(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년12월31일
(11) 등록번호 10-1478415
(24) 등록일자 2014년12월24일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04W 12/10* (2009.01)
(21) 출원번호 10-2012-7012421
(22) 출원일자(국제) 2010년10월15일
심사청구일자 2012년05월14일
(85) 번역문제출일자 2012년05월14일
(65) 공개번호 10-2012-0092635
(43) 공개일자 2012년08월21일
(86) 국제출원번호 PCT/US2010/052865
(87) 국제공개번호 WO 2011/047276
국제공개일자 2011년04월21일
(30) 우선권주장
61/251,920 2009년10월15일 미국(US)
(56) 선행기술조사문헌
US20090205028 A1
JP2009033354 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인터디지탈 패튼 홀딩스, 인크
미국, 델라웨어주 19809, 윌밍턴, 벨뷰 파크웨이 200, 스위트 300
(72) 발명자
구치오네 루이스 제이
미국 뉴욕 10709 이스트 체스터 링컨 팰리스 211
차 인혁
미국 펜실베이니아 19067 야들리 사우쓰릿지 써클 510
(74) 대리인
김성기, 김태홍

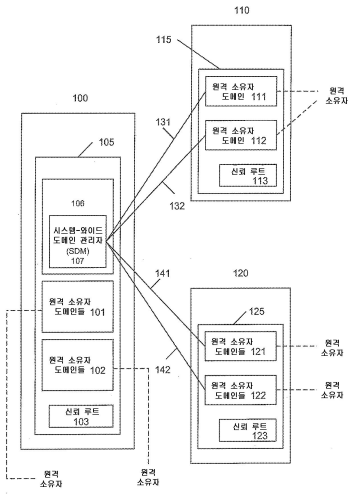
전체 청구항 수 : 총 20 항 심사관 : 이상윤

(54) 발명의 명칭 **가입 기반 서비스에 액세스하기 위한 등록 및 크리덴셜 롤 아웃**

(57) 요 약

사용자는, 하나 이상의 별개의 도메인들을 갖는 하나 이상의 디바이스들을 포함하는 시스템을 통해 가입-기반 서비스에 액세스할 수 있으며, 여기서 각각의 도메인은 하나 이상의 상이한 국지적 또는 원격적 소유자들에 의해 소유 또는 제어될 수 있다. 각각의 도메인은 상이한 소유자를 가질 수 있고 가입-기반 서비스를 제공하는 원격 소유자는 도메인의 소유권을 취득할 수 있으며, 이러한 도메인을 원격 소유자 도메인으로서 칭할 수 있다. 더 나아가, 사용자는 도메인의 소유권을 취득할 수 있으며, 이러한 도메인을 사용자 도메인이라고 칭할 수 있다. 사용자가 가입-기반 서비스에 액세스하기 위해, 등록 및 크리덴셜 롤-아웃이 요구될 수 있다. 예시적인 등록 및 크리덴셜 롤-아웃 프로세스는 사용자의 등록, 원격 소유자로부터 크리덴셜들의 획득 및 크리덴셜들의 저장을 포함할 수 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

적어도 하나의 플랫폼에 의해 지원되는 복수의 도메인들을 포함하는 제1 디바이스를 포함하는 시스템에서 수행되는 방법으로서, 상기 복수의 도메인들의 각 도메인은 적어도 하나의 플랫폼 상에서 실행하는 컴퓨팅 자원들의 구성을 포함하고 상기 복수의 도메인들의 각각의 도메인은 상기 제1 디바이스로부터 국지적으로 또는 원격적으로 위치될 수 있는 도메인의 소유자에 대한 기능들을 수행하도록 구성되고, 상기 복수의 도메인들의 각각의 도메인은 상이한 소유자를 가질 수 있고, 상기 복수의 도메인들 중의 적어도 하나의 도메인은 상기 제1 디바이스의 사용자에 의해 소유되며, 상기 복수의 도메인들 중의 적어도 하나의 다른 도메인은 원격 소유자 디바이스를 통해서 상기 제1 디바이스와 통신하는 원격 소유자에 의해 소유되는 것인, 상기 방법에 있어서,

제1 디바이스에 의해서, 상기 제1 디바이스의 원격 소유자 도메인을 통해 상기 원격 소유자에 의해 랜더링될 가입 기반 서비스의 가입된 사용자로서 상기 사용자를 상기 원격 소유자 디바이스에 등록하는 단계;

상기 제1 디바이스의 상기 원격 소유자 도메인에 의해서, 상기 사용자가 상기 가입된 사용자로서 상기 가입 기반 서비스를 이용하는 것을 가능하게 하는 크리덴셜(credential)들을 상기 원격 소유자 디바이스로부터 획득하는 단계;

상기 제1 디바이스의 상기 원격 소유자 도메인에 상기 크리덴셜들을 저장하는 단계; 및

상기 크리덴셜들이 상기 원격 소유자 도메인에 의해 수신되었다는 확인응답(acknowledgement)을 상기 제1 디바이스의 사용자 도메인에 의해 상기 원격 소유자 도메인으로부터 수신하는 단계를 포함하는, 시스템에서 수행되는 방법.

청구항 2

제 1 항에 있어서,

상기 사용자를 상기 원격 소유자 디바이스에 등록하는 단계는,

상기 사용자를 대신하여 상기 사용자 도메인에 의해, 등록 요청을 개시하는 단계;

상기 등록 요청에 응답하여 상기 원격 소유자 도메인에 의해, 상기 사용자에 대한 상기 가입 기반 서비스의 판매를 가능하게 해주는 제3자 디바이스(third party device)로부터, 상기 사용자를 상기 가입 기반 서비스의 가입된 사용자로서 상기 원격 소유자에게 식별해주는데 이용될 식별자를 요청하는 단계;

상기 원격 소유자 도메인에 의해, 상기 제3자 디바이스로부터 상기 식별자를 수신하는 단계; 및

상기 사용자 도메인에 의해, 상기 등록 요청이 수신되었다는 확인응답을 상기 원격 소유자 디바이스로부터 수신하는 단계를 포함하는 것인, 시스템에서 수행되는 방법.

청구항 3

제 2 항에 있어서,

상기 사용자를 상기 원격 소유자 디바이스에 등록하는 단계는,

상기 사용자 도메인에 의해, 상기 등록 요청과 연관된 제 1 프로세스 식별자 또는 상기 사용자와 관련되는 개인정보 중 적어도 하나를 송신하는 단계; 및

상기 사용자 도메인에 의해, 상기 제3자 디바이스로부터 상기 등록 요청과 연관된 제 2 프로세스 식별자를 수신하는 단계를 더 포함하는 것인, 시스템에서 수행되는 방법.

청구항 4

제 2 항에 있어서,

상기 식별자는, 상기 가입 기반 서비스의 사용자들을 등록하는데 사용하기 위해 상기 원격 소유자 디바이스에 의해 상기 제3자 디바이스에게 분배되는(dispensed) 식별자들의 그룹 중의 하나의 식별자인 것인, 시스템에서

수행되는 방법.

청구항 5

제 1 항에 있어서,

상기 원격 소유자 디바이스로부터 크리덴셜들을 획득하는 단계는,

상기 사용자 도메인에 의해, 크리덴셜 롤 아웃 요청(credential roll-out request)을 상기 원격 소유자 도메인에 송신하는 단계로서, 상기 크리덴셜 롤 아웃 요청은 상기 사용자에 대한 상기 가입 기반 서비스의 판매를 가능하게 해주는 제 3 자 또는 상기 사용자 중 적어도 하나를 상기 원격 소유자 도메인에게 식별해주는 정보를 포함하는 것인, 상기 송신하는 단계;

상기 원격 소유자 도메인에 의해, 상기 크리덴셜 롤 아웃 요청을 상기 원격 소유자 디바이스로 포워딩(forward)하는 단계; 및

상기 원격 소유자 도메인에 의해, 상기 원격 소유자 디바이스로부터 상기 크리덴셜들을 수신하는 단계를 포함하는 것인, 시스템에서 수행되는 방법.

청구항 6

제 5 항에 있어서,

상기 원격 소유자 도메인에 의해, 상기 복수의 도메인들의 컴포넌트에 의한 상기 적어도 하나의 플랫폼의 반 자율적인 무결성 검증(semi-autonomous integrity verification)을 요청하는 단계; 및

상기 원격 소유자 도메인에 의해, 상기 적어도 하나의 플랫폼으로부터 무결성 검증 정보를 수신하는 단계를 더 포함하는, 시스템에서 수행되는 방법.

청구항 7

제 6 항에 있어서,

상기 무결성 검증 정보는, 상기 원격 소유자 디바이스가 상기 제1 디바이스의 복수의 도메인들 중의 적어도 하나의 도메인의 신뢰성(trustworthiness)을 평가하는 것을 허용하는 것인, 시스템에서 수행되는 방법.

청구항 8

제 1 항에 있어서,

상기 제1 디바이스에 의해서, 상기 사용자를 상기 사용자 도메인에 등록하는 단계를 더 포함하는, 시스템에서 수행되는 방법.

청구항 9

제 8 항에 있어서,

상기 사용자를 상기 사용자 도메인에 등록하는 단계는, 상기 사용자를 상기 사용자 도메인에게 식별해주는 정보를 상기 사용자로부터 상기 제1 디바이스의 상기 사용자 도메인이 수신하는 단계를 포함하는 것인, 시스템에서 수행되는 방법.

청구항 10

제 1 항에 있어서,

상기 크리덴셜들은 상기 사용자가 상기 가입 기반 서비스를 이용할 때마다 상기 사용자가 인증되는 것을 가능하게 하는 것인, 시스템에서 수행되는 방법.

청구항 11

시스템에 있어서,

적어도 하나의 플랫폼에 의해 지원되는 복수의 도메인들을 포함하는 제1 디바이스를 포함하고,

상기 복수의 도메인들의 각각의 도메인은 적어도 하나의 플랫폼 상에서 실행하는 컴퓨팅 자원들의 구성을 포함하고 상기 복수의 도메인들의 각각의 도메인은 상기 제1 디바이스로부터 국지적으로 또는 원격적으로 위치될 수 있는 도메인의 소유자에 대한 기능들을 수행하도록 구성되고, 각각의 도메인은 상이한 소유자를 가질 수 있고, 상기 복수의 도메인들 중의 적어도 하나의 도메인은 상기 제1 디바이스의 사용자에 의해 소유되고, 상기 복수의 도메인들 중의 적어도 하나의 다른 도메인은 원격 소유자 디바이스를 통해서 상기 제1 디바이스와 통신하는 원격 소유자에 의해 소유되며,

상기 제1 디바이스는,

상기 제1 디바이스의 원격 소유자 도메인을 통해 상기 원격 소유자에 의해 랜더링될 가입 기반 서비스의 가입된 사용자로서 상기 사용자를 상기 원격 소유자 디바이스에 등록하고,

상기 사용자가 상기 가입된 사용자로서 상기 가입 기반 서비스를 이용하는 것을 가능하게 하는 크리덴셜(credential)들을 상기 원격 소유자 디바이스로부터 획득하고,

상기 원격 소유자 도메인에 상기 크리덴셜들을 저장하며,

사용자 도메인에 의해, 상기 크리덴셜들이 상기 원격 소유자 도메인에 의해 수신되었다는 확인응답(acknowledgement)을 상기 원격 소유자 도메인으로부터 수신하도록 구성되는 것인, 시스템.

청구항 12

제 11 항에 있어서,

상기 사용자를 상기 원격 소유자 디바이스에 등록하기 위해서 상기 제1 디바이스는 또한,

상기 사용자를 대신하여 상기 사용자 도메인에 의해 등록 요청을 개시하고,

상기 등록 요청에 응답하여 상기 원격 소유자 도메인에 의해, 상기 사용자에 대한 상기 가입 기반 서비스의 판매를 가능하게 해주는 제3자 디바이스로부터, 상기 사용자를 상기 가입 기반 서비스의 가입된 사용자로서 상기 원격 소유자에게 식별해주는데 이용될 식별자를 요청하며,

상기 원격 소유자 도메인에 의해, 상기 제3자 디바이스로부터 상기 식별자를 수신하고;

상기 사용자 도메인에 의해, 상기 등록 요청이 수신되었다는 확인응답을 상기 원격 소유자 디바이스로부터 수신하도록 구성되는 것인, 시스템.

청구항 13

제 12 항에 있어서,

상기 사용자를 상기 원격 소유자 디바이스에 등록하기 위해서 상기 제1 디바이스는 또한,

상기 사용자 도메인에 의해, 상기 등록 요청과 연관된 제 1 프로세스 식별자 또는 상기 사용자와 관련되는 개인 정보 중 적어도 하나를 송신하며;

상기 사용자 도메인에 의해, 상기 제3자 디바이스로부터 상기 등록 요청과 연관된 제 2 프로세스 식별자를 수신하도록 구성되는 것인, 시스템.

청구항 14

제 12 항에 있어서,

상기 식별자는 상기 가입 기반 서비스의 사용자들을 등록하는데 사용하기 위해 상기 원격 소유자 디바이스에 의해 상기 제3자 디바이스로 분배되는(dispensed) 식별자들의 그룹 중의 하나의 식별자인 것인, 시스템.

청구항 15

제 11 항에 있어서,

상기 원격 소유자 디바이스로부터 크리덴셜들을 획득하기 위해서 상기 제1 디바이스는 또한,

상기 사용자 도메인에 의해, 크리덴셜 롤 아웃 요청(credential roll-out request) - 상기 크리덴셜 롤 아웃 요

청은 상기 사용자에 대한 상기 가입 기반 서비스의 판매를 가능하게 해주는 제 3 자 또는 상기 사용자 중 적어도 하나를 상기 원격 소유자 도메인에게 식별해주는 정보를 포함함 - 을 상기 원격 소유자 도메인에 송신하고,

상기 원격 소유자 도메인에 의해, 상기 크리덴셜 롤 아웃 요청을 상기 원격 소유자 디바이스로 포워딩하며,

상기 원격 소유자 도메인에 의해, 상기 원격 소유자 디바이스로부터 상기 크리덴셜들을 수신하도록 구성되는 것인, 시스템.

청구항 16

제 15 항에 있어서,

상기 제1 디바이스는 또한,

상기 원격 소유자 도메인에 의해, 상기 복수의 도메인들의 컴포넌트에 의한 상기 적어도 하나의 플랫폼의 반 자율적인 무결성 검증(semi-autonomous integrity verification)을 요청하며,

상기 원격 소유자 도메인에 의해, 상기 적어도 하나의 플랫폼으로부터 무결성 검증 정보를 수신하도록 구성되는 것인, 시스템.

청구항 17

제 16 항에 있어서,

상기 무결성 검증 정보는 상기 원격 소유자 디바이스가 상기 제1 디바이스의 상기 복수의 도메인들 중의 적어도 하나의 도메인의 신뢰성(trustworthiness)을 평가하는 것을 허용하는 것인, 시스템.

청구항 18

제 11 항에 있어서,

상기 제1 디바이스는 또한 상기 사용자를 상기 사용자 도메인에 등록하도록 구성되는 것인, 시스템.

청구항 19

제 18 항에 있어서,

상기 사용자를 상기 사용자 도메인에 등록하기 위해서, 상기 제1 디바이스는 또한, 상기 사용자 도메인에 의해, 상기 사용자를 상기 제1 디바이스의 상기 사용자 도메인에게 식별해주는 정보를 상기 사용자로부터 수신하도록 구성되는 것인, 시스템.

청구항 20

제 11 항에 있어서,

상기 크리덴셜들은 상기 사용자가 상기 가입 기반 서비스를 이용할 때마다 상기 사용자가 인증되는 것을 가능하게 하는 것인, 시스템.

명 세 서

기 술 분 야

[0001] 관련 출원들에 대한 상호-참조

[0002] 본 출원은 2009년 10월 15일 출원된 미국 가특허 출원 번호 제61/251,920호에 기초하고 이에 대한 우선권을 청구하며, 그의 개시물은 여기에 참조로서 그 전체가 통합된다.

배 경 기 술

[0003] 오늘날, 디바이스, 또는 디바이스 내의 몇몇 부분 또는 컴퓨팅 환경이 개인, 조직 또는 몇몇 다른 엔티티에 의해 "소유"되는 방식으로, 다른 디바이스들 또는 엔티티들과 통신하거나 통신하지 않을 수 있는 컴퓨팅 디바이스가 이용되는 다수의 상황들이 존재한다. "소유되는" 것에 대해서, 우리는 디바이스, 디바이스 내의 몇몇 부분 또는 컴퓨팅 환경이 엔티티에 대해 인증될 수 있고, 그 후 엔티티는 디바이스 또는 디바이스의 몇몇 부분에 대

한 임의의 형태의 제어를 취득한다는 것을 의미한다. 이러한 상황의 일 예는 모바일 전화와 같은 무선 디바이스의 사용자가 특정한 모바일 통신 네트워크 운용자의 서비스들에 가입할 수 있는 무선 모바일 통신 산업에 존재한다.

[0004] 오늘날 모바일 통신 산업에서, 무선 디바이스들(이 무선 디바이스들의 사용자는 특정 네트워크 운용자의 서비스들에 가입할 수 있음)은 통상적으로 가입자 식별 모듈(Subscriber Identity Module; SIM) 또는 범용 집적 회로 카드(Universal Integrated Circuit Card; UICC)를 포함한다. SIM/UICC는 안전한 실행 및 저장 환경을 무선 디바이스에 제공하여 이로부터 인증 알고리즘을 실행하고 크리덴셜(credential)들을 저장하며, 이는 디바이스가 네트워크 운용자에 대해 네트워크 운용자와의 디바이스 사용자의 가입을 인증하는 것을 가능하게 하고 네트워크 운용자가 디바이스에 대한 임의의 형태의 제어, 즉, 소유권을 갖는 것을 허용한다. 불행히도, 이 SIM/UICC 매커니즘은 통상적으로 단일의 네트워크 운용자와의 이용으로 제한된다.

[0005] 따라서, 모바일 통신 디바이스들과 관련하여 위에서 기술된 상황과 유사한 오늘날의 다수의 컴퓨팅 상황에서의 문제는 컴퓨팅 디바이스들이 종종 단일의 엔티티에 의해 완전히 "소유"되는 것으로 제한된다는 것이다. 그리고, 소유권이 사용자에 의한 디바이스의 구매 시에 설정되어야 하는 다수의 경우들에서, 추후에 소유권을 설정하는 것이 바람직할 수 있는 비지니스 모델들(business models)을 방해한다. 또한, 이 제한들은 디바이스의 다수의 서로 분리된 부분들의 다수의 소유권들이 존재하거나, 또는 소유권이 매번 다른 엔티티들로 천이되는 것이 바람직할 수 있는 상황들에서 디바이스들의 이용을 방해한다. 예를 들어, 모바일 전화와 같은 무선 모바일 통신 디바이스의 경우에, 사용자들은 통상적으로 구매시에 특정 모바일 네트워크 운용자의 서비스들에 가입하도록 요구되고, 이러한 디바이스들은 모바일 네트워크 운용자가 종종 무선 디바이스를 구매하고 나서 몇시간 후에나 인지될 수 있는 애플리케이션들에서 이용되는 것이 방지된다. 또한, 통상적으로 이러한 디바이스들이 한번에 다수의 운용자 네트워크들에 대한 액세스를 제공하는 것은 가능하지 않다. 모바일 네트워크 및 서비스 가입의 갱신 또는 변경은 어려울 수 있고, OTA(over-the-air)로 이를 수행하는 것은 보통 가능하지 않다.

[0006] 또한, 특히 무선 모바일 통신 디바이스의 환경에서, SIM/UICC 매커니즘은 일반적으로 매우 안전한 것으로 고려되지만, 보안은 그것이 상주하고 있는 전체 디바이스의 보안 특성들에 강하게 링크되지 않는다. 이는 모바일 금융 거래(financial transaction)와 같은 진보된 서비스들 및 애플리케이션들에 대한 보안 개념들을 스케일링하는 애플리케이션들을 제한한다. 특히, 이러한 단점들은 M2M(machine-to-machine) 통신 디바이스들과 같은 자율적인 디바이스들에 관련된다.

[0007] 이에 따라, 보다 동적인 해결책이 바람직하다.

