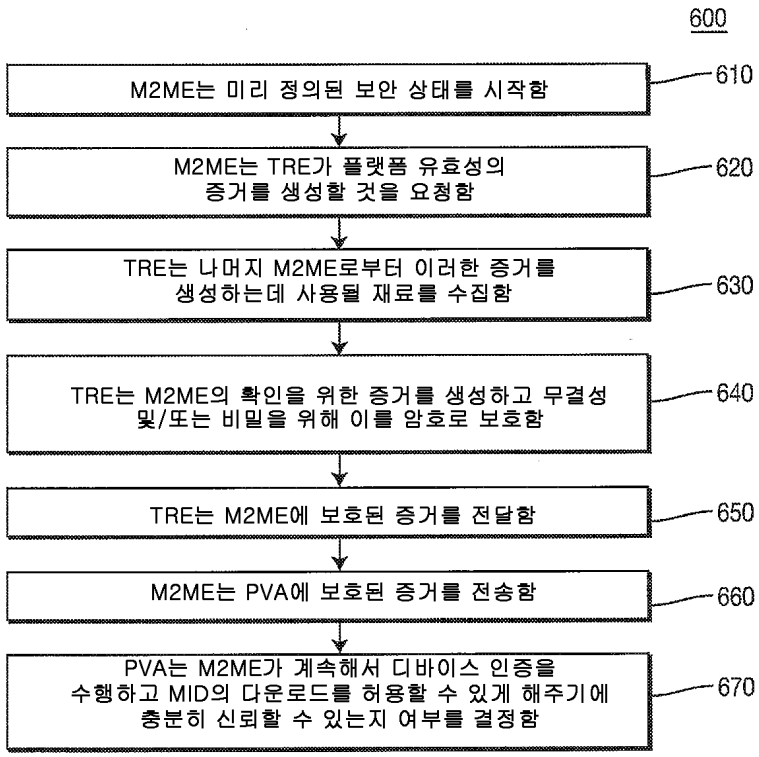
도면4


400
TRE는 미리 정의된 상태의 보안 시작을 달성했는지 여부를 결정함
410
TRE는 보안 시작을 필요로 하는 나머지 M2ME의 미리 정의된 부분이 미리 정의된 상태의 보안 시작을 달성했는지 여부를 결정함
420
TRE 자체에 의해 또는 TRE 외부에 있지만 TRE에 의해 무결성 보호되는 M2ME에서의 측정 컴포넌트에 의해 부가적인 체크가 일어날 수 있음
430
TRE는 네트워크 엔티티에 확인의 결과를 시그널링함
440