발명의 내용

[0008] 사용자가 디바이스 상에서 도메인의 원격 소유자로부터 가입 기반 서비스에 액세스하는 것을 허용할 수 있는 시스템들 및 방법들이 개시된다. 사용자는 각각의 도메인이 하나 이상의 상이한 국지적 또는 원격적 소유자들에 의해 소유되거나 제어될 수 있는 하나 이상의 별개의 도메인들과 더불어 하나 이상의 디바이스들을 포함하는 시스템을 통해 가입 기반 서비스에 액세스할 수 있다. 하나 이상의 디바이스들은 적어도 하나의 플랫폼에 의해 지원되는 하나 이상의 도메인들을 포함할 수 있다. 각 플랫폼은 도메인들에 대한 저-레벨 컴퓨팅, 저장, 또는 통신 자원들을 제공할 수 있다. 플랫폼은 몇 개의 하드웨어, 운영체제, 몇 개의 저-레벨 펌웨어 또는 소프트웨어(예를 들어, 부트 코드들, BIOS, API들, 드라이버들, 미들웨어, 또는 가상 소프트웨어(virtualization software) 및 몇 개의 고-레벨 펌웨어 또는 소프트웨어(예를 들어, 응용 소프트웨어) 및 이러한 자원들의 각각의 구성 데이터로 구성될 수 있다. 각각의 도메인은 적어도 하나의 플랫폼 상에서 실행하는 컴퓨팅, 저장 또는 통신 자원들의 구성을 포함할 수 있고 각 도메인은 도메인으로부터 국지적으로 또는 원격적으로 위치될 수 있는 도메인의 소유자에 대한 기능들을 수행하도록 구성될 수 있다. 각각의 도메인은 상이한 소유자를 가질 수 있고, 각각의 소유자는 자신의 도메인의 동작들은 물론, 도메인이 상주하고 있는 플랫폼 및 다른 도메인들에 관하여 자신의 도메인들의 동작들에 대한 정책들을 특정할 수 있다. 가입 기반 서비스를 제공하는 원격 소유자는 원격 소유자 도메인으로서 지칭될 수 있는 도메인의 소유권을 취득할 수 있다. 또한, 사용자는 사용자 도메인으로서 지칭될 수 있는 도메인의 소유권을 취득할 수 있다.

[0009] 사용자가 가입-기반 서비스에 액세스하기 위해, 등록 및 크리덴셜 롤-아웃이 요구될 수 있다. 예시적인 등록 및 크리덴셜 롤-아웃 프로세스는 사용자의 등록, 원격 소유자로부터 크리덴셜들을 획득 및 크리덴셜들의 저장을 포함할 수 있다.

[0010] 등록은 원격 소유자 도메인을 통해 원격 소유자에 의해 랜더링되는 가입-기반 서비스의 가입된 사용자로서 원격

소유자에 사용자를 등록하는 것을 포함할 수 있다. 사용자 도메인은 원격 소유자 도메인에 요청을 송신함으로써 사용자 대신 등록을 개시할 수 있다. 원격 소유자 도메인은 가입-기반 서비스의 가입된 사용자로서 원격 소유자에게 사용자를 식별시키도록 이용되는 식별자를 요청할 수 있다. 요청은 사용자에게 가입-기반 서비스의 판매를 용이하게 하는 제 3 자에 대해 행해질 수 있다. 원격 소유자 도메인은 제 3 자로부터 식별자를 수신할 수 있고, 사용자 도메인은 등록을 위한 요청이 수신되었다는 확인응답(acknowledgement)을 원격 소유자로부터 수신할 수 있다.

[0011] 크리덴셜들의 획득 및 저장은 사용자 도메인이 크리덴셜 롤-아웃 요청(credential roll-out request)을 원격 소유자 도메인에게 송신하는 것을 포함할 수 있다. 요청은 사용자 및/또는 제 3 자를 식별하는 정보를 포함할 수 있다. 원격 소유자 도메인은 크리덴셜 롤-아웃 요청을 원격 소유자에게 송신할 수 있다. 원격 소유자 도메인은 원격 소유자로부터 크린덴셜들을 수신하고 크리덴셜들이 원격 소유자 도메인에 의해 수신되었다는 확인응답을 사용자 도메인에 송신할 수 있다.

[0012] 여기서 기술되는 시스템들, 방법들 및 수단들의 다른 특징들은 이하의 상세한 설명 및 첨부 도면들에서 제공된다.

도면의 간단한 설명

[0013] 도 1은 여기서 기술되는 방법들 및 수단들이 이용될 수 있는 예시적인 시스템을 예시하는 도면.

도 2는 여기서 기술되는 방법들 및 수단들이 사용자 장비(UE)에서 실현되는 시스템의 실시예를 예시하는 도면.

도 3 및 3a는 도메인의 소유권을 취득하기 위한 예시적인 부트업(boot up) 및 프로세스를 예시하는 도면.

도 4 및 4a는 도메인의 소유권을 취득하는 프로세스를 위한 예시적인 호 흐름도를 예시하는 도면.

도 5 및 도 5a는 완전한 입증(full attestation)을 통해 도메인의 소유권을 취득하는 프로세스에 대한 예시적인 호 흐름도를 예시하는 도면.

도 6은 신뢰적인 하드웨어 가입 모듈의 실시예의 예시적인 상태 정의들, 천이들, 및 제어 지점 정의를 예시하는 도면.

도 7은 원격 소유자 도메인들을 달성할 수 있는 예시적인 상태들 및 천이들이 동적으로 관리되는 환경에서 발생할 수 있는 조건들을 예시하는 도면.

도 8은 등록 및 크리덴셜 롤-아웃 프로세스를 구현하는 예시적인 호 흐름들을 예시하는 도면.

도 9는 하나 이상의 개시된 실시예들이 구현될 수 있는 예시적인 통신 시스템의 시스템도이다.

발명을 실시하기 위한 구체적인 내용

[0014] **I. 예시적인 다중-도메인 시스템**

[0015] 도 1 내지 도 7은 개시되는 시스템들, 방법들 및 수단들이 구현될 수 있는 예시적인 실시예들에 관한 것일 수 있다. 그러나 본 발명이 예시적인 실시예들과 관련하여 기술될 수 있지만, 본 발명은 이것으로 제한되지 않고, 다른 실시예들이 이용될 수 있거나, 또는 본 발명으로부터 벗어남 없이 본 발명의 동일한 기능을 수행하도록 기술된 실시예들에 대해 수정들 및 부가들이 행해질 수 있다는 것이 이해될 것이다.

[0016] 개시된 시스템들, 방법들, 및 수단들이 구현될 수 있는 예시적인 시스템은 각각이 적어도 하나의 플랫폼에 의해 지원되는 하나 이상의 도메인들을 포함할 수 있는 하나 이상의 디바이스들을 포함한다. 각각의 플랫폼은 도메인들에 대한 저-레벨 컴퓨팅, 저장, 또는 통신 자원들을 제공할 수 있다. 플랫폼은 몇 개의 하드웨어, 운영 체제, 및 다른 저-레벨 펌웨어 또는 소프트웨어(예를 들어, 부트 코드들, BIOS, 및 드라이버들) 및 이러한 자원들에 대한 각각의 구성 데이터로 구성될 수 있다. 각각의 도메인은 적어도 하나의 플랫폼 상에서 실행하는 컴퓨팅, 저장, 또는 통신 자원들의 구성을 포함할 수 있으며, 각각의 도메인은 도메인으로부터 국지적으로 또는 원격적으로 위치될 수 있는 도메인의 소유자에 대한 기능들을 수행하도록 구성될 수 있다. 각각의 도메인은 상이한 소유자를 가질 수 있고, 각각의 소유자는 자신의 도메인의 동작들은 물론, 도메인이 상주하고 있는 플랫폼 및 다른 도메인들에 관하여 자신의 도메인들의 동작들에 대한 정책들을 특정할 수 있다.

[0017] 각각의 도메인은 (입력 관점으로부터) 컴퓨팅, 저장, 또는 통신 자원들 또는 (출력 관점으로부터) 이러한 컴퓨팅, 저장, 또는 통신 자원들을 이용함으로써 도메인이 제공하는 기능들에 관하여 다른 도메인들로부터 분리될

수 있다. 각각의 도메인은 공통 기저 플랫폼(common underlying platform)의 컴퓨팅, 저장, 또는 통신 자원들 또는 기능들을 이끌어낼 수 있다(draw on). 몇몇 도메인들은 공통 플랫폼에 의해 제공되는 이러한 기능들 중 일부를 공유할 수 있다. 플랫폼 자원들 및/또는 기능들의 이러한 공유는 공통 자원들 또는 기능들의 각각의 도메인의 이용이 다른 도메인의 이러한 이용으로부터 분리될 수 있는 방식으로 행해질 수 있다. 예를 들어, 이러한 분리는 자원들에 대한 엄격한 액세스 제어를 시행하는 디바이스의 플랫폼에 의해 달성될 수 있으며, 이 플랫폼은 도메인의 자원들에 대한 임의의 액세스가 사용자(들), 소유자(들), 또는 플랫폼 및/또는 도메인의 소유자에 의해 인가되는 도메인 외부의 다른 엔티티들 또는 프로세스들에만 허용될 수 있도록 도메인들 각각에 자원을 제공한다. 또한, 도메인의 기능 중 임의의 기능이 디바이스 상의 도메인들 중 임의의 도메인 외부에 있는 디바이스의 자원들에 의존하는 한, 플랫폼은 단순히 분리된 도메인들 중 임의의 도메인의 부분이 아닌 디바이스의 부분으로 단순히 구성된다.

[0018] 동일한 또는 상이한 플랫폼들 상의 또는 동일한 또는 상이한 디바이스들 상의 임의의 2개의 도메인들 간의 통신은 안전하게 행해질 수 있는데, 이는 도메인들이 안전한 방식(예를 들어, 암호 수단을 이용함으로써)으로 서로 인증하고, 비밀성(confidentiality), 무결성 및 선도(freshness)와 같은 보안 양상들에 대해서 도메인들 간에 교환되는 메시지를 또한 보호할 수 있다는 것을 의미한다. 도메인들이 상주하는 플랫폼(들)에 의해 제공되는 암호 수단은 임의의 이러한 2개의 도메인들 사이에서 이러한 안전한 통신을 제공하는데 이용될 수 있다.

[0019] 시스템-와이드 도메인 관리자(system-wide domain manager)는 도메인들 중 하나 상에 상주할 수 있다. 시스템-와이드 도메인 관리자는 상주하고 있는 도메인들의 정책들을 시행할 수 있고, 시스템-와이드 도메인 관리자는 시스템-와이드 도메인 관리자가 상주하는 도메인에 관하여 다른 도메인들 각각의 정책들에 의한 다른 도메인들의 시행(enforcement)을 조절할 수 있다. 부가적으로, 시스템-와이드 도메인 관리자는 다른 도메인들 사이에서 그들 각각의 정책들에 따라 상호작용을 조절할 수 있다. 시스템-와이드 도메인 관리자가 상주하는 도메인은 도메인을 하우징하는 디바이스의 소유자에 의해 소유될 수 있다. 대안적으로, 이러한 도메인은 도메인을 하우징하는 디바이스를 소유하지 않을 수 있는 소유자에 의해 소유될 수 있다.

[0020] 도 1은 이러한 시스템의 일 실시예를 예시한다. 도시된 바와 같이, 시스템은 하나 이상의 디바이스들(100, 110 및 120)을 포함할 수 있다. 각각의 디바이스는 적어도 하나의 플랫폼에 의해 지원되는 하나 이상의 도메인들을 포함할 수 있다. 예를 들어, 디바이스(100)는 도메인(106) 및 하나 이상의 다른 도메인들(101, 102)을 포함할 수 있다. 3개의 도메인들이 디바이스(100)에 대해 도시되었지만, 다른 실시예들에서, 도메인들의 수는 더 많거나 더 적을 수 있다. 이 도메인들(101, 102, 106) 각각은 디바이스의 적어도 하나의 플랫폼(105) 상에서 실행하는 컴퓨팅, 저장, 또는 통신 자원들의 구성을 포함할 수 있다. 각각의 도메인은 도메인으로부터 국지적으로 또는 원격적으로 위치될 수 있는 도메인의 소유자에 대한 기능들을 수행하도록 구성될 수 있다. 예를 들어, 도메인(106)은 디바이스 소유자(도시되지 않음)에 의해 소유될 수 있는 반면에, 도메인들(101, 102)은 하나 이상의 원격 소유자들에 의해 소유될 수 있다. 각각의 도메인은 상이한 소유자를 가질 수 있거나, 또는 디바이스의 2개 이상의 도메인은 동일한 소유자에 의해 소유될 수 있다. 각각의 소유자는 자신의 도메인의 동작은 물론, 도메인이 동작하는 플랫폼, 도메인이 상주하는 디바이스, 및 동일하거나 상이한 디바이스 내의 다른 도메인들에 관하여 그의 도메인의 동작에 대한 정책들을 특정할 수 있다.

[0021] 언급한 바와 같이, 시스템은 또한 다른 도메인들이 상주하는 다른 디바이스들을 포함할 수 있다. 예를 들어, 디바이스(110)는 각각이 동일한 원격 소유자에 의해 소유될 수 있는 도메인들(111 및 112)을 포함할 수 있다. 물론, 도메인들(111 및 112) 각각은 대신 상이한 소유자에 의해 소유될 수 있다. 도메인들(111, 112) 각각은 디바이스(110)의 플랫폼(115) 상에서 실행하는 컴퓨팅, 저장, 또는 통신 자원들의 구성을 포함할 수 있다. 유사하게, 디바이스(120)는 도메인들(121 및 122)을 포함할 수 있다. 이 예에서 도시되는 바와 같이, 이 도메인들 각각은 상이한 소유자에 의해 소유될 수 있다. 대안적으로, 이 도메인들은 동일한 소유자에 의해 소유될 수 있다. 재차, 도메인들(121, 122) 각각은 디바이스(120)의 플랫폼(125) 상에서 실행하는 컴퓨팅, 저장, 또는 통신 자원들의 구성을 포함할 수 있다.

[0022] 시스템-와이드 도메인 관리자(system-wide domain manager; SDM)(107)는 도메인들 중 하나 상에 상주할 수 있다. 이 예에서, SDM(107)은 디바이스(100)의 도메인(106) 상에 상주한다. 일 실시예에서, SDM이 상주하는 도메인(예를 들어, 도메인(106))은 디바이스(100)의 소유자에 의해 소유된다. SDM(107)은 디바이스(100)에서 제공되는 통신 매커니즘을 통해 디바이스(100) 상의 원격 소유자 도메인(101)과 통신한다. 부가적으로, SDM(107)은 유선 또는 무선 채널들일 수 있는 각각의 통신 채널들(131, 132, 141, 142)을 통해 다른 디바이스들 상의 도메인들과 통신한다. 통신 채널들(131, 132, 141, 및 142)은 안전할 수 있다. SDM(107)은 SDM(107)이 상주하는 도메인(106)의 정책들을 시행하고, SDM(107)은 도메인(106)에 관하여 그들 각자의 정책들에 의한 다른 도

메인들(101, 111, 112, 121, 122))의 시행을 조절할 수 있다. 부가적으로, SDM(107)은 그들 각자의 정책들은 물론, SDM이 상주하는 도메인의 정책(그 특정한 도메인의 소유자의 정책일 수 있음)에 따라 다른 도메인들 간의 상호작용을 조절할 수 있다.

[0023] 예로서, 일 실시예에서, 도메인은 서비스 제공자에 의해 소유될 수 있다. 예를 들어, 디바이스(100)의 도메인(102)은 단지 예로서, 모바일 네트워크 운용자와 같은 서비스 제공자에 의해 소유될 수 있다. 도메인(102)은 디바이스(100)와 서비스 제공자 간의 통신을 가능하게 하기 위해, 서비스 제공자에 대해서 디바이스(100)를 인증하거나, 또는 몇몇 경우들에서 동등하게, 디바이스의 사용자 또는 소유자의 가입은 인증하기 위한 가입자 식별 모듈(SIM) 기능을 수행할 수 있다.

[0024] 위에서 기술한 SDM의 기능들 외에, SDM(107)은 정보에 액세스하고 상기 하나 이상의 도메인들에 의한 이용을 위해 이용 가능한 자원들의 리스트를 제공할 수 있다. SDM(107)은 또한, 원격 소유자들에 의해 소유되는 도메인들의 로딩(loading) 및 유지보수(maintenance)를 감독할 수 있다. SDM(107)은 SDM(107)이 상주하는 디바이스(100)의 사용자들에게 로딩 가능한 도메인들의 리스트를 제공할 수 있고, 리스트된 도메인들 중에서 사용자가 로딩할 도메인을 선택하도록 요청할 수 있다. SDM은 또한 플랫폼 또는 디바이스 상에 로딩과 이에 따른 하나 이상의 도메인들의 동작을 지원하기에 충분한 컴퓨팅 자원들이 존재하는지를 평가할 수 있다.

[0025] 위에서 또한 언급한 바와 같이, SDM(107)은 여기서 시스템-와이드 도메인 정책(system-wide domain policy; SDP)으로서 지칭될 수 있는 그 자신의 정책(들)은 물론, 다른 도메인들의 정책(들), 즉 도메인-특정 정책(domain-specific policy; DP)들을 시행하는데 가담할 수 있다. SDM(107)은 새로운 도메인을 로딩할지를 평가할 때 하나 이상의 기존의 도메인들의 정책들을 고려할 수 있다. 예를 들어, 원격 소유자에 의해 소유되는 주어진 도메인의 정책은, 특정 타입의 다른 도메인이 활성이 될 때 주어진 도메인이 비활성이 된다는 것을 특정할 수 있다. 다른 예에서, 원격 소유자에 의해 소유되는 주어진 도메인의 정책은, 특정한 다른 원격 소유자에 의해 소유되는 다른 도메인이 활성이 될 때 주어진 도메인이 비활성이 된다는 것을 특정할 수 있다. 또 다른 예에서, 원격 소유자에 의해 소유되는 주어진 도메인의 정책은, 특정한 타입의 다른 도메인이 활성이 될 때 임의의 특정한 방식(들)으로 주어진 도메인의 동작이 제한된다는 것을 특정할 수 있다. 추가의 예에서, 원격 소유자에 의해 소유되는 주어진 도메인의 정책은, 특정한 다른 원격 소유자에 의해 소유되는 다른 도메인이 활성이 될 때 임의의 특정한 방식(들)으로 주어진 도메인의 동작이 제한된다는 것을 특정할 수 있다. SDM(107)은 이러한 타입들의 정책들 모두의 시행을 전담할 수 있다.

[0026] SDM(107)은 또한 원격 소유자들이 추후에 소유권을 취득할 수 있는 도메인들을 설정하거나 로딩할 수 있다. 예를 들어, 이러한 도메인은 어떠한 소유자에 의해서도 소유되지 않는 "원래의(pristine)" 상태로서 여기서 지칭되는 상태로 설정될 수 있으며, SDM(107)은 원격 소유자에 의한 도메인의 소유권의 설정을 관리할 수 있다.

[0027] 이를 위해, SDM(107)은 도메인의 소유권을 설정해야 할지를 결정하는데 있어서 원격 소유자가 고려할 수 있는 정보를 원격 소유자에게 전송할 수 있다. 정보는 (i) 소유권이 조사되는 도메인의 무결성을 입증하는 정보; 및 (ii) 시스템의 적어도 하나의 다른 도메인의 무결성을 입증하는 정보 중 적어도 하나를 포함할 수 있다. 정보는 또한, (i) 동작을 위해 소유권이 조사되는 도메인이 동작하는 그의 자원들을 이용하여 플랫폼의 무결성을 입증하는 정보; 및 (ii) 시스템의 적어도 하나의 다른 도메인이 동작하는 그의 자원들을 이용하여 플랫폼의 무결성을 입증하는 정보를 포함할 수 있다. 또한, 정보는 디바이스의 현재 환경에 관한 정보를 포함할 수 있다. 이러한 정보는, (i) 시스템 내의 다른 도메인들의 수를 표시하는 값; (ii) 시스템 내의 다른 도메인들의 간략한 본질(summary nature)을 제공하는 정보; 및 (iii) 소유권이 설정되도록 시도되는 도메인에 의한 이용을 위해 이용 가능한 플랫폼의 자원들을 특정하는 정보를 포함할 수 있다. 시스템의 다른 도메인들에 관하여 정보가 원격 소유자에게 제공되는 정도(degree)는 비밀성 및/또는 분리에 관하여 이 다른 도메인들의 각자의 정책이 조건부로 될 수 있다.

[0028] 원격 소유자가 도메인의 소유권을 취득한 이후, 원격 소유자는 도메인에 대해 어느 정도의 제어(a degree of control)를 행사할 수 있다. 예를 들어, 원격 소유자가 도메인의 소유권을 설정한 이후, 도메인은 도메인의 기능을 증가시키기 위해 암호 키들, 구성 정보, 파라미터 및 실행 가능한 코드 중 적어도 하나를 원격 소유자로부터 수신할 수 있다. 다른 예에서, 원격 소유자가 도메인의 소유권을 설정한 이후, 도메인은 원격 소유자로부터 그 도메인-특정 정책을 수신할 수 있다.

[0029] 여기서 개시된 시스템은 또한 하나 이상의 도메인들의 분리 및 보안을 제공할 수 있다. 예를 들어, 도메인들 중 하나 이상의 도메인들은 다른 도메인들로부터 분리되는 안전한 실행 및 저장 환경을 포함할 수 있다. 이러한 안전한 환경을 달성하기 위해, 도 1에서의 디바이스(100)의 플랫폼(105)과 같이, 하나 이상의 도메인들이 설

정되는 디바이스의 플랫폼은 신뢰 루트(root of trust)(103)를 포함할 수 있다. 신뢰 루트(103)는 하드웨어 자원들의 미리 설정된 도메인의 원격 소유자를 포함하여, 불변의 그리고 부동의 세트를 포함할 수 있으며, 도메인의 무결성은 도메인의 원격 소유자를 포함해서, 다른 것들에 의해 의존될 수 있다. 도메인(101)과 같은 도메인의 무결성은 신뢰 루트(103)에 의해 앵커되는 신뢰의 체인에 의해 설정될 수 있다. 예를 들어, 도메인(101)의 무결성은 도메인의 무결성을 검증하기 위해 신뢰 루트에 의해 이용되고 신뢰 루트(103)에 저장될 수 있는 기준 무결성 메트릭(reference integrity metric)에 도메인(101)의 적어도 하나의 컴포넌트의 측정(이 측정은 신뢰 루트(103)에 의해 생성될 수 있음)을 비교함으로써 설정될 수 있다. 대안적으로, 기준 무결성 메트릭은 원격 소유자에 의해 저장될 수 있으며, 측정은 기준 무결성 메트릭과의 비교를 위해 원격 소유자에 전송될 수 있다. 도메인의 무결성은 측정이 기준 무결성 메트릭에 매칭하는 경우 검증될 수 있다. 일 예시적인 실시예에서, 측정치는 컴포넌트 상에서 계산된 해시(hash)를 포함할 수 있으며, 기준 무결성 메트릭은 컴포넌트 상에서 앞서 계산되고 기준 무결성 메트릭의 진정성(authenticity)의 표시를 제공하는 디지털 인증서가 수반되는 해시를 포함할 수 있다. 기준 무결성 메트릭은 디바이스를 그 소유자에게 전달 시에 또는 제조 시에 디바이스내에 사전-준비(pre-provision)될 수 있다. 기준 무결성 메트릭은 또한, 디바이스의 제조/공급 이후에 통신 채널(예를 들어, 공중의 무선 통신 채널)을 통해 원격 소스로부터 그의 소유자에게 전달되고 전달 이후에 디바이스내에서 준비될 수 있다. 기준 무결성 메트릭은 인증서에 동봉되어 디바이스에 전달될 수 있다. 이러한 인증서는 디바이스로의 인증서의 전달 이후에 사용을 위해 신뢰적인 제 3 자에 의해 검증될 수 있다.

[0030] 여기서 개시된 시스템 및 그 다양한 방법들 및 수단들은 매우 다양한 컴퓨팅 및 통신 문맥들로 구현될 수 있다. 이에 따라, 도 1의 예시적인 디바이스들(100, 110 및 120)과 같은 시스템의 디바이스들은 다양한 형태들을 취할 수 있다. 예로서, 그리고 어떠한 제한도 없이, 시스템의 디바이스는 무선 전송/수신 유닛(wireless transmit/receive unit; WTRU), 사용자 장비(user equipment; UE), 모바일 스테이션, 고정식 또는 이동식 가입자 유닛, 호출기, 셀룰러 전화, 개인 휴대 정보 단말(personal digital assistant; PDA), 컴퓨터, 머신-투-머신(machine-to-machine; M2M) 디바이스, SIM 카드, 범용 집적 회로 카드(Universal Integrated Circuit Card; UICC), 스마트 카드, 지리-추적 디바이스(geo-tracking device), 센서-네트워크 노드, 미터링 디바이스(예를 들어, 물, 가스 또는 전기 미터), 또는 무선 또는 유선 환경에서 동작할 수 있는 임의의 다른 타입의 컴퓨팅 또는 통신 디바이스를 포함할 수 있다. 이어지는 도면들 및 설명은 무선 전송/수신 유닛(WTRU)에서 본 개시의 시스템들 및 방법들의 다수의 부가적인 예시적인 실시예들을 제공한다. 그러나 이 실시예들은 단지 예시적이며 여기서 개시된 시스템들 및 방법들은 이 실시예들로 어떠한 의미로도 제한되지 않는다는 것을 이해한다. 오히려, 위에서 기술된 바와 같이, 여기서 기술된 시스템들 및 방법은 매우 다양한 컴퓨팅 및 통신 환경들에서 이용될 수 있다.

[0031] 도 2는 여기서 기술되는 시스템들 및 방법들이 구현될 수 있는 WTRU의 일 실시예를 예시하는 도면이다. 도시된 바와 같이, WTRU는 UE(200)와 같은 모바일 디바이스를 포함할 수 있다. UE(200)는 모바일 장비(Mobile Equipment; ME)(210) 및 신뢰적인 하드웨어 가입 모듈(Trusted Hardware Subscription Module; THSM)(220)을 포함할 수 있다. 또한, THSM(220)은 추가로 THSM 디바이스 제조자(Device Manufacturer; DM) 도메인(221), THSM 디바이스 소유자(Device Owner; DO) 도메인(222), THSM 디바이스 사용자(Device User; DU 또는 U) 도메인(223), 시스템-와이드 도메인 관리자(SDM)(230), 도메인 간 정책 관리자(240) 및 RO의 도메인 A(224), RO의 도메인 B(225) 및 RO의 도메인 C(226)과 같은 하나 이상의 원격 소유자(RO) 도메인들을 포함할 수 있다. 또한, UE(200)는 다음의 비-예시되는 컴포넌트들: 처리기, 수신기, 전송기 및 안테나를 포함할 수 있다. 여기서 기술되는 예시적인 구현들은 도 2에 관하여 기술되는 것과 같은 컴포넌트들을 참조할 수 있다.

[0032] THSM은 통상적으로 SIM 기능들, USIM 기능들, ISIM 기능들, 액세스 네트워크 가입들에 의해 수행되는 기능들을 포함하는 신뢰적인 가입 관리 기능들을 제공하는 하드웨어-기반 모듈일 수 있다. THSM은 하드웨어-보호 모듈일 수 있다. THSM은 구체적으로 적절한 보안 특징들로 설계되는 하드웨어를 포함할 수 있다. THSM은 다수의 분리된 도메인들을 내부적으로 지원할 수 있게 될 수 있다. 도메인은 이른바 원격 소유자(Remote Owner; RO)라 칭해지는 특수한 소유자에 의해 소유되거나 청구(claim)될 수 있다. RO에 의해 청구되는 도메인은 각자의 RO에 대한 프록시로서 기능할 수 있다.

[0033] 도메인들 중 하나 이상의 도메인들은 신뢰적인 가입 아이덴티티 관리(Trusted Subscription Identity Management; TSIM)와 같은 가입 관리 기능들을 수행할 수 있다. TSIM 기능을 갖는 다수의 도메인들이 단일의 THSM 상에 존재할 수 있으므로, THSM은 다수의 RO들에 대한 가입 관리를 지원할 수 있다. TSIM-가능 도메인들의 관리의 몇몇 양상들은 이른바 시스템-와이드 도메인 관리자(System-wide Domain Manager; SDM)라 칭해지는 단일의 관리 기능에 의해 수행될 수 있다. 다른 양상들은 개별적인 도메인 내에서 또는 그 상에서 개별적으로

관리될 수 있다.

[0034] 범용 모바일 전기통신 시스템(Universal Mobile Telecommunication System; UMTS) 환경의 견지에서 기술되었지만, 당업자는 여기서 기술된 방법들 및 장치들이 본 출원의 범위를 초과함 없이 다른 환경들에 응용 가능하다는 것을 인지할 수 있다. TSIM은 "가입 애플리케이션(subscription application)"의 대표적인 예일 수 있다. 예를 들어, 3G UMTS 네트워크에서 동작하는 WTRU 상에서 구현되는 경우, TSIM은 그 기능의 일부로서, UMTS 인증 및 키 동의(authentication and key agreement; AKA) 기능을 포함하는 가입 관련 기능들 모두를 포함할 수 있다. TSIM은 UICC와 같은 특정 하드웨어에 묶여지지 않을 수 있다. 이는 UICC 상에서만 존재할 수 있는 USIM과 대조적이다. 대신, TSIM은 여기서 기술되는 바와 같이 신뢰적인 하드웨어 가입 모듈(THSM) 상에서 구현될 수 있다. 당업자는 여기서 기술되는 바와 같은 THSM의 기능이 UICC 또는 유럽 전기통신 표준 협회(European Telecommunications Standards Institute (ETSI)) UICC 요건들에 따르는 UICC와 같은 유사한 스마트 카드 또는 본 출원의 범위를 벗어남 없이 글로벌 플랫폼 규격들에 따르는 스마트 카드에 통합될 수 있다는 것을 또한 인지할 것이다.

[0035] WTRU는 THSM 및 모바일 장비(mobile equipment; ME)를 포함할 수 있다. ME는 모뎀, 라디오, 전원, 및 WTRU에서 통상적으로 발견되는 다양한 다른 특징들을 포함할 수 있다. THSM은 별개의 하드웨어-기반 모듈을 포함할 수 있다. THSM은 WTRU에 내장될 수 있거나 또는 THSM은 독립적일 수 있다. THSM이 WTRU 상에 내장되는 경우 THSM은 ME로부터 논리적으로 분리될 수 있다. THSM은 안전한, 신뢰적인 서비스들 및 애플리케이션들을 제공하기 위해 소유자의 이익을 위해 운용되고 도메인의 특정한 소유자에 의해 각각 소유되는 하나 이상의 도메인들을 포함할 수 있다. 그러므로 예를 들어, DM의 도메인은 TD_{DM}으로서 표현될 수 있고, DO의 도메인은 TD_{DO}로서 표현될 수 있다. THSM의 도메인들은 ME에서 수행하는데 안전하지 않거나 편리하지 않을 수 있는 보안-민감성 기능들 및 애플리케이션들을 수행할 수 있다.

[0036] 몇몇 도메인들은 하나 이상의 서비스 제공자들에 의해 소유되고 관리될 수 있다. 모바일 네트워크 운용자들(mobile network operator; MNO); 무선 근거리 영역 네트워크(wireless local area network; WLAN) 제공자들, 또는 WiMax 제공자들과 같은 다른 통신 네트워크 운용자들; 모바일 결제, 모바일 티켓팅, 디지털 권한 관리(digital rights management; DRM), 모바일 TV 또는 위치-기반 서비스들과 같은 애플리케이션 서비스 제공자들; 또는 IP 멀티미디어 코어 네트워크 서브시스템(IP Multimedia Core Network Subsystem; IMS) 서비스 제공자들이 예가 될 수 있다. 가입 관리는 서비스 제공자들에 의해 소유되는 도메인들에 의해 지원될 수 있다. 단순함을 위해, THSM 도메인 상에서 구현되는 가입 관리 기능들은 이하 TSIM 기능으로 표시될 수 있다. TSIM 기능들에 대한 지원은 도메인에 의해 변경될 수 있다. 예를 들어, 지원되는 TSIM 기능은 모바일 단말 상의 UICC 상의 USIM 및 ISIM 애플리케이션들에 의해 제공되는 기능과 유사한 기능들을 포함할 수 있다. THSM은 UICC와 유사하게, TSIM에 의해 제공되는 것 이외의 기능, 애플리케이션 및 데이터를 포함할 수 있다.

[0037] TSIM은 소프트웨어 유닛 또는 가상 애플리케이션일 수 있다. TSIM은 초기에 특정한 네트워크 운용자 또는 공중 지상 모바일 네트워크(Public Land Mobile Network; PLMN)와 연관되는 크리덴셜들을 갖지 않을 수 있다. TSIM은 UMTS 셀룰러 액세스 네트워크에 대한 가입 크리덴셜들/애플리케이션들의 관리를 참조할 수 있다. 예를 들어, TSIM은 UMTS 인증 키와 같은 강한 비밀(strong secret)(Ki)의 관리를 포함할 수 있다. M2M 문맥에서, TSIM은 또한 M2M 연결 아이덴티티 관리(M2M Connectivity Identity Management; MCIM)를 포함할 수 있다.

[0038] THSM은 신뢰적인 플랫폼 모듈(trusted platform module; TPM) 또는 모바일 신뢰 모듈(mobile trusted module; MTM)을 갖는 컴퓨팅 디바이스에서 발견될 수 있는 측정 신뢰 루트(root of trust of measurement; RTM)와 유사한 측정의 신뢰 코어 루트(Core Root of Trust(RoT) of Measurement; CRTM))를 포함할 수 있다. THSM의 CRTM은 예를 들어, THSM의 부트 시간(boot time)에 THSM 부트 코드의 무결성을 측정할 수 있다. 무결성 메트릭(integrity metric)은 예를 들어, THSM의 부트 코드, BIOS 및 선택적으로는 버전 번호, 소프트웨어 구성, 또는 릴리스 번호와 같은 THSM의 제조자의 특성들에 관하여 암호 다이제스트 값 동작(cryptographic digest value operation)을 적용함으로써 확장 동작을 통해 계산될 수 있다. 예를 들어, 무결성 메트릭은 SHA-X와 같은 암호 해시 알고리즘의 버전을 이용하여 계산될 수 있다.

[0039] THSM은 보호되는 스토리지에 무결성 메트릭들을 저장하기 위해 구성된, TPM 또는 MTM에서 발견되는 스토리지를 위한 신뢰 루트(root of trust for storage; RTS)와 유사한 스토리지의 코어 RoT(core RoT of Storage; CRTS) 유닛을 포함할 수 있다. THSM은 또한 THSM의 무결성 측정을 외부 챌린저들(challenger)에 리포트하도록 구성된, TPM 또는 MTM에서 발견되는 리포팅을 위한 신뢰 루트(root of trust for reporting; RTR)와 유사한 리포팅의 코어 RoT(Core RoT of Reporting; CRTR) 유닛을 포함할 수 있다.

[0040] 따라서, THSM은 신뢰 측정, 스토리지 및 리포팅의 견지에서 TPM 또는 MTM의 성능과 유사한 성능을 유효하게 제공할 수 있다. THSM은 또한 다수의 신뢰적인 이해관계자 엔진(trusted stakeholder engine)을 실현하기 위한 성능을 포함할 수 있다. 또한, THSM은 각자의 다중-이해관계자 신뢰적인 서브시스템(multiple-stakeholder trusted subsystem)들을 실현하도록 구성될 수 있다. 그러므로, THSM은 TCG 모바일 전화 워킹 그룹(Mobile Phone Working Group; MPWG) 규격들에 의해 정의되는 것과 같이 신뢰적인 모바일 전화와 유사할 수 있다.

[0041] THSM은 예를 들어, 여기서 기술되는 코어 RoT 성능들을 이용하여 다수의 내부 "이해관계자 도메인들(stake-holder domains)"을 구축하도록 구성될 수 있다. 이해관계자는 THSM 디바이스 제조자(Device Manufacturer; DM), THSM 디바이스 소유자(DO), 또는 THSM 디바이스 사용자(DU)일 수 있다. DU는 DO와 동일할 수 있거나, 또는 DO와 별개일 수 있다. THSM 당 2개 이상의 DU가 존재할 수 있다. 이해관계자는 또한 DO에 의해 특별히 임대되거나 소유되는 도메인들의 상이한 원격 소유자(RO)일 수 있다. 예를 들어, MNO와 같은 제 3 파트너쉽 프로젝트(third generation partnership project; 3GPP) PLMN 운용자, 비-3GPP 액세스 네트워크 운용자, 또는 부가 가치 애플리케이션 서비스 제공자가 이해관계자일 수 있다.

[0042] 일부 도메인들은 강제적일 수 있는데, 이 경우 일부 도메인들은 THSM의 제조 시간에 사전-구성될 수 있다. 예를 들어, DM의 도메인은 강제적일 수 있으며, DM의 도메인은 사전-구성된 파일에 따라 부트 시간에 구축 또는 로딩될 수 있다. DO의 도메인이 또한 강제적일 수 있고, DO의 도메인은 사전-준비되는 구성으로 구축될 수 있다. 대안적으로, 도메인은 다운로드되는 구성 파일에 따라 구축될 수 있다.

[0043] DM의 도메인 이외의 도메인들은 이들이 도메인의 소유자에 의해 "청구"되고 "소유"될 수 있기 이전에 원격 소유권-취득(Remote Take-Ownership) 프로세스에 처해질 수 있다. 특정 도메인이 RTO 프로세스를 통과하기 이전에, 비-특정된 소유자에 대한 "원래의" 도메인이 존재할 수 있다. 이 경우, 그 도메인에 대해 청구되는 특정 소유권이 존재하지 않는다.

[0044] THSM 상의 도메인은 THSM-ME 인터페이스를 통해 ME 정보를 통신 및 교환할 수 있다. 예를 들어, 도메인은 부트-업 또는 RTO 프로세스 동안 ME와 통신할 수 있다. THSM-ME 인터페이스를 통해 교환되는 데이터의 보호가 요구될 수 있다.

[0045] THSM-ME 인터페이스를 통한 모든 통신들의 무결성 보호가 요구될 수 있다. 예를 들어, 무결성 보호는 인증된 키 교환 매커니즘들을 이용함으로써 교환되는 사전-준비된 임시 키들 또는 키들과 같은 암호 키들을 이용할 수 있다. 암호 키들은 Ktemp_I과 같이 대칭적, 또는 무결성을 위해 THSM에 의해 이용되는 공개 또는 개인 키들을 위한 Kpub/priv_THSM_temp_I 및 무결성을 위해 ME에 의해 이용되는 공개 또는 개인 키들을 위한 Kpub/priv_ME_temp_I와 같이 비대칭적일 수 있다. 임시 키들은 인터페이스들의 보호를 위해 이용될 수 있다. 예를 들어, 임시 키(temporary key)는 유효 기간과 연관될 수 있거나 또는 한번, 또는 미리 결정된 회수만큼 사용될 수 있다.

[0046] THSM-ME 인터페이스를 통한 통신의 비밀성은 암호 수단을 이용하여 또한 제공될 수 있다. 인증된 키 교환 매커니즘들을 이용함으로써 교환되는 사전-준비된 임시 키들 또는 키들이 이용될 수 있다. 암호 키들은 암호화(ciphering)를 위해 Ktemp_C와 같이 대칭적 또는 암호화를 위해 THSM에 의해 이용되는 공개 또는 개인 키들을 위한 Kpub/priv_THSM_temp_C 및 암호화를 위해 ME에 의해 이용되는 공개 또는 개인 키들을 위한 Kpub/priv_ME_temp_C와 같이 비대칭적일 수 있다. 여기서 기술되는 RTO 방법들 및 장치들은 단순함을 위해 사전-준비된 대칭적 임시 키들의 이용을 참조한다. 그러나 당업자는 다른 키 구현들이 본 출원의 범위를 초과함 없이 이용될 수 있다는 것을 인지할 것이다.

[0047] RO들과 관련하여 THSM-ME 사이에서 보통문으로 전달되는 메시지들에 대한 리플레이 공격(replay attack)들에 대한 방지가 제공될 수 있다. THSM-ME 인터페이스를 통해 송신되는 각각의 메시지는 임시 사용에 있어서 선도 품질(freshness quality)을 보유할 수 있다. 단순함을 위해, 여기서 기술되는 RTO 프로토콜들은 ME-THSM 인터페이스를 통해 교환되는 모든 메시지들의 반-리플레이 보호(anti-replay protection)를 포함할 수 있지만, 당업자는 다른 인터페이스 보호 구성들이 본 출원의 범위를 초과함 없이 이용될 수 있다는 것을 인지할 것이다.

[0048] 서명들이 해시들에 적용될 수 있다. 예를 들어, 해시들은 SHA-X 알고리즘에 의해 생성될 수 있다. 신뢰적인 제 3 자는 인증서($Cert_{TSIM}$), $K_{TSIM-Priv}$ 및 $K_{TSIM-Pub}$와 같이 THSM과 연관된 개인-공개 키 쌍을 이용하여 증명할 수 있다. 신뢰적인 제 3 자는 또한 인증서($Cert_{RO}$), $K_{RO-Priv}$ 및 K_{RO_Pub}와 같이 네트워크와 연관된 키들의 다른 세트를 이용하여 증명할 수 있다. 이 인증서들은 해당 도메인에 배분된 보호 스토리지에 저장될 수 있다.

[0049] 공개 키(K_{RO_Pub})는 RO로부터의 서명을 검증하기 위해 또는 RO에 송신된 메시지를 암호화하기 위해 THSM 플랫폼, 구체적으로 TSIM에 의해 이용될 수 있다. 개인 키($K_{RO-Priv}$)는 사인 목적(signing purpose)들을 위해 그리고 대응하는 공개 키를 이용하여 TSIM에 의해 암호화된 메시지들을 복호화하기 위해 네트워크에 의해 이용될 수 있다. 공개-개인 키 쌍($K_{TSIM-Pub}$ 및 $K_{TSIM-Priv}$)은 TSIM 및 RO의 역할들이 스위치되는 것을 제외하면 유사한 기능들을 가질 수 있다. 대안적으로 RO 및 TSIM 둘 다에서, 암호화 및 사인을 위한 별개의 키 쌍들이 존재할 수 있다.

[0050] 키 쌍들(K_{RO_Priv} 및 K_{RO_Pub} 및 $K_{TSIM-Priv}$ 및 $K_{TSIM-Pub}$)은 소유자, 사용자, 또는 둘 다에 의해 선택된 특정한 네트워크 서비스에 의존할 수 있다. RO와 같은 각각의 서비스 제공자는 해당 제공자와 연관된 THSM 상의 각 도메인에 대한 그 자신의 증명된 공개-개인 키 쌍을 가질 수 있다. 선택된 서비스는 키 쌍들의 세트가 이용되는지를 결정할 수 있다. 예를 들어, 공개 개인 키 쌍들의 세트는 선택된 서비스 제공자 및 THSM 상의 연관된 도메인에 의해 결정될 수 있다. 이용된 키 쌍의 협상이 존재하지 않을 수 있다. 공개 또는 개인 키 쌍은 서비스 제공자에 의해 결정될 수 있고 도메인 또는 THSM 서브시스템과 밀접하게 연관될 수 있다.