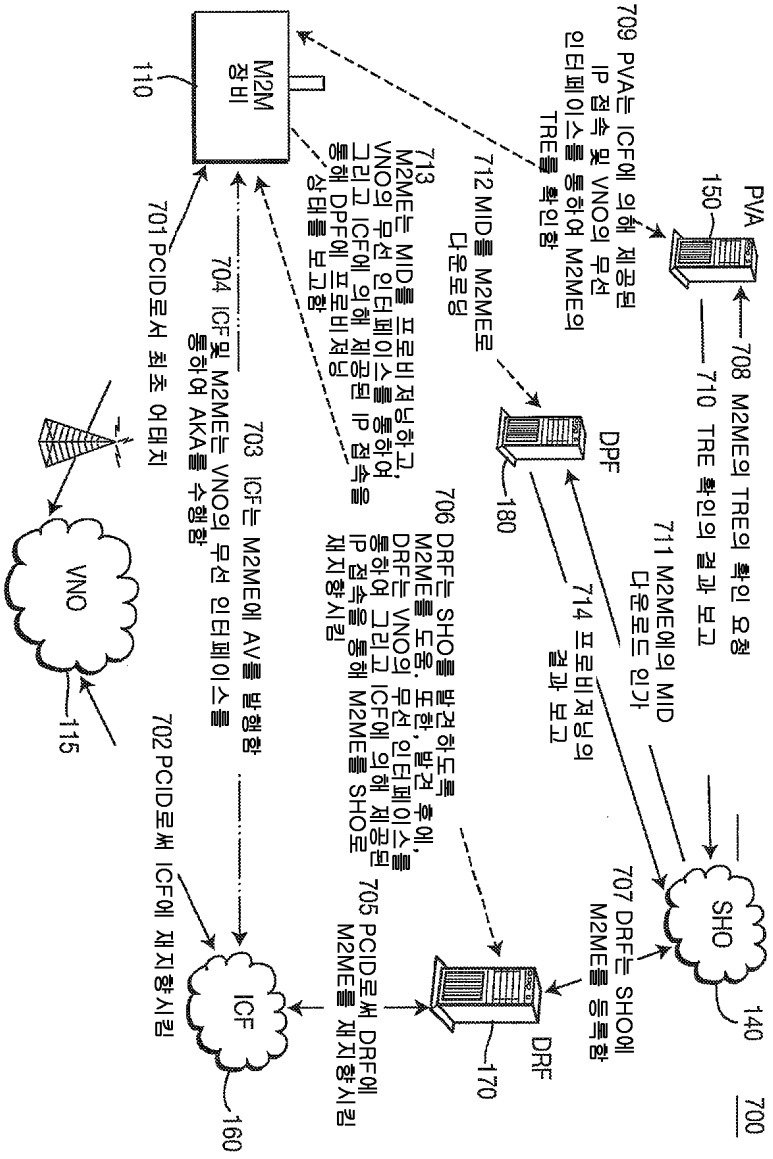
도면5


500
PVA 또는 SHO는 주기적으로 확인을 수행하도록 TRE에 요청함
510
TRE가 요청에 따라 확인 절차를 수행함
520
TRE는 마지막 확인이 일어난 시간을 표시한 타임 스탬프를 후속 메시지에 포함시킴
530