[0051] THSM TD_{DO}는 "서브시스템-와이드 도메인 관리자(System-wide Domain Manager)"(SDM)를 구성할 수 있다. SDM은 "서브시스템-와이드 도메인 정책(System-wide Domain Policy)"(SDP)을 포함하는 사전-구성된 파일을 보호 가능하게 저장할 수 있다. SDM은 SDP에 따라 THSM에 대한 RO의 도메인들을 구축 또는 로딩할 수 있다. SDM은 DO의 도메인의 원래의 구성에 포함될 수 있다. SDM은 다른 도메인이 구축되어야 하는지 그리고 어떤 순서로 구축되어야 하는지를 결정하기 위해 사전-구성된 SDP를 이용할 수 있다.

[0052] 대신에 그리고 RO 도메인에 의해 요청될 때, SDM은 THSM 플랫폼 환경 요약(THSM Platform Environment Summary; TPES) 및 THSM 플랫폼 무결성 입증(THSM Platform Integrity Attestation; TPIA)을 준비 및 공급한다. TPES는 THSM의 가장 최근의 "환경"에 관한 요약 정보를 기술할 수 있다. 이러한 정보는 THSM 상에서, 비밀성 및 분리에 관하여 각자의 도메인 정책들에 의해 컨디셔닝 또는 허용되는 도메인들의 수 및 간략한 본질 및 요청 도메인과 기능들 또는 자원들의 통신 및 공유를 위해 이용 가능할 수 있는 THSM 상의 임의의 남은 자원들을 포함할 수 있다. TPIA는 THSM의 도메인들 중 하나 이상의 도메인에 관한 무결성 입증의 콜렉션(collection)을 포함할 수 있다. TPIA는 또한 상기 도메인들을 지원하는 플랫폼에 대한 무결성 입증들을 포함할 수 있다. TPIA는 THSM 상에서 원래의 도메인에 대한 RTO 프로세스를 수행하는데 있어 관심이 있는, RO와 같은 외부 검증기에 관심의 도메인의 신뢰 상태 및 이 도메인들을 지원하는 플랫폼을 입증하는데 이용될 수 있다. RO 또는 RO의 도메인(TD_{RO})은 TPIA를 SDM에 요청할 수 있다. SDM은 SDP에 따라 요청을 들어주거나 거절할 수 있다.

[0053] SDM은 또한 구축되어야 하는 다른 도메인 및 그 순서를 상호작용식으로 식별하기 위해 THSM의, 서비스 요원과 같은 물리적으로 존재하는 디바이스 소유자와 상호작용할 수 있다. 또한, SDM은 구축될 도메인들에 대한 입력 및 구축 순서를 제공하기 위해 THSM의 물리적으로 존재하는 사용자와 상호작용하도록 사용자의 도메인에 요청할 수 있다. 이 정보는 도메인 구축 프로세스에서의 입력으로서 이용될 수 있다.

[0054] THSM이 RO의 도메인에 대한 RTO 프로세스들을 수행할 때, THSM은 원격 소유권-취득 프로토콜의 완료 이전에 4개의 특수한 시스템 상태들을 달성하도록 구성될 수 있다. THSM Pre_Boot 시스템 상태는 THSM이 "전력공급(powered-on)"되지 않는다는 것을 표시할 수 있다. $THSM\_TD_{DM}\_LOAD\_COMPLETE$ 시스템 상태는 THSM의 전력공급 이후에 제 1 단계로서 THSM 상에 DM의 도메인이 구축 또는 로딩된다는 것을 표시할 수 있다. $THSM\_TD_{DO}\_LOAD\_COMPLETE$ 시스템 상태는 DO의 도메인(TD_{DO})이 이용 가능한-마지막-구성(last-configuration-available)으로 구축 또는 로딩되었었다는 것을 표시할 수 있다. 이 "이용 가능한 마지막 구성"은, DO의 도메인이 결코 단독으로 RTO 프로세스를 통과하지 못하는 경우 "원래의" 구성 또는 "포스트-RTO (post-RTO)" 구성일 수 있다. DM의 도메인은 DO의 도메인을 구축 또는 로딩할 수 있다. DO의 도메인이 적어도 하나의 RTO 프로세스를 통과하기 이전에, DO의 도메인은 "원래의" 상태에 있을 수 있고, 어떠한 특정한 DO에 의해서도 청구되거나 소유되지 않을 수 있다. "원래의" 도메인은 "쉘(shell)"을 포함할 수 있다. DO의 도메인이 구축되거나 로딩되는 최초 시간, "이용 가능한 마지막 구성"(여기서부터 마지막-구성으로서 지칭됨)은 사전-구성된 파일에서 비롯될 수 있다. 대안적으로, "마지막 구성"이 RO의 도메인에 대한 RTO 프로세스에 기인한 경우, THSM 상의 특정한 도메인은 적어도 한번 원격 소유권-취득 프로토콜을 통과했을 수 있고, 원격 소유자는 TSS_{RO}의 소유권을 취득할 수 있다. 이는 원격 소유권 취득 완료시에 플랫폼 상에 구성되는 신뢰적인 서브시스템을 표시할 수 있다. 이

상태에 도달하기 이전에 또는 도달할 때, 특정한 RO는 다른 작업들을 수행하기 시작할 수 있다.

[0055] THSM_TD_{RO}_LOAD_COMPLETE 시스템 상태는 RO의 도메인(TD_{RO})이 이용 가능한 마지막 구성으로 구축 또는 로딩되었다는 것을 표시할 수 있다. "이용 가능한 마지막 구성"은 RO의 도메인이 결코 단독으로 RTO 프로세스를 통과하지 못하는 경우 "원래의" 구성일 수 있거나 또는 "포스트-RTO" 구성일 수 있다. DM의 도메인은 RO의 도메인을 구축 또는 로딩할 수 있다. DO의 도메인이 적어도 하나의 RTO 프로세스를 통과하기 이전에, DO의 도메인은 "원래의" 상태에 있을 수 있고, 어떠한 DO에 의해서 청구되거나 소유되지 않을 수 있다. "원래의" 도메인은 "쉘"을 포함할 수 있다. RO의 TD가 구축되거나 로딩되는 최초의 시간, 마지막-구성은 사전-구성된 파일들에서 비롯될 수 있다.

[0056] 대안적으로, 마지막 구성은 RO의 TD에 대한 RTO 프로세스에 기인하는 경우, THSM 상의 특정한 TD는 적어도 한번 RTO 프로토콜을 통과했을 수 있고 RO는 TD_{RO}의 소유권을 취득한다. 이는 RTO 완료시에 플랫폼 상에 구성되는 신뢰적인 서브프레임을 표시한다. 이 상태에 도달하는 시간에, 특정한 RO는 다른 작업들을 수행하기 시작할 수 있다. RO의 TD(TD_{RO})가 MNO의 TD인 경우, 이 단계에 의해, MNO의 TD는 그 TD_{RO} 상에 실현되는 최종 신뢰적인 가입 아이덴티티 관리(eventual Trusted Subscription Identity Management; TSIM) 기능을 제공할 수 있다.

[0057] 대안적으로, 시스템-와이드 도메인 관리자(System-wide Domain Manager; SDM)는 DO의 TD 보단, DM의 TD에 구현될 수 있다. 적절한 인가 데이터를 DM의 TD에 제공한 이후, DO는 THSM 상의 다양한 원격-소유자 TD들을 생성, 로딩 및 다른 방식으로 관리하는 작업을 수행하기 위해 DM의 TD에 의해 제공된 SDM을 이용할 수 있다. 이 경우의 THSM 시스템 부트 시퀀스 및 RTO 프로세스 시퀀스의 상세들은 여기서 기술되는 것과 상이할 수 있지만, 본 출원의 범위 내에 있다. 이 경우에 대한 부트-업 및 RTO 프로세스들은 물론, DO 또는 DO의 TD가 DM의 TD에 의해 제공되는 SDM을 어떻게 이용하는지에 관한 설명, 예를 들어, 어떤 종류의 인가 데이터가 제공될 수 있는지(그리고 그것이 어떻게 제공될 수 있는지)는 여기서 기술된 것과 유사할 수 있다. 예를 들어, 스마트 카드로서 구현되는 THSM은 카드 발행자 대신에, 카드 상에서 보안 도메인들의 관리를 전담하는, 글로벌 플랫폼과 같은 표준들에 의해 특정되는 카드 관리자 기능을 지원하는 기능을 갖는 카드 관리자를 포함할 수 있다. 카드 발행자는 DM과 유사할 수 있고, 카드 관리자는 SDM의 기능 중 일부를 포함할 수 있다. 그러므로, 카드 관리자는 DM의 도메인에 보유되는 SDM과 유사할 수 있다.

[0058] 제 1 실시예에서, ME는 안전한 부트 성능들을 제공하도록 구성될 수 있고, THSM은 완전한 MTM 성능들을 제공하도록 구성될 수 있다. 전력 공급시에, ME는 안전하게 부트할 수 있다. 예를 들어, ME는 오픈 모바일 단말 플랫폼(open mobile terminal platform; OMTP) 신뢰적인 실행 환경 TRO 규격에 따라 비-TCG "안전한" 부팅을 수행할 수 있다. 부트 시간에, THSM은 먼저 예를 들어, 부팅-업(booting-up)함으로써 THSM DM의 도메인(TD_{DM})을 구축하고 그 후 "원래의" THSM DO의 도메인(TD_{DO})을 구축할 수 있다. DO 및 DU가 분리된 경우, THSM은 또한 THSM DU의 도메인을 구축할 수 있다.

[0059] THSM TD_{DM}은 초기에 THSM에서 보호되고 부트 시간에 이용 가능하게 되는 사전-구성된 파일로 구축될 수 있다. THSM TD_{DO}는 주로 사전-구성된 파일들로 구축될 수 있지만, RTO 프로세스를 이용해서도 구축될 수 있다. THSM TD_{DO}는 RTO 프로토콜을 통과할 수 있다. 이 프로토콜은 RO의 도메인(TD_{RO})에 대한 RTO 프로토콜과 동일한 형태를 취할 수 있거나, 상이한 프로토콜일 수 있다. THSM TE_{DO}는 RTO 프로토콜을 통과하지 않는 경우, 소유권을 취득하는데 요구되는 크리덴셜들이 사전-구성되고 사전-준비된다. THSM TE_{DO}는 DO에 의해 소유될 수 있다. DO는 실제 인간 사용자 또는 소유자, 기업체와 같은 조직, 또는 조직의 정보 기술(Information Technology; IT) 부서 또는 원격 네트워크 운용자(Network Operator; NO)일 수 있다.

[0060] THSM TD_U는 THSM TE_{DO}에서 미리 준비되는 사전-구성된 파일로 구축될 수 있다. THSM의 RO 도메인은 THSM DO의 시스템-와이드 도메인 정책(SDP)에 따라 "원래의" 구성으로 먼저 구축될 수 있다. THSM의 RO 도메인은 RO와의 RTO 프로세스를 통과할 수 있다. DO의 도메인의 SDM은 SDP에 따라 RO의 도메인의 RTO 프로세스를 관리할 수 있다. THSM의 RO가 MNO이어서 RO의 도메인이 MNO의 도메인인 경우, 이러한 MNO의 도메인은 또한, i) MNO의 도메인이 MNO에 등록되는 방법; ii) 가입 크리덴셜들(예를 들어, USIM 또는 MCIM 비밀 키(Ki)들 및 국제 모바일 가입자 아이덴티티(International Mobile Subscriber Identity; IMSI) 등)이 MNO의 모바일 네트워크로부터 THSM 상의 MNO의 도메인으로 롤 오프(rolled off)되고 그 후 거기서 준비되는 방법; 및 iii) 일단 가입 크리덴셜들이 다운로딩되며, 이러한 크리덴셜들을 처리하거나 이용하는 기능, 또는 심지어 가입 관리 기능을 제공하는 도메인

이 하나의 디바이스로부터 다른 디바이스로 이주(migrate)될 수 있는 방법을 정의하는 프로토콜을 통과할 수 있다. 이러한 프로토콜들은 i) 등록 프로토콜; ii) 크리덴셜 롤-오프 프로토콜; 및 3) 이주 프로토콜로서 각각 지칭될 수 있다. THSM의 RO 도메인은 RTO가 완료된 이후 그 자신의 구성을 입증하여 RO에 리포트할 수 있다.

[0061] ME의 신뢰-구축 매커니즘이 시동 시간 안전한 부트 프로세스(power-up time secure boot process)의 수행으로 제한될 수 있는 제 1 실시예에서, ME 구성은 ME 또는 THSM에 의해 추가로 입증 가능하지 않을 수 있다. 대안적으로, ME는 자체-무결성 검사를 수행하고, 안전한 부트를 완료한 것으로서 무결성 값(integrity value; IV)을 생성할 수 있다. ME는 OTA(over the air) 방법을 이용하여 UMTS 보안 모드 특징들과 같은 보안 모드 특징들에 따라 비밀성 및 무결성 보호용 엔진(engine)과 같은 소프트웨어를 설치할 수 있다. 선택적으로, RO의 도메인의 소유권이 RO와의 RTO 프로세스를 통해 취득될 때, RO는 다운로드 또는 다른 방식으로 입수(import)되고 그 다음 RTO 프로세스가 완료되는 것을 허용하기 위해 수락할 수 있는 THSM의 조건들에 관한 그 자신의 정책을 어써트(assert)한다. RO들은 RO가 전반적인 THSM의 조건들, THSM의 다른 도메인들의 구축 구조(building structure)의 조건들 또는 둘 다에 동의할 때 THSM 플랫폼 상에 자신을 위한 도메인을 "게이트-킵(gate-keep)" 설치하도록 구성될 수 있다. 따라서, RTO 프로세스의 부분으로서, RO는 DO의 조건들 또는 "도메인-구축 계획들(domain-building plans)"을 식별하기 위해 DO의 도메인들의 SDM과 일부 정보를 교환하고, 이러한 조건이 RO에 수용 가능한 경우에 RTO 프로세스가 완료되는 것을 허용할 수 있다. RO 도메인은 또한 권리들을 가질 수 있고, 초기에 THSM 상의 그의 RTO-완료된 RO의 도메인을 구축하도록 동의한 이후에 THSM의 조건 또는 도메인 구축 계획의 임의의 변경이 통지되거나, 또는 임의의 변경이 업데이트되는 것을 허용하기 위해 이러한 권리들을 시행하기 위한 기능을 수행하도록 구성될 수 있다. RO의 도메인-특정 정책(DP)은 RO의 도메인이 통지되도록 요구될 수 있는 변경들의 타입을 특정할 수 있다.

[0062] SDM은 의도된 RO와 연관된 RO 도메인을 위한 RTO 프로세스를 개시할 수 있다. 이는 RO의 도메인이 "원래의," 미청구(unclaim)" 상태에 있을 때 발생할 수 있다. 예를 들어, RO의 도메인은 DO의 도메인 및 DO에 의해 "도메인 X"(TD_X)라 칭해질 수 있다. 도메인은 아직까지-미청구 쉘(as-yet-unclaimed shell) 또는 "원래의" 조건에서 생성될 수 있다. 이러한 경우, SDM은 RTO 프로세스를 개시할 수 있고, 그에 의해 SDM은 도메인 TD_X 대신, 의도된 RO와 접촉하게 된다. 일단 RO가 이 도메인에 대한 RTO 프로세스를 통과하면, SDM은 이 동일한 도메인에 대해 다른 RTO 프로세스를 더 이상 개시하지 않을 수 있다. 대신, RO는 이 특정한 도메인 상에서 다른 종류의 소유권-취득 프로세스를 스스로 개시할 수 있다. 이러한 소유권-취득 프로세스는 전자(former)가 (가능하게는 SDM 또는 DO의 도메인의 조절 하에서) 디바이스의 소유자/사용자 또는 디바이스 스스로에 의해 국부적으로 개시되기 보단 원격 소유자에 의해 원격으로 개시될 수 있다는 점에서 지금까지 특정된 RTO 프로세스와 상이할 수 있다. DO는 RO의 도메인이 RTO 프로세스를 통과하고, 이에 따라 적절한 RO에 의해 "청구" 또는 "소유"된 이후 조차도, 임의의 RO의 도메인을 삭제, 파괴, 또는 연결해제하기 위한 권한(authority)을 보유할 수 있다. 그러나, DO는 일반적으로 RO의 도메인 내에 저장된 비밀(secret)들을 알거나, 또는 RO의 도메인 내에서 수행되는 중간의 계산들 또는 기능들을 알지 못할 수 있다.

[0063] SDM이 원래의 RO의 도메인에 대한 RTO 프로세스를 개시하기 이전에, SDM은 도메인 구축을 위해 이용 가능한 자원들의 리스트를 룩업(look up)할 수 있다. 이 리스트는 DM의 도메인에 의해 보유될 수 있다. SDM은 "원하는 도메인(desired domain)들" 리스트를 또한 룩업할 수 있다. 원하는 도메인들 리스트는 DO의 도메인 TD_{DO}에 보유될 수 있다. SDM은 또한 시스템 도메인 정책(SDP), 및 DM의 도메인으로부터의 질의를 위해 이용 가능하게 될 수 있는, 플랫폼의 그리고 THSM의 기존의 도메인들의 현재 상태(신뢰 상태들을 포함)를 룩업할 수 있다. 이 정보는 특정한 RO의 도메인에 대한 원하는 RTO 프로세스가 이용 가능한 자원들, 정책 하에서 가능한지, 원하는 도메인 리스트 하에서 요구되는지, 예를 들어, THSM의 기존의 도메인들의 신뢰 상태와 같은 상태 하에서 허용되는지를 결정하기 위해 이용될 수 있다.

[0064] 대안적으로, 원격 소유자의 도메인(TD_{RO})은 스스로 RTO 프로세스를 시작하고 관리할 수 있다. TD_{RO}는 RTO 프로세스 이전에 미청구되고 "원래의" 상태에 있을 수 있다. "원래의" RO의 도메인(TD_{RO})은 부트 업시에 그의 의도된 RO에 접촉하고 RTO 프로세스를 자율적으로 시작하는 것을 가능하게 하는 사전-구성된 기능을 포함할 수 있다. 선택적으로, RTO 프로세스는 THSM의 소유자 또는 사용자가 TD_{RO} 프롬프트(prompt)들을 획득한 이후 시작되고, 그 후 RTO 프로세스를 개시하기 위해 THSM의 소유자 또는 사용자로부터 "nod"를 획득할 수 있다. (타겟) 원격 소유자 RO_target에 의해 소유되도록 생성되고 의도되었지만, RTO 프로세스를 통해 아직 소유되지 않고 여

전히 "원래의" 상태에 있는 도메인 TD는 이하 TD_{RO_target} *라 지칭될 수 있다.

[0065] 다른 대안으로, TD_{RO}는 특정한 RO와의 적어도 하나의 RTO 프로세스를 통과할 수 있고, TD_{RO}는 현재 RO에 의해 "청구" 또는 "소유"될 수 있다. DO 또는 도메인 TD_{DO}와 같은 THSM 상의 그의 프록시든지 간에 무엇이든 RO의 정책 및/또는 SDM의 정책에 의존하여 동일한 RO의 도메인에 대해 다른 RTO 프로세스를 시작하도록 허용될 수 있다. SDM은 RTO의 목적들을 조사할 수 있고 그의 정책 구조 내의 허용 가능한 목적들 또는 활동들에 기초하여, 이러한 새로운 RTO가 진행되는 것을 허용할지를 결정할 수 있다. 원격 시그널링을 통해 RO 또는 RO의 도메인(TD_{RO})은 동일한 RO와 더불어 도메인에 대해 다른 RTO 프로세스를 개시할 수 있다. 이는 RO가 TD_{RO} 내의 구성 파일들, 보안 정책들, 또는 실행 가능한 코드를 업에이트하도록 요구할 때 발생할 수 있다. RO는 업데이트들을 다운로드할 수 있다. 업데이트들은 비-RTO를 통해, OTA(over the air) 업데이트 프로세스를 통해 행해질 수 있다. 그러나, 몇몇 경우들에서, RO 또는 TD_{RO}는 일부 파일들 또는 코드를 업데이트하기 위해 다른 RTO 프로세스를 이용할 수 있다.

[0066] "원래의" TD_{RO}가 단독으로 RTO 프로세스를 개시할 때, 그것은 DM의 도메인에 의해 보유될 수 있는, 도메인 구축을 위한 이용 가능한 자원들의 리스트를 룩업하기 위해 SDM에 의존하도록 요구될 수 있다. TD_{RO}는 또한 DO의 도메인에 의해 보유될 수 있는 "원하는 도메인들" 리스트, 시스템 도메인 정책(SDP), 및 DM의 도메인으로부터의 질의에 대해 이용 가능할 수 있는, THSM의 기존의 도메인들의 현재 상태(신뢰 상태들을 포함함)를 룩업하기 위해 SDM에 또한 의존할 수 있다. 이 정보는 특정한 RO의 도메인에 대한 원하는 RTO 프로세스가 이용 가능한 자원들, 정책 하에서 가능한지, 원하는 도메인 리스트 하에서 요구되는지, 및 THSM의 기존의 도메인들의 상태 또는 신뢰 상태 하에서 허용되는지를 결정하는데 이용될 수 있다.

[0067] SDM 정책은 DO에 대한 소유권-취득(TO) 프로세스 동안 구성될 수 있다. 이 프로세스는 부트 프로세스 동안 시행되는 사전-존재하는 구성 구조를 통해 국지적으로 발생할 수 있다. DO의 TO는 또한 원격적으로 발생할 수 있는데, 이 프로세스는 비-디바이스-소유자 원격 소유자(non-device-owner remote owner)에 대한 RTO 프로세스의 경우에서와 달리 DO의 도메인에 대한 TO 프로세스의 경우에 RTO의 차단 또는 허용에 대한 SDM 조사가 발동(invoke)되지 않을 수 있다는 것을 제외하면, 여기서 특정된 바와 같이 디바이스 소유자의 도메인들이 아닌 도메인들의 소유권-취득에 사용하도록 의도되는 RTO 프로세스와 유사할 수 있다. SDP는 국지적으로(DO가 물리적으로 존재하고 디바이스와 상호작용함), 또는 원격적으로 위치된 디바이스 소유자와의 원격 상호작용을 포함하는 방식으로 수행될 수 있는 DO 소유권-취득 프로세스 동안에 설정될 수 있다. SDP의 컴포넌트는 모든 비-DO 도메인들에 공통적인 허용 가능한 활동들 또는 목적들의 리스트이다. 이는 또한 도메인들의 소유권 취득이 허용되지 않는 원격 소유자들을 특정하는 부가적인 엔트리들을 포함할 수 있다.

[0068] 제 2 실시예에 따라, ME는 안전한 부트 성능들을 가질 수 있고 그의 부트 코드 중 일부 코드의 "안전한 부트" 검사 중 일부를 수행하기 위해 THSM에 의존할 수 있다. ME는 OMTP TRO 안전한 부트와 같은 비-TCH 안전한 부트를 수행할 수 있다. THSM은 THSM에 제공되는 물리적인 보호를 "활용"하도록 ME의 무결성을 검사하는데 이용될 수 있다. 예를 들어, ME는 THSM에 원(raw) 데이터를 송신하고, THSM은 ME의 무결성을 검사할 수 있다. WTRU는 ME와 THSM 사이에서 안전한 채널 및 안전한 방식으로 THSM에 코드 또는 데이터를 송신하고 THSM이 ME에 대한 무결성 검사를 실행하기 위해 예를 들어, 안전한 채널을 통해 THSM과 안전하게 통신하도록 적어도 신뢰적일 수 있는 ME의 "다소 신뢰할 수 있는" 부분을 제공하기 위한 매커니즘을 구현할 수 있다. THSM은 또한 ME 대신 ME의 코드 중 일부를 그 자신 내에 저장할 수 있다. 이 코드들은 부트 프로세스 동안 ME에 로딩될 수 있다. 그 자신과 ME 사이에서 THSM은 그의 하드웨어-기반 보호 매커니즘에 기인하여 더욱 신뢰할 수 있는 환경일 수 있기 때문에, THSM은 ME의 무결성 검사를 수행하고 ME에 대한 코드들 중 일부를 저장 및 로딩하는 역할을 수행할 수 있다.

[0069] 제 3 실시예에서, THSM은 ME의 코드에 대한 안전한-부트 또는 무결성-검사 중 일부를 수행할 수 있다. 이는 RO에 대해서 입증될 수 있다. ME는 단일의 신뢰적인 엔티티; 모바일 신뢰 환경(Mobile Trusted Environment; MTE)을 포함할 수 있다. MTE는 ME 내의 국지적으로 별개의 환경일 수 있으며, MTE는 잔여 ME 보다 더욱 신뢰된다. MTE는 하드웨어 기반 신뢰 루트(hardware based roots of trust; RoT)들과 같은 몇몇의 하드웨어 기반 보호 매커니즘을 활용할 수 있다. ME의 베이스 코드(base code)가 로딩된 이후, MTE는 로딩될 수 있다. MTE는 신뢰적인 사인 키(trusted signing key)의 이용과 같이 신뢰의 증명을 외부 검증자에게 제공한다는 점에서 신뢰적인 엔티티일 수 있다. MTE가 신뢰적인 엔티티일지라도, MTE는 실제 TPM과 연관된 측정 프로그램 코드인 측정용 신뢰 코어 루트를 소유하지 않을 수 있다. 전력공급되는 디바이스와 같은 ME가 THSM이 동작할 수 있는 "플

랫폼"을 제공하는 한, ME는 ME 플랫폼으로서 여기서 지칭될 수 있다. MTE는 ME 플랫폼의 무결성의 증거를 수집하고, 적어도 MTE 내에서 보호되는 사인 키의 이용에 의해 제공되는 무결성 보호 하에서 포스트-루트 SDM과 같은 THSM 내의 신뢰적인 엔티티에 이 증거를 포워딩하도록 구성될 수 있다. THSM은 TCH TPM 또는 MTM-유형의 무결성 특정 및 검증 기능을 구현하기 때문에, THSM은 '확장(Extend)' 동작을 수행하기 위한 TCG TPM 또는 MTM의 성능을 또한 구현할 수 있고, 그럼으로써, 현재 소프트웨어의 측정들은 PCR들에 대한 새로운 값들을 계산하기 위해 소프트웨어의 로딩의 이력 상태를 표시하는 플랫폼 구성 레지스터(Platform Configuration Register; PCR)들의 현재 값들과 조합된다. THSM은 또한 다이제스트 값들(소프트웨어 컴포넌트들의 무결성의 원 측정 값들일 수 있음) 또는 PCR들의 값들을, THSM에 대한 ME 플랫폼의 신뢰성(trustworthiness)의 입증을 위해 이용될 수 있는 다른 무결성 데이터로 변환하기 위한 매커니즘을 구현한다. 단순함을 위해, ME 플랫폼 무결성의 수집 데이터는 이하 ME 플랫폼 무결성 데이터(ME Platform Integrity Data; MPID)로 표시될 수 있다. THSM은 ME 또는 MTE에 대한 도메인을 유지하지 않을 수 있다. THSM은 사전-구성된 파일로부터 또는 DM과의 실시간 접촉에 의해 THSM이 계산된 다이제스트를 검사하는 증명 메트릭(certified metric)을 획득할 수 있을 수 있다. ME의 입증이 이어질 수 있으며, 매칭이 결정되는 것을 제공한다. MTE는 또한 모델 번호들과 같은 ME의 "환경", MTE가 어떤 종류의 서비스들을 수행하기 위해 의도되었는지 및 누구를 위한 것인지를 기술하는 데이터를 수집할 수 있을 수 있다. 단순함을 위해, 이러한 ME의 환경 설명은 이하에 ME 플랫폼 환경 서베이(ME Platform Environment Survey; MPES)로 표시될 수 있다. THSM DO의 RO는 그 자신의 도메인은 물론 ME의 플랫폼의 무결성을 입증할 수 있다. 이러한 입증은 PCT 특허 출원 WO 2009/092115 (PCT/US2009/031603)에서 특정된 것과 같이, M2M 문맥에서 신뢰적인 환경(TRE)의 M2ME 확인 기능과 유사할 수 있다. ME는 THSM으로부터의 요청 시에 또는 스스로, 그의 변하는 상태들을 THSM에 연속적으로 리포트할 수 있다.

[0070] 제 4 실시예에서, ME와 THSM 둘 다는 완전한 MTM 기능을 수행하도록 구성될 수 있다. ME 또는 그의 도메인의 신뢰성은 ME에 의해 또는 도메인에 의해 직접 입증 가능할 수 있다. ME의 DO 도메인은 연속적으로, 또는 요청 당 원칙(basis)으로 RO에 그의 상태들을 리포트할 수 있다. THSM의 RO 도메인은 유사하게 기능할 수 있다. ME의 RO 도메인 및 THSM의 RO 도메인에 의한 리포트들은 동기화될 수 있고, 서로 묶여질 수도 있다. 리포트들은 또한 프로토콜 흐름의 공통 세션을 이용하여 형성될 수 있다.

[0071] 이 실시예에서, ME는 여기서 기술되는 바와 같은 THSM의 몇 개의 기능들을 수행하도록 구성될 수 있다. ME는 그 자신의 하나 이상의 도메인들을 포함할 수 있으며, 각각은 특정한 소유자에 대한 것이다. 이 도메인들은 THSM에 따라 신뢰적인 엔티티들의 특성들을 포함할 수 있다. 이러한 도메인들은 디바이스 제조자(DM) 도메인 및 사용자(U) 도메인을 포함할 수 있다. 이 도메인들은 THSM과 유사한 방식으로 사전-구성될 수 있다. THSM 상의 도메인들로부터 ME 상의 도메인들을 구분하기 위해, 글자 ME는 도메인 자체를 지정하는 글자들이 아래첨자로 기입될 수 있다. 따라서, DM에 대한 도메인은 ME_{DM}으로 표시될 수 있다. THSM 상의 디바이스 소유자(DO) 도메인은 SDM 내에 상주하는 시스템-와이드 도메인 정책(SDP)에 대한 순응(conformance)을 보장하기 위해 ME 측 상에서 도메인을 모니터링할 수 있다. ME의 각각의 도메인의 생성에 있어서, SDM과의 통신은 THSM이 각각의 새로운 도메인 구성을 인지하게 할 수 있다.

[0072] ME는 THSM의 SDM의 것과 유사한 방식으로 기능할 수 있는 플랫폼 도메인 관리자(platform domain manager; ME_{PDM})로서 지칭될 수 있는 도메인 관리자를 포함할 수 있다. ME_{PDM}은 ME_{DM}에 상주할 수 있고, 초기에 DM에 의해 정의되는 바와 같은 사전-구성을 가질 수 있다. 초기 구성은 그 목적 및 기능면에서 THSM 상의 TD_{DM}의 초기의 사전-구성된 정의의 목적 및 구성과 유사할 수 있다. ME_{DM} 셋업은 TD_{DO}가 THSM에서 예시된 이후 발생하도록 타이밍이 정해질 수 있다. SDM은 ME_{DM}에 대한 셋업이 완료되었음을 통지받으면, SDM은 시스템-와이드 제약들에 의존하여, SDP의 반향(reflection) 내의 또는 반향으로부터 발생하는 정책 제한들을 부과할 수 있다. SDM은 다수의 원격 소유자들 및 THSM 상의 그들의 도메인들의 리스트를 유지할 수 있다. 리스트 내의 소유자들 중 하나에 속하는 ME 상에서 도메인이 생성되고 관리되는 경우, SDM은 ME 상에서의 이들의 도메인들의 생성 및 관리에 대한 특정한 제어를 가질 수 있다.

[0073] 이러한 방식으로, ME는 완전한 MTM 기능을 가질 수 있다. 따라서, ME는 측정을 위한 신뢰 코어 루트(core root of trust for measurement; CRTM), 리포팅을 위한 신뢰 코어 루트(core root of trust for reporting; CRTR), 및 저장을 위한 신뢰 코어 루트(core root of trust for storage; CRTS)를 포함할 수 있다. THSM 상에서, 도메인 가입 기능은 TSIM 기능에 의해 관리될 수 있다. THSM내의 하나 및 ME 상의 다른 하나와 같은 2개의 도메인들이 동일한 RO를 위한 것인 경우, THSM 상의 도메인은 가입 기능 및 해당 원격 소유자에 대한 그의 관리와 같이 매우 높은 보안 및/또는 신뢰 레벨을 요구하는 RO에 대한 기능들 또는 서비스들을 위해 이용될 수 있는 반

면에, ME 상의 도메인은 THSM 상의 도메인으로부터 기대되는 기능들 및 서비스들 위해 요구되는 레벨과 동일하지 않지만 특정한 보안 또는 신뢰 레벨을 여전히 요구할 수 있는 동일한 RO에 대한 기능들 및 서비스들을 위해 이용될 수 있다. 사전-구성된 파일들로부터 구축되지 않는 도메인들은 원격 소유권 취득(RTO) 프로세스를 통해 구성될 수 있다. ME에 대한, 통상적인 원격 소유자(RO)에 대한 RTO는 THSM에 대한 RTO와 유사할 수 있다.

[0074] ME 상의 도메인들은 원격 소유자들에 대한 가입 관리를 위해 이용되도록 의도되지 않는다. 대신, 이들은 사용자, 소유자, 원격 소유자, 또는 이들의 임의의 조합의 이익을 위해 계산 및 자원-집약적인 작업들을 수행하기 위해 이용되도록 의도될 수 있다. 예를 들어, 이 도메인들은 THSM 상의 상대적으로 제한된 자원들에 대해서 실행 가능하지 않을 수 있는 작업들을 수행할 수 있다. ME 상의 도메인들은 일단 생성되고 명시적으로 삭제될 때까지 ME 내에 머무르는 대신, 이 도메인들은 가상화(virtualization)와 비슷하게, 부트 시에 또는 심지어 실시간 세션들 동안 생성되고 그들의 특정한 목적들을 위해, 임시로, 세션-기반 원칙으로 이용될 수 있다는 점에서 보다 "순간적(ephemeral)" 또는 "임시적"일 수 있다. ME 상의 도메인의 원격 소유자는 다른 원격 소유자들에 의해 소유되는 ME 상의 다른 도메인들 또는 THSM 상의 이러한 다른 도메인들의 자원들의 할당 및 그 목적의 입증된 서베이(attested survey)를 요청하고 획득하는 견지에서 동일한 레벨의 특권을 갖지 않을 수 있다.

[0075] 제한들 없이 모바일 네트워크 운용자의 임의의 선택을 허용하기 위해 MNO 원격 소유자로도 알려진 특정한 PLMN에 의해 개시되고 사전-할당되지 않는 "블랭크(blank)" WTRU를 구매하기 위한 모바일 신뢰적인 플랫폼(mobile trusted platform)의 디바이스 소유자를 위한 방법을 제공하는 것이 유리하다. 방법은 RTO 프로세스와 같이, UMTS 디바이스(UE)와 같은 WTRU의 소유권-취득 프로세스를 수행하는 것을 포함할 수 있으며, 여기서 원격 소유자는 PLMN 운용자, 또는 가입 애플리케이션이 의도되는 다른 유사한 운용자이고, THSM 내부의 도메인이고 정확한 RO에 의해 청구될 수 있는 RO의 도메인과 같은 서브시스템을 셋업, 고객맞춤 및 마무리한다.

[0076] 앞서 언급한 바와 같이, 신뢰적인 하드웨어 가입 모듈(THSM)은 IMS 가입 아이덴티티 모듈(ISIM)과 같이, PLMN 운용자들에 대한 가입 애플리케이션을 위한 기능을 포함하는 탬퍼-저항성 하드웨어 컴포넌트 모듈(tamper-resistant hardware component module)로서 구축될 수 있거나, 또는 그 내에 포함할 수 있다. THSM은 WTRU로부터 제거가능하거나 제거가능하지 않을 수 있다. 글로벌 플랫폼 표준들에 순응하는 UICC 또는 스마트 카드의 강화된 버전은 이러한 THSM의 일 실시예일 수 있다.

[0077] 소유권-취득 동작은 운용자 또는 PLMN과 WTRU 간의 기본적인 "신뢰" 관계를 구축한다. 이 절차는 일반적인 "신뢰적인" 소프트웨어 구성과 더불어 "원래의" 엔진을 포함하는 "블랭크 신뢰적인(blank trusted)" TSIM을 설치 및 예시할 수 있다. 이 서브시스템은 플랫폼이 그의 "원래의" 구성 및 보안 속성들의 증거를 제공할 수 있는 경우 원격 소유자에 의해 "증명"될 수 있다. 도 3 및 도 3a는 구체적으로 여기서 기술된 제 1 실시예와 관련되는 이러한 프로세스의 예를 예시한다. 원격 소유자는 요청된 서비스를 사용자에게 제공하고, 적절한 보안 정책을 셋업하고, 서비스와 일관되는 디바이스 구성을 시행하는 모바일 네트워크일 수 있다. 이 프로토콜에 대한 소유자는 국지적일 수 있다.

[0078] 도 3 및 3a는 예시적인 부트업 및 RTO 프로세스를 예시한다. ME는 사전-부트 상태(304)를 가질 수 있다. 디바이스는 블록(306)에서 전력 공급될 수 있다. ME는 블록(308)에서 "안전한" 부트(비-TCG)를 수행할 수 있다. ME는 블록(310)에서 베이스 코드 부트된 상태에 도달할 수 있다. 또한, ME는 블록(312)에서 "베이스 부트 완료" 신호를 THSM에 송신할 수 있다. ME는 블록(314)에서 기본 구성 당 부가적인 소프트웨어를 로딩할 수 있다. ME는 블록(316)에서 부트 완료된(애플리케이션-로딩된) 상태일 수 있다. ME는 블록(318)에서 부트 완료된 메시지를 THSM에 송신할 수 있다.

[0079] THSM은 블록(330)에서 사전-부트 상태에 있을 수 있다. THSM은 블록(334)에서 TE_{DM}을 로딩할 수 있다. THSM은 구성 동안 사전-구성된 파일들을 수신할 수 있는데, 예를 들어, 블록(336)은 사전-구성된 파일들의 사용을 예시한다. 블록(338)에서, THSM은 "TD_{DM} 구축" 상태(기본적인 구성 상태)에 도달할 수 있다. THSM은 예를 들어, 블록(340)에서 예시되는 바와 같이 RO 도메인들에 대해 이용 가능한 자원들에 관한 DM의 규격을 수신할 수 있다.

[0080] 블록(342)에서, TD_{DM}은 TD_{DO}(TD_{DO}는 SDM은 포함할 수 있음)를 구축할 수 있다. 블록(344)에서 THSM은 예를 들어, (이전의 RTO들로 인해 이용 가능할 수 있는) 도메인들을 구축하기 위해 보관된 스테이트먼트 구성 파일(saved statement configuration file)들을 이용할 수 있다. 블록(346)에서, THSM은 TD_{DO} 구축 상태(SDM을 포함)에 도달할 수 있으며, 여기서 TD_{DO}는 DO에 의해 미청구 또는 청구될 수 있다. 블록(350)에서, TD_{DO}는 TD_{U}를 구축할 수

있다. 블록(352)에서, 입력은 DO로부터 수신될 수 있다. 블록(354)에서, THSM은 TD_U 구축 상태에 도달할 수 있으며, 여기서 TD_U는 청구되거나 미청구될 수 있다. 블록(356)에서, THSM은 DO 또는 DU로부터 (예를 들어, 파일 또는 상호작용에 의해 DO가 구축하고자 하는 도메인이 어떤 것인지를 특정하는) 입력을 수신할 수 있다. 블록(358)에서, TD_{DO}는 RO 도메인들, TD_{RO}들을 구축할 수 있다.

[0081] 이제 도 3a를 참조하면, 블록(362)에서, THSM은 TD_{RO}가 구축된 상태에 도달할 수 있으며, 여기서 TD_{RO}는 RO에 의해 청구되거나 미청구될 수 있다. 블록(366)에서, SDM은 RTO를 수행하도록 TD_{RO}에 요청할 수 있거나, 또는 TD_{RO}는 TD_{RO}가 RTO를 수행할 것임을 SDM에 통지(또는 요청)할 수 있다. 블록(370)에서, TD_{RO}는 RTO 프로세스를 시작할 수 있다. 블록(380)에서, 대표적인 원격 소유자들($RO_1,...,RO_n$)이 존재한다. 블록(384)에서, 정보가 교환될 수 있다. 예를 들어, 원격 소유자와의 RTO 프로세스의 부분으로서, 교환된 정보는: 입증들, 구성들, 정책들, 목적들, 증명서(여기서 CERT로서 지칭됨), 키(key)들 및 TD_{RO}들에 대한 SP 중 하나 이상을 포함할 수 있다. 선택적으로, RO는 RTO 프로세스 동안 DO의 '환경' 또는 '도메인 계획'을 밝혀낼 수 있고, 그것이 환경/계획에 동의하는 경우 프로세스가 지속되는 것을 허용할 수 있다.

[0082] 블록(372)에서, THSM은 다양한 도메인들을 위한 시스템 구성을 포착/업데이트하고, 정보를 보관하고, THSM내의 비-휘발성 보호 메모리에 이 정보를 저장할 수 있다. 블록(374)에서, THSM은 포스트-RTO TD_{RO}들을 갖는 상태에 도달할 수 있다.