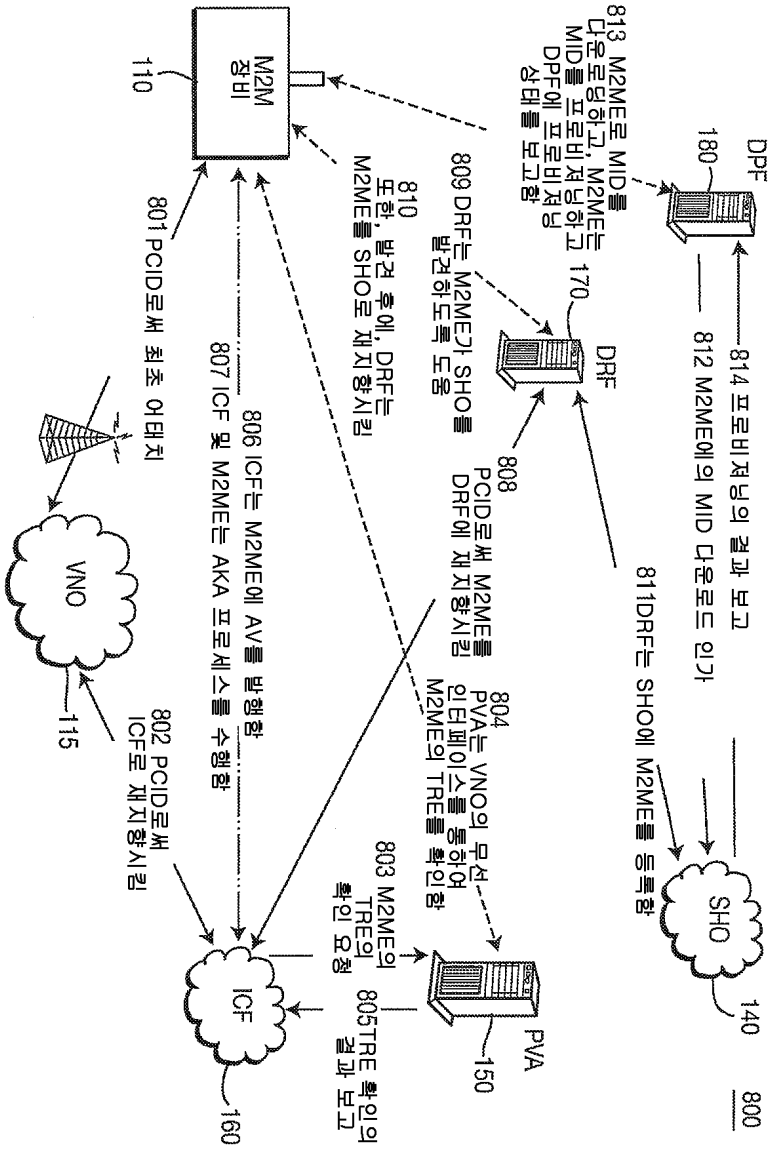
도면6


600
M2ME는 미리 정의된 보안 상태를 시작함
610
M2ME는 TRE가 플랫폼 유효성의 증거를 생성할 것을 요청함
620
TRE는 나머지 M2ME로부터 이러한 증거를 생성하는데 사용될 재료를 수집함
630
TRE는 M2ME의 확인을 위한 증거를 생성하고 무결성 및/또는 비밀을 위해 이를 암호로 보호함
640
TRE는 M2ME에 보호된 증거를 전달함
650
M2ME는 PVA에 보호된 증거를 전송함
660
PVA는 M2ME가 계속해서 디바이스 인증을 수행하고 MID의 다운로드를 허용할 수 있게 해주기에 충분히 신뢰할 수 있는지 여부를 결정함
670