[0083] 제 1 실시예를 참조하면, DO의 RTO에 의해 형성되는 정책 도메인은 후속 RTO 프로세스들의 도메인 구성들에 영향을 미치는 조항(stipulation)을 포함할 수 있다. RTO 프로토콜은 비-DO RO에 대해 적절할 수 있다. 도메인-특정 정책(domain-specific policy; DP)은 RTO 트랜잭션(transaction) 동안 다운로딩될 수 있다. DO에 대한 DP는 이러한 DP(DP_{DO})가 THSM에서 원격으로 소유될 수 있는 다른 도메인들을 구축 및 유지하기 위해 이용하도록 의도되는 시스템-와이드 도메인 정책(SDP)을 포함할 수 있다는 점에서, RO에 대한 DP와 상이할 수 있다. RTO 프로세스 동안 또는 그 이전에, 도메인의 RO는 신뢰적인 제 3 자(TTP)로부터, THSM의 모든 도메인들의 서브셋 또는 모두를 지원하는 하드웨어 또는 소프트웨어의 현재 무결성 상태 및 구성에 대한 기준 무결성 메트릭(RIM_{RO})을 획득할 수 있으며, 다음과 같이 표현될 수 있다:

수학식 1

$$\text{TTP} \rightarrow \text{RO: } RIM_{RO} = \{\text{THSM의 도메인들을 지원하는 HW/SW의 구성 및 상태, 및/또는 다이제스트 값들}\}$$

[0084]

[0085] 몇몇 경우들에서, TTP는 도메인들을 포함해서, RO가 검증하는데 관심이 있는 THSM의 HW 및 SW의 서브셋에 대한 RIM_{RO}를 제공할 있게 될 수 있다. 2개 이상의 TTP는 RIM_{ROS}를 제공하도록 요구될 수 있으며, RO는 집합적 기준 메트릭을 수집 및 형성한다. RTO 프로세스를 경험하는 THSM의 타겟 도메인(TD_{RO_target})은 THSM의 SDM의 도움으로, 그의 RO에 사인된 THSM 플랫폼 무결성 입증(THSM Platform Integrity Attestation; TPIA)을 제공하도록 구성될 수 있다. TPIA는 THSM 상의 도메인들의 개별적인 무결성 입증들의 연계(concatenation) 및/또는 TD_{RO_target}과의 RTO 프로세스의 완료를 허용하기 이전에 타겟 도메인의 RO가 검증하는데 관심이 있는 디바이스의 플랫폼의 무결성 입증일 수 있다. THSM의 타겟 도메인(TD_{RO_target})은 THSM의 SDM의 도움으로, 사인된 THSM 플랫폼 환경 요약(THSM Platform Environment Summary; TPES)을 그의 RO에 제공할 수 있게 될 수 있다. TPES는 THSM 상의 다른 도메인들의 수 및 본질 및 THSM의 플랫폼의 자원들과 같이 $TE_{RO-target}$의 이익을 위해 이용될 수 있는 임의의 잔여 이용 가능한 자원들을 포함해서, THSM의 환경의 요약을 포함할 수 있으며, 다음과 같이 표현될 수 있다:

수학식 2

[0086] $$TD_{RO\_target} \rightarrow RO: \quad [TPIA]_{signed} \| [TPES]_{signed}$$

[0087] 대안적으로, 관심의 모든 도메인들에 대한 모든 입증들을 포함할 수 있는 TPIA를 RO에 리포트하는 대신, SDM은 모든 이러한 도메인들의 무결성을 검사하고 그들이 신뢰할 수 있다고 간주된다는 사인된 스테이트먼트(반-자율적인 스테이트먼트일 수 있음)를 제공할 수 있다. 이 입증은 도메인들의 콜렉션의 무결성의 국지적 검증을 포함할 수 있다. 국지적 검증기는 THSM 상의 각각의 도메인에 대한 유효한 구성 리스트를 포함할 수 있다. SDM은 AIK에 의해 사인될 수 있는 TPIA를 국지적 검증기에 제공할 수 있다. 개별적인 무결성 입증들의 검증은 그들이 구성 리스트 내의 대응하는 국지적으로 저장된 엔트리들과 매칭한다는 것을 요구할 수 있다. SDM은 무결성 측정들, 로깅(logging) 및 각각의 도메인의 신뢰성을 증명하고 TPIA를 구성하는데 필요한 PCR들에 대한 확장들을 수행할 수 있다. 이 측정들 및 그들의 확장들은 요구되는 도메인들에 대한 입증이 발생했다는 것을 설정하기 위해 검증기에 의해 이용될 수 있다.

[0088] 검증이 달성되면, 적절한 입증들이 발생했다는 스테이트먼트를 국지적 검증기가 준비하고, 증명된 키 쌍($K_{sign\_verify\_priv}$, $K_{sign\_verify\_pub}$)으로부터 개인 키를 이용하여 이 스테이트먼트를 사인할 수 있다. 사인된 TPES와 연계되는 사인된 검증 스테이트먼트를 포함하는 메시지는 다음과 같이 표현될 수 있다:

수학식 3

[0089] $$TD_{RO\_target} \rightarrow RO: \quad [\text{ 검증 스테이트먼트 }]_{Ksign\_verify\_priv} \| [TPES]_{signed}$$

[0090] TTP(들)로부터{RIM_{RO}}(들), 및 TD_{RO_target}으로부터 사인된 TPIA 및 사인된 TPES를 수신시에, RO는 TD_{RO_target}이 THSM 내의 환경과 같은 환경에 있는 경우, RO가 RTO 프로세스를 지속하는데 동의하고, TD_{RO_target} 및 RO가 관심있는 임의의 다른 도메인들을 지원하는 하드웨어 또는 소프트웨어가, 무결성이 RO에 동의한다는 상태에 있다는 것을 검증할 수 있다.

[0091] 원래의 도메인에 대한 RTO 프로토콜은 전력 구동시에 시작할 수 있다. 선택적으로는, RTO 프로토콜은 전력-구동 이후에 시작할 수 있다. THSM의 안전한 부트가 완료될 때, 도메인들의 결과적인 구축은 콘텐츠들이 구성 파일에 의해 결정될 수 있으며, 구성 파일의 콘텐츠들은 최소의 전력-공급 시간과 같은 초기의 플랫폼의 상태, 또는 디바이스가 이전에 부트-업되고 그 후 전력 공급 중단(powered down)될 때의 이전의 상태를 반영한다. 따라서, 디바이스는 TD_{DM} 구축, "원래의" TD_{DO} 및 "원래의" TE_U 상태들을 포함하는 베이스 구성에 있을 수 있다. 대안적으로, WTRU는 예를 들어, TD_{DM}, "포스트-RTO" TD_{DO}, 및 "포스트-RTO" TE_U 상태들을 포함하는 RTO 프로세스들 또는 이전의 부트-업 및 도메인 구축에 기초하는 구성과 같은 추후의 구성에 있을 수 있다. 다른 대안에서, WTRU는 도 2에서 도시된 것과 같이 부가적인 도메인들의 확장된 세트를 또한 포함하는 구성에 있을 수 있다. 이러한 도메인들은 이전의 전력공급되는 세션 동안 생성될 수 있고 소유권은 이전의 세션들 동안 발생한 이전에 실행된 RTO 프로세스들에 의해 각자의 소유자들에 의해 취득될 수 있다.

[0092] 제 1 실시예를 참조하면, 플랫폼의 안전하고 신뢰적인 엔티티로서, THSM은 소유권-취득 프로토콜을 제어하고 ME가 초기에 신뢰적일 수 있는 상태에 있는지를 결정할 수 있다. 사전-준비된 키 K_{temp}는 THSM-ME 인터페이스를 통해 송신된 메시지의 비밀성을 보호하기 위해 이용될 수 있다. 단순함을 위해, 암호화된 메시지 A는 {A}에 의해 표시될 수 있고 메시지의 사인은 [A]에 의해 표시될 수 있고, 표시들(ID_{ME} 및 ID_{THSM})은 각각 ME 및 THSM의 사전-준비된 임시 ID들을 나타낸다.

[0093] RTO 개시는 특정 RO와의 RTO 프로세스 이후에 RO에 의해 청구되도록 의도되는 "미청구된", "원래의" 도메인에 대한 RTO를 TD_{DO}의 SDM이 개시하는 것을 포함할 수 있다. 사용자는 ME 플랫폼의 전력-공급을 개시할 수 있다. 전력-공급 시에, ME는 OMTP에 의해 정의된 부트와 같이, 베이스 코드들의 "비-TCG"안전한 부트"를 수행할 수 있

으며, ME는 "얼라이브(alive)"가 된다. 비-TCG 안전한 부트 프로세스의 부분으로서, ME의 베이스 코드들의 무결성이 자율적으로 확인될 수 있다.

[0094] 제 3 실시예를 참조하면, 모바일 신뢰 환경(Mobile Trusted Environment; MTE)은 베이스 코드 부트 프로세스의 완료에 후속하여 로딩될 수 있다. 사인 키를 이용하여, MTE는 ME 플랫폼 구성의 무결성을 입증할 수 있다.

[0095] 베이스 코드들의 로딩 후에, ME는 최소 안전 설정으로 부팅되었음을 표시하는 신호를 THSM에 주기적으로 송신할 수 있다. 신호가 송신되었을 때 THSM의 DO의 도메인이 아직 부트되지 않았을 수 있으므로, THSM의 DO의 도메인으로부터 확인응답 신호를 다시(back) 수신할 때까지 ME는 상이한 랜덤 넌스(random nonce)(넌스 1)를 갖는 동일한 신호를 송신할 수 있다. 이 신호는 다음과 같이 표현될 수 있다:

수학식 4

$$\text{Def)}\ \ \text{패키지\_1} = \text{“ME 베이스 코드 부트 완료 ”}\ \text{MSG} \| \text{넌스\_1} \| \text{ID}_{\text{ME}}$$

$$\text{ME} \rightarrow \text{THSM의 TD}_{\text{DO}}\text{: 패키지\_1} \| [\text{SHA-X(패키지\_1)}]_{\text{Ktemp\_I}}$$

[0096]

[0097] 제 3 실시예를 참조하면, 시그널링은 다음과 같이 표현될 수 있다:

수학식 5

$$\text{Def) 패키지\_1= “ME 베이스 코드 부트 완료 \& MTE 로딩 ”}\ \text{MSG} \| \text{넌스\_1} \| \text{ID}_{\text{ME}}$$

$$\text{ME} \rightarrow \text{THSM의 TD}_{\text{DO}}\text{: 패키지\_1} \| [\text{SHA-X(패키지\_1)}]_{\text{Ktemp\_I}}$$

[0098]

[0099] THSM은 THSM이 그의 DM의 도메인, "원래의" DO의 도메인, 사용자의 도메인 및 RO에 의해 아직 소유되지 않았지만 소유되기로 되어있는 적어도 하나의 "원래의" 도메인을 로딩할 수 있도록 "안전하게" 부트할 수 있다. 또한, 이 도메인들의 로딩에 있어서, 도메인들의 코드 상태들 각각의 무결성은 도메인들 각각의 기준 무결성 메트릭들(reference integrity metrics; RIM들)에 대하여 확인될 수 있다. 이 확인은 TCG MPWG 규격과 같은 규격에 따라 수행될 수 있다.

[0100] 디바이스 소유자의 도메인(TD_{DO})은, DO에 대한 RTO 프로세스를 이전에 통과했던 경우 "사전-구성된" 구성 또는 "마지막-보관된(포스트-프리비어스-RTO(post-previous-RTO))" 구성 둘 중 하나로 로딩될 수 있다. 로딩될 때, DO의 도메인은 시스템-와이드 도메인 관리자(SDM)를 포함할 수 있다. SDM은 다른 원격 소유자들(RO들)에 속하도록 도메인들의 구축 또는 로딩 및 관리를 감독할 수 있다. SDM은 DM의 도메인으로부터 "도메인들에 대해 이용 가능한 자원들의 리스트"를 룩업할 수 있고, 또한 TD_{DO}가 보호하는 시스템-와이드 도메인 정책(SDP)을 룩업할 수 있다.

[0101] 부트 시간에, SDM은 또한 "구축될 수 있는 도메인들의 리스트"를 THSM의 인간 사용자 또는 인간 소유자(DO)에게 촉구시키고 구축될 도메인들을 선택하기 위한 입력을 요청한다. 사용자 또는 소유자로부터의 그 입력을 획득한 이후, SDM은 인간 소유자 또는 사용자로부터의 응답에서 특정된 해당 도메인들만을 구축하도록 진행할 수 있다. SDM은 이 트랜잭션들에 대한 사용자 인터페이스(UI)를 제공하도록 ME와 상호작용할 수 있다.

[0102] 안전한 부트 이후에, THSM의 TD_{DO}는 "THSM 부트 완료" 메시지를 ME에 송신할 수 있다. 메시지 내에, TD_{DO}는 또한 로딩된 RO의 도메인의 수 및 명칭들과 같이, 도메인들의 현재 상태의 외부적으로 개시 가능한 요약(externally disclose-able summary)을 포함시킬 수 있다. TD_{DO}의 SDM은 도메인들의 현재 상태의 요약의 외부 개시의 정도를 결정 및 시행할 수 있고, 이러한 결정은 THSM 및/또는 ME 상의 도메인들의 사용자-특정 정책들(DP들) 및/또는 SDP에 기초할 수 있다. TD_{DO}는 SHA-X 무결성 확인 코드 입력의 부분으로서 수신된 넌스 1을 포

함시킴으로써 이 메시지에서 패키지 1의 수신을 확인응답할 수 있으며, 이는 다음과 같이 표현될 수 있다:

수학식 6

$$\text{Def) 패키지\_2} = \text{“THSM 부트 완료 ”} \, \text{MSG} \,||\, \text{넌스\_2} \,||\, \text{ID}_{\text{THSM}}$$

$$\text{TD}_{\text{DO}} \rightarrow \text{ME: 패키지\_2} \,||\, [\text{SHA-X(패키지\_1} \,||\, \text{넌스\_1)}]_{\text{Ktemp\_I}}$$

[0103]

[0104] ID_{THSM}과 같은 THSM의 ID는 DM의 도메인(TD_{DM})에서 유지될 수 있고, TD_{DM}의 ID와 동등하게 될 수 있다. DO의 도메인 TD_{DO}는 수학식(6)의 패키지_2를 구성하도록 TD_{DM}으로부터 이를 페치(fetch)할 수 있다.

[0105] "THSM 부트 완료" 신호에 응답하여, ME는 그의 부트 프로세스를 완료하도록 지속할 수 있다. 그의 부트 프로세스의 완료 이후에, ME는 THSM의 TD_{DO}에 다음과 같이 표현될 수 있는 메시지를 송신할 수 있다:

수학식 7

$$\text{Def) 패키지\_3} = \text{“ME 부트 완료 ”} \,||\, \text{넌스\_3}$$

$$\text{ME} \rightarrow \text{TD}_{\text{DO}}\text{: 패키지\_3} \,||\, [\text{SHA-X(패키지\_3} \,||\, \text{넌스\_ 2)}]_{\text{Ktemp\_I}}$$

[0106]

[0107] 다음은 DO의 도메인의 SDM이 현재 "원래의" RO의 도메인에 대한 RTO 프로세스를 개시 및 감독하는 경우에 적용된다.

[0108] TD_{DO}가 ME로부터 패키지_2를 수신한 이후, RTO 프로세스가 개시될 수 있다. TD_{DO} 내의 시스템-와이드 도메인 관리자(SDM)는 RTO 프로세스를 시작하도록 "원래의" 타겟 RO의 도메인($TD^*_{RO\_Target}$)에 요청함으로써 RTO 프로세스를 개시할 수 있다. SDM은 자율적으로 또는 인간 소유자 또는 사용자에 의해 촉구될 때 이 프로세스를 개시할 수 있다. SDM은 타겟 RO에 대한 RTO 프로세스를 시작하도록 TD^*_{RO}에 요청을 송신할 수 있다. 이 요청은 RO의 ID 또는 네트워크 액세스 식별자(NAI)와 같이 타겟 RO가 누구인지를, 그리고 현재 요청의 유효 기간을 포함할 수 있다. 요청의 부분으로서 또는 요청에 부수적인 별개의 패키지로서, SDM은 "허용된 RO의 도메인들의 SDP의 조건들"(이하 SCARD로 지칭됨)의 리스트를 또한 송신할 수 있다. SDM은 또한 의도된 RTO 프로세스 이후에 그것이 완료되었을 때 TD_{RO}에 대한 "타겟 도메인 계획"을 송신할 수 있다. 이 메시징은 다음과 같이 표현될 수 있다:

수학식 8

$$\text{Def) 패키지\_4a} = \text{Request\_to\_start\_RTO} \,||\, \text{SCARD} \,||\, \text{Target\_Domain\_Plan} \,||\, \text{넌스\_4}$$

$$\text{SDM} \rightarrow \text{TD}^*_{\text{RO\_Target}}\text{: 패키지\_4a} \,||\, [\text{SHA-X(패키지\_4a)}]_{\text{Ksign\_SDM}}$$

[0109]

[0110] 패키지 4의 수신에 응답하여, $TD^*_{RO_Target}$는 이 요청을 수락 또는 거절할 수 있다. 이 요청은 RO가 RO의 도메인의 소유권을 취득하는 것을 허용하기 위한 "오퍼(offer)"로서 해석될 수 있다. $TD^*_{RO_Target}$는 사전-구성된 기준 또는 로딩된 RO의 도메인 정책의 그 자신의 "원래의" 버전에 기초하여 판단을 내릴 수 있다. $TD^*_{RO_Target}$는 $\text{Request\_to\_start\_RTO}$, SCARD, 및 $\text{Target_Domain_Plan}$을 조사하고, 실제 타겟 원격 소유자

가 또는 그의 부재시에 그의 이익을 위해 이러한 판단들을 내리도록 구성될 수 있다. 이는 다음과 같이 표현될 수 있다:

수학식 9

$$\text{Def)} \quad \text{패키지\_5a} = \text{Okay(or Not\_Okay)\_to\_start\_RTO} \,||\, \text{넌스\_5a}$$

$$TD^*_{RO\_Target} \rightarrow SDM: \quad \text{패키지\_5a} \,||\, [\text{SHA-X(패키지\_5a)} \,||\, \text{넌스\_4}]_{Ksign\_TD^*RO\_Target}$$

[0111]

[0112] "원래의" 타겟 RO의 도메인($TD^*_{RO\_Target}$)은 이 프로세스를 개시할 수 있다. $TD^*_{RO_Target}$은 RTO 프로세스에 대한 그의 "최종 도메인 계획"의 SDM을 경고(alert)할 수 있다. SDM은 요청을 허가 또는 거절할 수 있다. SDM이 요청을 허가하는 경우, TD^*_{RO}은 RTO 프로세스를 시작할 수 있으며, 이는 다음과 같이 표현될 수 있다:

수학식 10

$$\text{Def) 패키지\_5b} = \text{Intend\_to\_start\_RTO} \,||\, \text{최종 도메인 계획} \,||\, \text{넌스\_5b}$$

$$TD^*_{RO\_Target} \rightarrow SDM: \text{패키지\_5b} \,||\, [\text{SHA-X(패키지\_5b)}]_{Ksign\_TD^*RO\_Target}$$

[0113]

[0114] 패키지_5a 또는 패키지_5b 둘 중 하나의 수신에 응답하여, SDM은 $TD^*_{RO_Target}$에 대한 RTO 프로세스를 위해 TD_{DO}에 대한 RTO 프로세스에 의해 획득되거나 사전-구성될 수 있는 시스템 도메인 정책(SDP), 소유자에 의해 공급되거나 사전-구성될 수 있는 "원하는 도메인들"의 리스트, DM의 도메인에 의해 유지되고 연속적으로 업데이트되는 "도메인들에 대한 이용 가능한 자원들"의 리스트, 또는 THSM 내의 도메인들의 현재 상태를 룩업할 수 있다.

[0115] SDM은 또한 메모리 또는 THSM 상의 다수의 도메인들을 구축 또는 유지하기 위해 이용 가능한 가상 머신 스레드(virtual machine thread)들에 대한 컴퓨팅 자원들과 같은 자원들이 충분히 존재하는지, THSM 내의 도메인들의 현재 상태가 "원하는 도메인들" 리스트 내에 특정된 것과 매칭하는지, "원하는 도메인들" 내의 임의의 새로운 도메인들의 구축 또는 로딩이 THSM 내의 도메인들의 현재 상태에 의해 지원되고 SDP 하에서 또한 허용되는지, 또는 도메인들 중 하나 이상의 도메인이 RTO 프로세스를 통과하도록 요구되는지를 평가할 수 있다.

[0116] $TD^*_{RO_Target}$이 이용 가능한 자원들, THSM의 기존의 도메인들의 현재 상태 및 SDP에 따라 RTO 프로세스를 통과할 수 있다고 SDM이 결정하는 경우, SDM은 이 결정을 표시하고($TD^*_{RO\_Target}$) $TD^*_{RO\_Target}$ 및 그 주변 도메인들의 그의 평가를 위해 RTO 프로세스 동안 RO에 포워딩될 다수의 무결성 입증들을 준비하도록 진행할 수 있다. 이는 다음과 같이 표현될 수 있다:

수학식 11

$$\text{Def)} \quad \text{패키지\_6} = \text{Okay\_to\_go\_ahead\_with\_RTO} \,||\, \text{넌스\_6}$$

$$SDM \rightarrow TD^*_{RO\_Target}: \quad \text{패키지\_6} \,||\, [\text{SHA-X(패키지\_6)} \,||\, \text{넌스\_5(a또는b)}]_{Ksign\_SDM}$$

[0117]

[0118] SDM은 예를 들어, 특정한 도메인에 대한 RTO 프로세스를 개시할 것임을 WTRU 상에 디스플레이되는 메시지에 의해 인간 사용자에게 표시할 수 있다. SDM은 또한 "RTO 프로세스를 시작하기를 원하는 도메인들 및 원하는 RO"의 리스트를 인간 사용자 또는 인간 소유자(DO)에 촉구시키고 이 촉구에 응답하여 소유자 또는 사용자가 특정하

는 RO의 도메인들에 대해서만 RTO 프로세스들을 개시하도록 진행할 수 있다. SDM은 이러한 트랜잭션들에 대한 사용자 인터페이스(UI)를 제공하는 ME와 상호작용할 수 있다.

[0119] $TD^*_{RO_Target}$은 THSM 플랫폼 무결성 입증(TPIA) 및 THSM 플랫폼 환경 요약(TPES)을 구성하도록 이용할 수 있는 자료(material)를 준비하도록 SDM에 요청할 수 있다. 이는 다음과 같이 표현될 수 있다:

수학식 12

$$\text{Def) 패키지\_7} = \text{Request\_for\_TPIA} \,\|\, \text{Request\_for\_TPES} \,\|\, \text{넌스\_7}$$

$$TD^*_{RO\_Target} \rightarrow \text{SDM:}$$

$$\text{패키지\_7} \,\|\, [\text{SHA-X(패키지\_7)} \,\|\, \text{넌스\_6}]_{Ksign\_TD^*RO\_Target}$$

[0120]

[0121] 제 3 실시예를 참조하면, 요청은 다음과 같이 표현될 수 있다:

수학식 13

$$\text{Def) 패키지\_7a} = \text{Request\_for\_TPIA} \,\|\, \text{Request\_for\_TPES} \,\|\, \text{Request for MPID} \,\|\, \text{Request for MPES} \,\|\, \text{넌스\_7a}$$

$$TD^*RO\_Target \rightarrow \text{SDM:}$$

$$\text{패키지\_7a} \,\|\, [\text{SHA-X(패키지\_7a} \,\|\, \text{넌스\_6)}]Ksign\_TD^*RO\_Target.$$

[0122]

[0123] TPIA 및 TPES에 대한 요청들에서, RO는 RO가 TPIA 및 TPES에 관한 어떤 종류의 정보를 SDM으로부터 요구하는지를 특정할 수 있다. 예를 들어, TPIA의 경우, RO는 그 자체보단, RO가 무결성을 검증하고자 하는 도메인들의 명칭들 또는 영역들을 특정할 수 있다. 마찬가지로, TPES의 경우, RO는 그 자체 보단, 네트워크 할당 식별자들(NAI들)과 같이, 도메인들의 소유자들의 공개 ID들을 특정할 수 있다.

[0124] 제 3 실시예를 참조하면, 타겟 RO는 ME 플랫폼의 무결성에 관한 특정(이하 MPID로 치칭됨) 및 ME 환경에 관한 다른 정보를 또한 요청할 수 있다. 대안적으로, RO는 MTE가 로딩되었고, MPID 및 MPES가 ME에 의해 SDM에 송신되었다는 단순 표시자를 요청할 수 있다. MTE, ME 플랫폼에 상주하는 신뢰적인 엔티티는 SDM에 의해 상기와 같이 수행하도록 요청될 때 값들(MPID 및 MPES)을 준비할 수 있다. 이는 다음과 같이 표현될 수 있다:

수학식 14

$$\text{Def) 패키지\_7b} = \text{Request for MPID} \,\|\, \text{Request for MPES} \,\|\, \text{넌스\_7b}$$

$$\text{SDM} \rightarrow \text{MTE:}$$

$$\text{패키지\_7b} \,\|\, [\text{SHA-X(패키지\_7b)}]Ksign\_SDM$$

[0125]

[0126] MTE는 ME로부터 구성 데이터를 모으고 MPID를 구축할 수 있다. 환경 데이터는 ME 플랫폼 환경 서베이(MPES)를 생성하기 위해 또한 획득될 수 있다. 이 값들은 시간이 경과함에 따라 변할 수 있는 현재의 ME 상태에 기초할 수 있다. 업데이트된 값들은 미래 요청들이 ME 상태 변화들에 따라 형성되면 SDM에 송신될 수 있다. 일반적으로, MTE는 응답을 SDM에 송신할 수 있으며, 이는 다음과 같이 표현될 수 있다:

[0127] [수학식 14a]

$$\text{Def) 패키지\_8a} = \text{MPID} \,||\, \text{MPES} \,||\, \text{Cert}_{\text{MTE}}$$

$$\text{MTE} \rightarrow \text{SDM:}$$

$$\text{패키지\_8a} \,||\, [\text{SHA-X(패키지\_8a} \,||\, \text{넌스\_7b)}]\text{Ksign\_MTE}$$

[0128]

[0129] MTE는 CA에 의해 사인될 수 있고, 그의 공개 키(K_{MTE_Pub})를 포함하는 인증서를 제공할 수 있다. 따라서, SDM은 CA들 서명의 검증을 이용하여 이 공개 키의 진정성을 검증하고, 그럼으로써 K_{MTE_Pub}를 이용하여 MTE로부터의 메시지의 무결성을 확인할 수 있다. SDM은 TPIA 및 TPES를 준비하고 추후에 이들을 $TD^*_{RO_Target}$에 포워딩할 수 있다.

[0130] TPIA의 준비를 위해, SDM은 "원래의" TD_{RO}에 의해 그리고 그의 무결성 입증, TE_{DM}에 의해 그리고 그의 무결성 입증, TE_{DO}에 의해 그리고 그의 무결성 입증, TE_{U}에 의해 그리고 그의 무결성 입증(디바이스 사용자가 DO와 상이한 경우), 및 관심있는 임의의 다른 기존의 TD_{RO}의 RO에 의해 그리고 그의 무결성 입증과 같이, 무결성 입증들을 수집할 수 있다.

[0131] 대안적으로, SDM은 PCR들로부터 무결성 값들을 수집한 이후, 국지적 프로세스에 의해, 각자의 도메인들에 대한 PCR들로부터의 다이제스트 값들에 대하여 도메인들, 코드 및 데이터와 같은 측정 로그들의 자율적 확인 및 재-계산을 검증할 수 있다. 이는 TTP(PCA)가 각자의 도메인을 포함해야 하는 가장 최근의 코드들을 인지하지 못할 때 수행될 수 있고, TTP는 WTRU 상에서 TPM 또는 MTM에 대해 증명되는 AIK에 링크되는 사인 키를 증명할 수 있다. TTP는 RO가 SDM으로부터 TPIA를 비교하기 위해 이용할 수 있는 다이제스트 메트릭에 대한 기준값들을 제공하기 위해 구성되지 않을 수 있다. SDM은 국지적으로, SDM이 도메인들에 대해 획득하는 PCR 인용들(quotes)이 최신인지를, 도메인들에 대한 코드들의 다이제스트를 재계산하고 이들을 인용된 PCR 값들과 비교함으로써 확인할 수 있다. 이 국지적 확인이 통과한다는 것을 조건으로 하여, SDM은 그 후 TPIA에 사인하고 MTE 또는 ME에 의해 이것을 TD_{RO_target} 및 RO_{target}에 전달할 수 있다.

[0132] 다른 대안에서, 3-방향 검증, 실제 코드들과 같이, 도메인들의 다이제스트들 및 측정 로그들을 SDM이 TPIA의 부분으로서 제공할 수 있다. RO는 다이제스트들과 함께 코드들을 획득하면, TTP로부터 다이제스트들에 대한 기준 메트릭들을 획득할 수 있고, 측정 로그들로부터 다이제스트들을 재계산할 수 있고, 이것을 TTP로부터 수신한 다이제스트의 기준 메트릭은 물론, TD_{RO_target}로부터 수신한 인용된 PCR 다이제스트들과 비교할 수 있다.

[0133] 측정 로그들을 없이 또는 측정 로그들을 이용하여, TPIA는 또한 PCR 인용이 발생한 "국지적 시간"의 표시, 유효하게는 개별적인 도메인들을 위한 다이제스트들에 대한 인용들의 타임-스탬핑(time-stamping)을 포함할 수 있다. 이것은 도메인들의 PCR 다이제스트들 각각이 SDM에 의해 획득된 마지막 시간의 임의의 표시를 제공한다. 측정 로그가 RO에 송신되지 않는 경우, PCR들의 타임-스탬핑된 인용은 국지적 다이제스트들이 TPIA에서 획득되고 포함된 시간이, 입증 검증(attestation verification)에 있어서 그것의 사용을 허용하기에 충분히 최신인지를 판단하는 견지에서, TPIA에 표시된 입증을 검증하기 위해 요구될 때 몇몇 부가적인 정보를 RO에 제공할 수 있다. 이러한 타임-스탬핑을 위해 이용되는 클록(clock)은 신뢰할 수 있는 클록일 수 있다.

[0134] 3-방향 검증이 실패하는 경우, RO는 TTP가 RO에 업데이트된 기준 메트릭들 또는 측정들 로그들을 제공하도록 요청할 수 있으며, 여기서 RO는 업데이트된 기준 메트릭들 또는 측정들 로그들로부터 원하는 다이제스트들을 계산할 수 있다. RO는 3-방향 검증을 재시도할 수 있다. 이 검증이 성공적인 경우 RTO는 지속된다. 이 검증이 실패하고, 성공적인 3-방향 검증이 RO 정책에 의해 요구되는 경우, RTO는 종결될 수 있다.

[0135] DO의 도메인의 무결성 입증을 위해, SDM은 예를 들어, SDM의 본질적인 기능을 통해 자율적으로 이것을 획득할 수 있다. 무결성 입증들에 있어서, DO의 도메인의 것을 제외하고, SDM은 각자의 다른 도메인들에 그 자신의 각자의 무결성 입증을 생성 및 사인하도록 요청할 수 있다. 요청에서, SDM은 토큰과 같이, SDM이 도메인으로부터 무결성 입증을 요청하고 획득할 권한을 가졌는지를 확인하는데 이용할 수 있는 권한 데이터(authorization data)를 포함할 수 있다. 요청은 타겟 RO의 요청의 포워딩자(forwarder)로서 SDM 및 타겟 RO가 수신자 도메인

의 무결성을 검사하도록 요구되는 수신자 도메인들의 플랫폼 구성 레지스터들(PCR들)의 범위를 또한 포함할 수 있다. 이 요청은 다음과 같이 표현될 수 있다:

수학식 15

$$\text{Def)}\ \ \text{패키지\_8b(i)} = \text{Request\_for\_Attestation} \parallel \text{넌스\_8b(i)},\ i=1,2,\ldots,N$$

$$\text{SDM} \rightarrow \text{TD}_{\text{Domain}(i)}:$$

$$\text{패키지\_8b(i)} \parallel [\text{SHA-X}(\ \text{패키지\_8b(i)})\ ]_{\text{Ksign\_SDM}}$$

[0136]

[0137] 도메인(i)(i=1, 2, ..., N, 여기서 N은 SDM의 PCR 값을 수집하는 도메인들의 수)로서 표시되는 도메인들 각각은 우선 $\text{Request_for_Attestation}$의 권한 데이터를 확인하고, 그 후 $\text{Request_for_Attestation}$에서 특정된 바와 같이 PCR들의 범위의 PCR 값들을 페치한다. 이 동작은 다음과 같이 표현될 수 있다:

수학식 16

$$\text{Def)}\ \ \text{패키지\_8c}(i) = \text{PCR들의 특정된 범위의 값들PCR들}\ \ \parallel \text{넌스\_8c}(i),\ i=1,2,..,N$$

$$\text{TD}_{\text{Domain}}(i) \rightarrow \text{SDM}:$$

$$\text{패키지\_8c(i)} \parallel [\text{SHA-X}(\ \text{패키지\_8c(i)} \parallel \text{넌스\_8b(i)}\ ]_{\text{Ksign\_TD\_Domain(i)}}$$

[0138]

[0139] SDM은 입증들 모두를 연계시키고 그의 사인 키를 이용하여 이것을 사인하기 위해 THSM 플랫폼 무결성 입증(TPIA)을 수행할 수 있다. 이는 다음과 같이 표현될 수 있다:

수학식 17

$$\text{Def) TPIA} = \text{연계}\{\ \text{도메인(i)로부터의 사인된 PCR 값들}\ \},\ i=1,2,..,N$$

[0140]

[0141] TPES의 준비를 위해, SDM은, DM의 도메인으로부터 획득될 수 있는 THSM, HW 및 SW 구성 및 버전 번호들, 플랫폼 상의 도메인들의 번호, 메모리와 같이 현재 도메인들을 위해 소모되는 총 플랫폼 자원들, 기존의 또는 새로운 도메인들의 추가적인 구축 또는 확장들을 위해 남아있는 플랫폼 자원들, 도메인들의 명칭들, 또는 NAI와 같이 그들 소유자의 명칭들 또는 ID들(각자의 도메인 소유자에 의해 허용되는 경우), 날자/시간, 또는 위의 환경 정보가 SDM에 의해 수집되었을 때 날자/시간이 아닌 단조로운 카운터 값(이것이 이용 가능한 경우), 임의의 다른 관련 정보와 같이 SDM이 TD_{DM}, TD_{DO} 및 $\text{TD}_{\text{Domains(i)}}$으로부터 수집하는 정보를 연계시킴으로써 TPES를 생성할 수 있다. 이 요청은 다음과 같이 표현될 수 있다:

수학식 18

$$\text{Def) TPES} = \{\ \text{수집된 정보}\ \}$$

[0142]

[0143] SDM은 TPIA 및 TPES에 사인하고 이를 $TD^*_{RO_Target}$에 포워딩할 수 있다. SDM은 또한 그것이 SCARD를 조사할 수 없었던 경우 DO가 임의의 원래의 $TD^*_{RO_Target}$에 의존하도록 요구되지 않을 수 있도록 사인된 SCARD를 포함할 수 있다. SCARD는 RO가 SCARD, TPIA 및 TPES를 조사한 이후 소유권 취득을 진행하도록 판단을 내릴 수 있다. 이 메시징은 다음과 같이 표현될 수 있다:

수학식 19

$$SDM \rightarrow TD_{RO\_Target}:$$

$$SCARD \parallel \text{넌스\_8fb} \parallel [SHA\text{-}X(SCARD) \parallel \text{넌스\_8fb})]_{Ksign\_SDM}$$

$$TPIA \parallel \text{연계}\{\text{넌스\_8c(i)}\}\ [SHA\text{-}X(TPIA) \parallel \text{연계}\{\text{넌스\_8c(i)}\}]_{Ksign\_SDM,}$$

$$TPES \parallel \text{넌스\_8f} \parallel [SHA\text{-}X(TPES \parallel \text{넌스\_8f})]_{Ksign\_SDM}$$

또는

$$SCARD \parallel TPIA \parallel TPES \parallel [SHA\text{-}X(SCARD \parallel TPIA \parallel TPES \parallel \text{넌스\_8f})]_{Ksign\_SDM}$$

[0144]

[0145] SDM으로부터 TPIA, TPES, 및 SCARD를 수신시에, $TD^*_{RO_Target}$는 SDM의 공개 사인키를 이용하여 이들을 확인함으로써 그들의 무결성을 확인할 수 있다. 그 다음, TPIA, TPES, SCARD, 사용자에 의해 요구되는 서비스들을 표시하는 목적 정보 엘리먼트(P), 및 소유권-취득 메시지에 대한 요청(request_TO)은 ME에 송신될 수 있다. RTO 프로세스가 완전한(full) TSIM 성능을 위해 준비되어야 하는 도메인에 대한 것인 경우, TSIM 기능에 대한 사인된 인증서($Cert_{TSIM}$)는 또한 위의 패키지와 함께 준비되고 송신될 수 있다.

[0146] TISM 기능을 위해 이용되는 2개 이상의 인증서들이 존재할 수 있다. 하나는 원래의 TSIM 기능($CERT^*_{TSIM}$)에 대한 것이고, 나머지는 완전히 예시되거나 업데이트되는 것들에 대한 것이다. 원래의 TSIM 기능에 대한 인증서는 DM으로부터의 기능인 DM에 대한 인증서 구조에 모듈식으로(modularly) 임베딩될 수 있는데, 예를 들어, 원래의 TSIM 기능에 대한 인증서는 원래의 도메인에 플러깅(plugged)될 수 있다.

[0147] TD_{RO}가 사전에 적어도 하나의 RTO를 통과한 이후에 RO가 RTO 프로세스를 수행할 때, RO는 더 이상 $CERT^*_{TSIM}$를 송신하도록 요구하지 않을 수 있는데, 왜냐하면 이 인증서는 단지 원래의 도메인과 더불어 이용하는데 적절한데, TD_{RO}는 더 이상 원래의 도메인이 아닐 수 있기 때문이다. 따라서, 이 경우에, RO는 업데이트된 인증서($CERT_{TSIM}$)를 송신할 수 있다.

[0148] 콘텐츠는 타겟 RO의 공개 키(K_Target_RO_pub)로 암호화될 수 있으며, 공개 키(K_Target_RO_pub)는 $TD^*_{RO_Target}$에 의한 이용 이전에, 타겟 RO가 원래의 $TD^*_{RO_Target}$가 로딩되는 때를 이미 인지하는 경우에, 예를 들어, 인증서 전달에 의해 또는 사전-구성에 의해 이용 가능하게 될 수 있다. TSIM은 사인 키($K_{\_TSIM\text{-}Sign}$)를 이용하여 사전-준비될 수 있다. 이 개인 사인 키의 공개 키는 타겟 RO에 사전-분배될 수 있다. ID_{ME}는 ME의 ID이며, $TD^*_{RO_Target}$는 ME ID를 안전하게 보유하는 THSM DM의 도메인 TD_{DM}으로부터 획득한다. 이는 다음과 같이 표현될 수 있다:

수학식 20

Def) 패키지_9 =
SCARD || TPIA || TPES || P || Request_TO || $Cert_{TSIM}$ || ID_{ME} || 넌스_9

$TD^*_{RO\_Target}$ → ME:

$\{패키지\_9\}_{K\_Target\_RO\_Pub}$ || $[SHA\text{-}X(패키지\_9)]_{K\_TSIM\text{-}SIGN}$

[0149]

[0150] 제 3 실시예를 참조하면, 값들(MPIA 및 MPES)은 메시지에 부가될 수 있다. MPIA는 MTE에 의해 컴파일되는 구성 데이터(MPID)에 기초하여 THSM에서 계산되는 다이제스트를 포함할 수 있다. 이 다이제스트는 DM과의 실시간 통신을 통해 전달되거나 구성 파일에 사전에 존재하는 획득 증명된 메트릭(acquired certified metric)과 부합하는 경우에만 입증될 수 있다. 환경 정보 및 무결성에 대한 RO 요청에 따라, 수학식(20)은 SDM이 MPID 및 MPES를 성공적으로 수신하였다는 단순한 표시를 포함할 수 있다. 이는 다음과 같이 표현될 수 있다:

수학식 21

Def) 패키지_9 = SCARD || TPIA || TPES || MPIA || MPES || P || Request_TO || $Cert_{TSIM}$ || ID_{ME}
|| 넌스_9

$TD^*_{RO\_Target}$ → ME:
$\{패키지\_9\}_{K\_Target\_RO\_Pub}$ || $[SHA\text{-}X(Package\_9)]_{K\_TSIM\text{-}SIGN}$

[0151]

[0152] ME는 RO에 위의 전체 메시지를 전달할 수 있으며, 이는 다음과 같이 표현될 수 있다:

수학식 22

ME → 타겟 RO:
$\{패키지\_9\}_{K\_Target\_RO\_Pub}$ || $[SHA\text{-}X(패키지\_9)]_{K\_TSIM\text{-}SIGN}$

[0153]

[0154] 제 3 실시예를 참조하면, 메시지는 MPIA 및 MPES를 포함할 것이다.

[0155] RO는 그의 개인 키($K_{Target\_RO\_Priv}$)를 이용하여 패키지_10을 복호화하고, ME의 ID를 확인하고 메시지를 해석할 수 있다. RO는 SCARD를 해석할 수 있고 RO가 SDP로부터의 이들 조건들에 "동의"하는지를 알 수 있다. RO가 SCARD에 동의하는 경우, 원래의 $TD^*_{RO_Target}$로부터의 값(TPIA)은 예를 들어, 임의의 서비스 크리덴셜들 또는 구성 제어들이 타겟 RO의 도메인 $TD^*_{RO_Target}$에 제공되기 이전에 전반적인 초기 TSIM 상태를 나타낸다고 해석될 수 있다. 값(P)은 사용자에 의해 요구되는 서비스들을 표시하는 것으로서 해석될 수 있다. THSM-가능 $TD^*_{RO_Target}$의 경우에 MNO일 수 있는 타겟 RO는 그것이 TTP로부터 독립적으로 획득한 기준 무결성 메트릭(RIM) 값들(RIM_{RO})과 그것을 비교함으로써 TPIA에서 표시되는 바와 같은 그의 관심의 도메인들의 무결성을 검증할 수 있다.

[0156] MNO는 예를 들어, WTRU/THSM의 공급자에 의해 TTP에 제공되는 인증서를 통해 TPIA의 예상 값을 인지하는 성능을 가질 수 있다. 제 3 실시예를 참조하면, MPIA 및 MPES의 예상값들은 MTE가 신뢰적인 엔티티(여기서 그의 신뢰성은 THSM에 의해 입증됨)라는 사실에 의해 가능하게 형성되는 인증 프로세스를 통한 시간보다 빨리 인지될 수 있다.

[0157] 타겟 RO는 수신된 TPES를 룩업하고 $TD^*_{RO_Target}$가 THSM 시스템 내에 있는지를 평가할 수 있으며, 예를 들어, TPES에 의해 표현되는 바와 같이, 상기 THSM 시스템의 "주변 시스템 환경"은 스스로 RTO 프로세스를 통해 추가로 진행하는 것을 허용하는 RO의 문맥에서 타겟 RO에 "동의"된다.