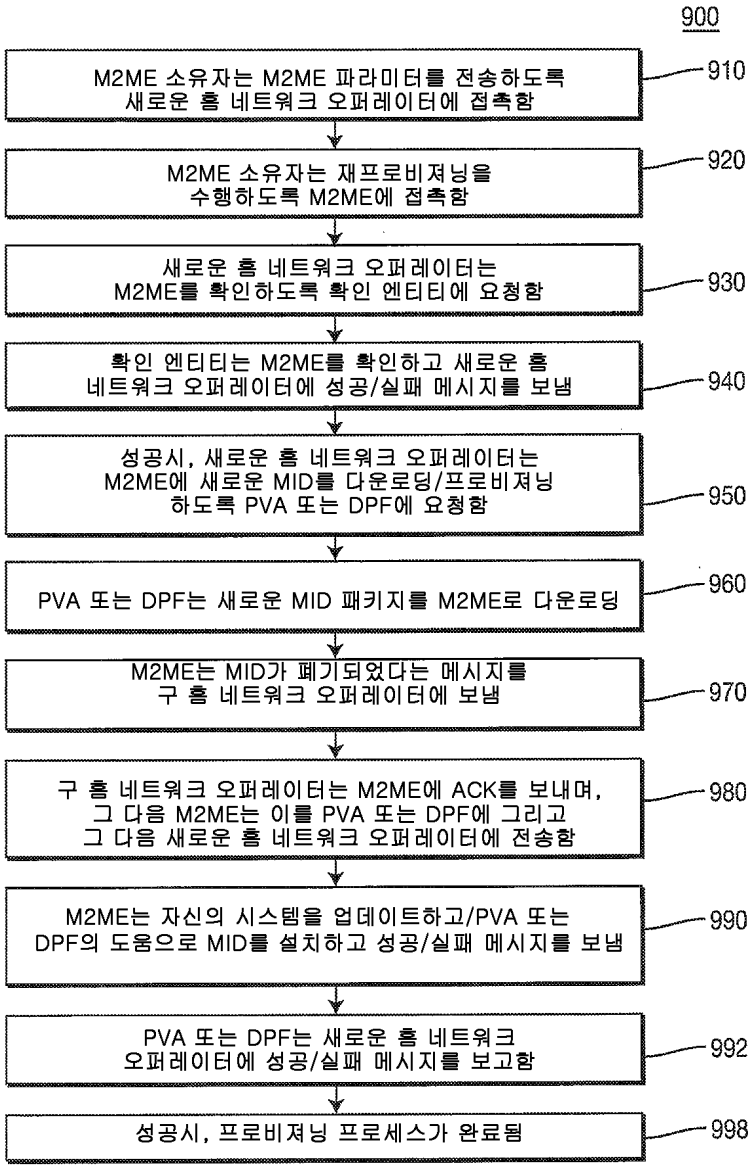
도면7


700
PVA
150
SHO
140
DPF
180
DRF
170
ICF
160
VNO
115
M2M 장비
110
708 M2ME의 TRE의 확인 요청
710 TRE 확인의 결과 보고
709 PVA는 ICF에 의해 제공된 IP 접속 및 VNO의 무선 인터페이스를 통하여 M2ME의 TRE를 확인함
711 M2ME에의 MID 다운로드 인가
712 MID를 M2ME로 다운로딩
714 프로비저닝의 결과 보고
707 DRF는 SHO에 M2ME를 등록함
705 PCID로써 DRF에 M2ME를 재지향시킴
706 DRF는 SHO를 발견하도록 M2ME를 도움. 또한, 발견 후에, DRF는 VNO의 무선 인터페이스를 통하여 그리고 ICF에 의해 제공된 IP 접속을 통해 M2ME를 SHO로 재지향시킴
713 M2ME는 MID를 프로비저닝하고, VNO의 무선 인터페이스를 통하여 그리고 ICF에 의해 제공된 IP 접속을 통해 DPF에 프로비저닝 상태를 보고함
701 PCID로서 최초 어태치
704 ICF 및 M2ME는 VNO의 무선 인터페이스를 통하여 AKA를 수행함
703 ICF는 M2ME에 AV를 발행함
702 PCID로써 ICF에 재지향시킴

도면8


800
DPF
180
814 프로비저닝의 결과 보고
812 M2ME에의 MID 다운로드 인가
811DRF는 SHO에 M2ME를 등록함
SHO
140
813 M2ME로 MID를 다운로딩하고, M2ME는 MID를 프로비저닝하고 DPF에 프로비저닝 상태를 보고함
170
DRF
809 DRF는 M2ME가 SHO를 발견하도록 도움
808 PCID로써 M2ME를 DRF에 재지향시킴
804 PVA는 VNO의 무선 인터페이스를 통하여 M2ME의 TRE를 확인함
803 M2ME의 TRE의 확인 요청
805TRE 확인의 결과 보고
PVA
150
M2M 장비
110
801 PCID로써 최초 어태치
810 또한, 발견 후에, DRF는 M2ME를 SHO로 재지향시킴
807 ICF 및 M2ME는 AKA 프로세스를 수행함
806 ICF는 M2ME에 AV를 발행함
VNO
115
802 PCID로써 ICF로 재지향시킴
ICF
160

도면9


900
M2ME 소유자는 M2ME 파라미터를 전송하도록 새로운 홈 네트워크 오퍼레이터에 접촉함
910
M2ME 소유자는 재프로비져닝을 수행하도록 M2ME에 접촉함
920
새로운 홈 네트워크 오퍼레이터는 M2ME를 확인하도록 확인 엔티티에 요청함
930
확인 엔티티는 M2ME를 확인하고 새로운 홈 네트워크 오퍼레이터에 성공/실패 메시지를 보냄
940
성공시, 새로운 홈 네트워크 오퍼레이터는 M2ME에 새로운 MID를 다운로딩/프로비져닝 하도록 PVA 또는 DPF에 요청함
950
PVA 또는 DPF는 새로운 MID 패키지를 M2ME로 다운로딩
960
M2ME는 MID가 폐기되었다는 메시지를 구 홈 네트워크 오퍼레이터에 보냄
970
구 홈 네트워크 오퍼레이터는 M2ME에 ACK를 보내며, 그 다음 M2ME는 이를 PVA 또는 DPF에 그리고 그 다음 새로운 홈 네트워크 오퍼레이터에 전송함
980
M2ME는 자신의 시스템을 업데이트하고/PVA 또는 DPF의 도움으로 MID를 설치하고 성공/실패 메시지를 보냄
990
PVA 또는 DPF는 새로운 홈 네트워크 오퍼레이터에 성공/실패 메시지를 보고함
992
성공시, 프로비져닝 프로세스가 완료됨
998