[0158] TPIA, TPES, 목적 P, Request_TO, 및 제 3 실시예를 참조하여, MPIA 및 MPES를 확인한 이후, MNO와 같은 타겟 RO는 $TD^*_{RO_Target}$를 포함하는 충분한 THSM은 물론 타겟 RO에 의해 "소유권 취득"이 되도록 요청하는 원래의 $TD^*_{RO_Target}$이, RTO 프로세스를 추가로 진행하게 하고, 또한 $TD^*_{RO_Target}$가 몇 개의 사전-지정된 기본 서비스들을 제공하기 위해 타겟 RO와 상호작용하도록 $TD^*_{RO_Target}$을 허가하게 하기에 충분히 "신뢰"할 수 있다고 결정할 수 있다.

[0159] 도메인이 추후에 키들, 더 완전한 구성들, 파라미터들 및 실행 가능한 것(executable)들을 다운로드하고 이들을 설치하여 기본적인 "원래의" 상태가 허용하는 것보다 더 기능적이 되고, 또한 타겟 원격 소유자(RO)에 의해 청구되거나 소유되고 관리되도록 $TD^*_{RO_Target}$의 소유권-취득을 수행하기 위해, 타겟 RO는 실행 가능한 것들을 포함할 수 있는 구성 신호(CONFIG)를 송신할 수 있다. RO는 또한, $TD^*_{RO_Target}$이 수신된 CONFIG에 따라 구성들, 파라미터들 및 실행 가능한 것들을 설치하는 경우, 포스트-설치 상태와 매칭할 수 있는 이른바 RIM_{TSIM}라 불리는 TSIM에 대한 RIM을 송신한다. RIM_{TSIM}은 $TD^*_{RO_Target}$상의 안전한 메모리에 저장될 수 있고, 추가의 부트 시간에 TSIM 기능의 무결성을 확인하는데 이용될 수 있다. 다른 구성 이슈들은 물론 이용될 보안 방법(security measure)들을 특정하는 도메인 정책(DP)은 트랜잭션에 포함될 수 있다.

[0160] RO-특정 도메인 정책(DP)은 SDM에 의해 보유되는 시스템-와이드 도메인 정책(SDP)과 상이하며 THSM 상의 특정 RO에 의해 소유되는 하나 이상의 도메인들을 구축 민 관리하기 위한 계획을 나타낼 수 있다. RO-특정 DP는 그 특정 도메인에 특정되고 배타적인 도메인-내 애플리케이션 및 보안 방법들만을 관리하는 정책들 또는 계획들을 포함할 수 있다.

[0161] 몇 개의 RO들은 이러한 방식으로 그들의 DP들을 형성하여서, DP는 어떤 다른 RO들이 THSM 상에 구축되거나 관리되는데 "동의"하는지에 관한 제한들을 규정하는 준비(provision)들을 또한 포함할 수 있다. 예를 들어, 모바일 네트워크 운용자(MNO_A)는, TD_{MNO_A}를 다운로딩 및 설치한 이후, THSM 상의 다른 도메인들 중 일부의 상태 및 본질에 관해 TD_{MNO_A}에 특정된 조건들 중 일부가 흡족하게 충족되는 것으로 밝혀지지 않는 경우, 그의 타겟 도메인(TD_{MNO_A})이 예를 들어, 그의 서비스들 또는 활동들에 관한 제한들의 세트에 의해 관리되는 방식으로 그의 DP_{MNO_A}을 형성할 수 있다. 예를 들어, MNO는 DP_{MNO_A}를 구현할 수 있으며, 이로써 TD_{MNO_A}는, THSM 내의 더 큰 환경을 검사(survey)한 이후, 동일한 THSM 상에 설치되고 활성인 다른 MNO의 도메인들이 그 자신의 활성화된 TSIM 기능들과 더불어 존재한다는 것을 밝혀내는 경우 그의 TSIM 기능들을 디스에이블(disable)시킬 것이다.

[0162] $TD^*_{RO_Target}$은 P에서의 요청된 서비스에 대응하는 방식으로 스스로 구성하도록 요구될 수 있다. 예를 들어, RO는 ME에 응답을 송신할 수 있고, 여기서 메시지 비밀성은 공개 키($K_{TSIM-Pub}$)를 이용하여 보호된다. ME는 THSM 상의 $TD^*_{Target_RO}$에 이 메시지를 전달할 수 있다. $Cert_{RO}$는 Target_RO의 공개 키(K_RO_{-priv})를 포함할 수 있다. RO는 이 때, TSIM에 대한 기준 무결성 메트릭(RIM)을 송신할 수 있다. RO 응답은 다음과 같이 표현될 수 있다:

수학식 23

$$\text{Def) 패키지\_10} = \{\text{CONFIG}, DP_{RO}, ID_{RO}, RIM_{TSIM}\}K_{TSIM\text{-}Pub} \,||\, Cert_{RO} \,||\, Cert_{TSIM} \,||\, \text{넌스\_10}$$

$$\text{Target RO} \rightarrow \text{ME:}$$
$$\{\text{패키지\_10}\}_{K\_RO\text{-}Priv} \,||\, [\text{SHA-X(패키지\_13}|| \text{넌스\_9})]_{K\_TSIM\text{-}SIGN}$$

[0163]

수학식 24

$$ME \rightarrow TD^{*}_{Target\ RO}:$$
$$\{패키지\_10\}_{K\_RO\text{-}Priv} \| [SHA\text{-}X(패키지\_13 \| 넌스\_9]_{K\_TSIM\text{-}SIGN}$$

[0164]

[0165] $TD^{*}_{Ro_Target}$는 개인 키($K_{TSIM\text{-}Priv}$)로 이 메시지를 복호화하고 CA로 증명하는 확인 이후에 $Cert_{RO}$ 내의 공개 키(K_{RO_Pub})를 이용하여 RO 서명을 검증할 수 있다. 이것은 THSM 애플리케이션을 위해 수신된 기준 무결성 메트릭(RIM_{TSIM})을 안전하게 저장할 수 있다. 그것은 ID_{RO}로부터의 RO의 ID를 확인하고, 그 다음 RO의 정책 DP_{RO}을 확인하고 CONFIG의 구성 및 설치의 나머지를 진행할 수 있는지를 결정할 수 있다. $TD^{*}_{Ro_Target}$은 "완료" 도메인 상태에 도달하기 위해 CONFIG를 통해 재구성을 수행하고 그 후 그의 TSIM 기능의 측정된 메트릭이 RIM_{TSIM}에 표현되고 네트워크에 의해 통신되는 것과 매칭하는지를 결정하기 위해 자가-테스트를 실행할 수 있다. 도메인 TD_{RO_Target}은 이제 "완료"되고 더 이상 "원래"가 아니며, 그에 따라, 표기에서 별표시(*)가 제거된다. 이는 다음과 같이 표현될 수 있다:

수학식 25

$$TD^{*}_{Target\ RO}: DP_{RO}\ 확인\ ,\ RIM_{TSIM}\ 저장,\ 및\ CONFIG\ 설치$$
$$\rightarrow$$
$$TD_{Target\ RO}: RO의\ 도메인은\ "완료"됨$$

[0166]

[0167] 완료된 도메인($TD_{Target\ RO}$)은 "RTO 성공 및 도메인 완료됨" 상태 메시지를 ME에 송신할 수 있으며, 이 메시지는 타겟 RO에 포워딩된다. 이 메시지는 다음과 같이 표현된다:

수학식 26

$$Def)\ 패키지\_11 = \{"\ 도메인\ 완료됨\ "\| ID_{RO\_Target}\}_{K\_RO\text{-}Pub} \| \ 넌스\_11$$

$$TD_{Target\ RO} \rightarrow ME:$$
$$패키지\_11 \| [SHA\text{-}X(\ 패키지\_11 \|\ 넌스\_10)]_{K\_TSIM\_SIGN}$$

[0168]

[0169] 선택적으로, ME는 사용자에게, 전화가 지금 등록 및 크리덴셜 롤-아웃을 위한 준비가 되었다는 상태 메시지를 송신할 수 있으며, WTRU의 스크린에 디스플레이된다.

[0170] ME는 플랫폼의 재구성이 성공적으로 완료되었고 TSIM 크리덴셜들을 등록할 준비가 되었다는 상태 메시지를 RO에 포워딩할 수 있다. TD_{RO_Target}은 "$THSM\_TD_{RO}\_LOAD\_COMPLETE$" 상태를 달성한다. 이 메시지는 다음과 같이 표현될 수 있다:

수학식 27

$$ME \rightarrow Target\ RO:$$
$$패키지\_11 \| [SHA\text{-}X(\ 패키지\_11 \|\ 넌스\_10)]_{K\_TSIM\_SIGN}$$

[0171]

[0172] 이 RTO 프로토콜은 가입된 서비스 및 인증 및 키 동의(AKA)에 대한 크리덴셜의 다운로딩 및 준비를 위한 추후 프로토콜을 또한 제공하는 3G UMTS 네트워크 운용자에 대해 THSM의 사용자 또는 소유자로서 가입자를 등록하기 위한 프로토콜에 대한 프리커서로서 역할할 수 있으며, 이는 공유 비밀(K) 및 가입자 아이덴티티(IMSI)의 다운로딩 및 준비를 포함한다.

[0173] 공개-개인 키 세트에 대한 인증서들($Cert_{TSIM}$ 및 $Cert_{RO}$)은 그들이 이용되는 메시지에서 전달될 수 있다. 대안적으로 RO의 도메인(TD_{RO}) 및 RO는 신뢰적인 제 3 자로부터 그들 각자의 인증서들을 획득할 수 있다. 이 획득은 다음과 같이 표현될 수 있다:

수학식 28

[0174]
$$TTP \rightarrow ME \rightarrow TD_{RO}: Cert_{RO}$$
$$TTP \rightarrow RO: \quad Cert_{TSIM}$$

[0175] 다른 대안에서, RO의 인증서($Cert_{RO}$)는 네트워크로부터 ME로 전달될 수 있고, THSM의 인증서($Cert_{TSIHM}$)는 이들이 이용되는 메시지들의 전달 이전에 ME로부터 네트워크로 전달될 수 있다. 이와 같은 통신은 여기서 기술되는 암호화된 메시지들 이전에 송신될 수 있으며, 이러한 통신들은 다음과 같이 표현될 수 있다:

수학식 29

[0176]
$$ME \rightarrow RO: \quad Cert_{TSIM}\,(\text{단계 9의 메시지가 송신되기 이전})$$
$$RO \rightarrow ME: \quad CERT_{RO}\,(\text{단계 13의 메시지가 송신되기 이전})$$

[0177] 이들 대안적인 인증서 전달 방법들 각각에 대해, 엔티티 ID는 공개 암호화 키들이 이용되는 메시지들에 동봉될 수 있다.

[0178] 다른 대안에서, 공개 키들 대신 대칭키들을 이용하는 것은 메시지의 비밀성을 보호하는데 이용될 수 있다. 각 상황에서, 송신자는 예를 들어, 의사-난수 생성기(PRNG)를 이용하여 대칭키(K_S)를 생성하고, 공개 키가 아닌 이 키를 이용하여 메시지의 비밀성을 보호할 수 있다. 대칭적 암호화 키는 또한 암호화된 메시지와 함께 수신자에 송신될 수 있으며, 여기서 대칭적 암호화 키는 공개 키로 보호된다. 따라서, 수신자는 그의 개인 키로 키(K_S)에 액세스하고 그 다음 이것을 이용하여 메시지를 복호화할 수 있다.

[0179] 제 2 실시예를 참조하면, THSM 및 ME는 제 1 실시예의 것들과 상이할 수 있다. ME 그 자체 또는 ME 내의 신뢰적인 엔티티 대신, THSM은 ME가 부트할 때 ME의 코드들 모두 또는 그 일부의 무결성 검사를 수행하도록 구성될 수 있다. 선택적으로 THSM은 또한 ME에 대한 부트 코드들 모두 또는 일부를 저장할 수 있다. THSM은 외부 평가기로 ME의 무결성을 입증하도록 구성되지 않을 수 있다. THSM은 부트 시간에 ME 코드들의 무결성의 "국지적" 확인을 수행하도록 구성될 수 있다.

[0180] ME에 대한 무결성 값은 부트-업 프로세스에서 이용될 수 있고 RTO 프로세스에서 이용되지 않을 수 있다. ME의 안전한 부트로부터 발생하는 ME 코드 및 구성 상태를 나타내는, meas_ME로 표시되는 ME의 무결성 측정은 THSM의 DM의 도메인 TE_{DM}에 의해 획득될 수 있다. THSM의 TD_{DM}은 meas_ME의 유효성을 확인할 수 있지만, THSM은 플랫폼 입증에서 이를 포함하지 않을 수 있다.

[0181] 제 4 실시예를 참조하면, ME는 예를 들어, TCG MPWG의 견지에서 신뢰적인 ME일 수 있다. ME는 모바일 신뢰 모듈(MTM)을 포함할 수 있고 저장, 리포팅, 측정, 검증, 및 시행을 위해 신뢰 루트를 제공하는 그의 신뢰 앵커(trust anchor)로서 MTM을 갖기 때문에 신뢰될 수 있다.

[0182] 도 4 및 4a는 원격 소유권-취득 프로세스에 대한 예시적인 호 흐름도를 예시한다. 예를 들어, 도 4 및 4a는 ME(402), TD_{DO}(404), SDM(406), $TD^*_{Target\_RO}$(408) 및 타겟 RO(410) 중 하나 이상 사이에서 예시적인 호들을 예시한다. 도 4 및 4a의 화살표들은 호의 발신지/수신지를 나타낼 수 있다.

[0183] 도 2 및 도 3에서 도시되는 바와 같이, SDM은 THSM에 상주하고 DO의 기능 중 일부를 제공하는 시스템 와이드 도메인 관리자를 포함할 수 있다. SDM은 모든 도메인들이 SDP에 순응하여 그리고 도메인-특정 정책들에 따라(이러한 정책들에 있어서의 임의의 충돌들이 다른 도메인들의 DO 및 RO들 대신 SDM에 의해 중재(reconcile)되는 한에 있어) 동작하고 서로 상호작용하는 것을 보장하기 위해 디바이스에서 모든 이러한 도메인 셋업의 감시 및 조절을 가질 수 있다. TD_{DO}는 THSM에 의무적인 디바이스 소유자 도메인을 포함할 수 있다. TD_{DO}는 SDM을 포함할 수 있으며, 이에 따라 TD_{DO}는 시스템 레벨 도메인 정책을 유지할 수 있다. MTE는 ME 측에 대한 정책 관리자 ME_{PDM}을 포함할 수 있다. ME_{PDM}은 ME 상에서 정책 관리자 기능을 수행할 수 있으나 THSM에서의 SDM의 감시 대상이 될 수 있다. $ME^{*}_{Target_RO}$는 허용된 원격 소유자에 의해 원격 소유권에 대한 원래의 도메인 셋업을 포함할 수 있다. 타겟 RO는 $ME^{*}_{Target_RO}$의 소유권을 요청하는 원격 소유자를 포함할 수 있다.

[0184] ME는 인지되는 원격 소유자들에 의해 ME 상의 도메인들의 원격 소유권 취득이 지원되도록 하는 완전한 MTM 기능을 가정할 수 있다. 제 1 실시예를 참조하여 기술되는 RTO의 것과 유사하게; 이들은 THSM 및 ME 둘 다 상의 동일한 원격 소유자들에 의해 소유되는 도메인들에 대한 ME_{PDM}을 통해서 SDM에 의해 조사되는 궁극의 정책 제어에 의해 본질적으로 상이하다. 따라서, THSM 상의 도메인들을 또한 소유하는 동일한 원격 소유자에 의해 소유되는 임의의 ME 도메인의 형성 및 관리는 SDM의 정책에 따르는 방식으로 발생해야만 한다.

[0185] 도 4를 계속 참조하여, 베이스 코드 부트는 엘리먼트(41)에서 ME(402)에 의해 완료될 수 있다. 엘리먼트(415)에서, THSM은 안전하게 부트할 수 있다. THSM은 SDM을 포함하는 DO의 도메인을 로딩할 수 있으며, 여기서 SDM은, 1) 도메인 구축을 위해 이용 가능한 자원들; 및/또는 2) 사용자에 수락 가능한 도메인들의 리스트를 제공할 수 있다. 엘리먼트(42)에서, THSM은 그의 부트를 완료할 수 있다. 엘리먼트(425)에서 ME는 그의 부트를 완료할 수 있다. 엘리먼트(43)에서, ME는 그의 부트가 완료되었음을 표시할 수 있다. 이 프로세스 동안, DM의 도메인이 구축될 수 있고, 최적의 사용자 도메인(ME_{U})이 또한 구축될 수 있고, 이용 가능한 자원들이 확인된다. DM의 도메인은 ME 디바이스에 대한 도메인 정책의 초기 구성 및 규격을 제공하는 ME_{PDM}을 포함할 수 있다. ME_{DM}의 사전-구성에 의해, 이 정책은 ME 도메인과 THSM 도메인 사이에서, 공통 원격 소유자들과 더불어, THSM 상의 도메인들과 ME 상의 다른 도메인들과 같이, 그 도메인들에 대한 정책들에 관하여 SDP의 정책과 일관되게 형성될 수 있다.

[0186] 도 4를 계속 참조하여, 그의 사전-구성된 도메인들을 갖는 ME는 RTO를 개시하는 "부트 완료" 메시지를 엘리먼트(431)에서 송신할 수 있다. 이 메시지는 ME 내의 이용 가능한 자원들 및 DM 도메인 정책에 관한 명시적 정보를 포함할 수 있다. 엘리먼트(44)에서 타겟 도메인 계획을 포함하는, RTO를 시작하기 위한 요청이 송신될 수 있다. 엘리먼트(455)에서, $TD^{*}_{Target\_RO}$(408)에 의해, RTO 시작 요청을 수락 또는 거절하기 위한 판단이 내려질 수 있다. 엘리먼트(45)에서, RTO가 시작되어야햐는지를 표시하는 메시지가 송신될 수 있다. 대안적으로, 엘리먼트(456)에서, RTO는 $TD^{*}_{Target\_RO}$(408)를 통해 발신될 수 있다. 엘리먼트(451)에서, $TD^{*}_{Target\_RO}$(408)는 "RTO 최종 도메인 계획을 시작하기 위한 의도(intention to start RTO final domain plan)"를 송신할 수 있다.

[0187] SDM은 THSM의 시스템-와이드 도메인 정책(SDP)을 평가하고 어떤 제한들이 ME 도메인들 상에 부과되거나 할당되는지를 결정함으로써 ME 부트 메시지에 반응할 수 있다. 이 정책 제한들은 ME 및 THSM 상에서 그들의 연관된 원격 소유자들에 따라 어떤 도메인들이 허용 가능한지를 포함할 수 있다. SDM은 소유자가 인식하고 있는 것들을 포함해서, THSM 상의 도메인들을 갖는 동일한 원격 소유자에 의해 소유되는 도메인들에 대해 이용하기 위해 어떤 시스템-와이드 자원들이 ME가 이용하는데 허용되는지를 결정할 수 있다. ME_{PDM}은 수학식(7)의 메시지를 통해 정보를 수신할 수 있다. SDM은 또한 그의 베이스 정책에 대한 정책 제한들 및 그의 자원 리스트에 허용 가능한 자원들을 포함시킬 수 있다. ME_{PDM}이 정보를 수신한 이후, ME_{PDM}은 판단들에 대한 SDM으로부터의 허가의 획득을 요구함 없이 ME 상에서 자원들 및 도메인들의 관리에 관한 이러한 모든 판단들을 내리고 시행하는 견지에서의 특정한 특권을 조사할 수 있다.

[0188] 도 4를 계속 참조하면, 프로세스는 엘리먼트(465)에서 지속될 수 있다. 엘리먼트(465)에서, 다음은 SDP, 이용 가능한 자원들, 및/또는 수용 가능한 도메인들 및/또는 상태들이 확인 및/또는 평가될 수 있다. 엘리먼트(46)에서, "시작 OK" 신호가 송신될 수 있다. 엘리먼트(47)에서, TPIA, TPES, MPID 및 MPES에 대한 요청이 송신될 수 있다. 엘리먼트(475)에서, SDM(406)은 예를 들어, 도메인 당 PCR들의 범위 상에서 기존의 도메인들로부터의 무결성 입증들을 수집/연계시키고, 및/또는 TPES 정보를 수집 및/또는 연계시킬 수 있다.

[0189] 엘리먼트(471)에서, MPID 및 MPES에 대한 요청이 송신될 수 있다. 엘리먼트(476)에서, MPID 및 MPES에 대한 요청의 응답이 MTE에 의해 처리될 수 있다. 엘리먼트(48)에서, MPID 및 MPES는 사인 키를 이용하여 신뢰의 증명(proof of trust)과 함께 송신될 수 있다. 엘리먼트(481)에서, TPIA, TPES, MPID 및 MPES는 SDM(406)으로부터 $TD^*_{Target\_RO}$(408)로 송신될 수 있다. 엘리먼트(485)에서, THSM은 MPID(원 데이터)로부터 다이제스트 MPIA를 계산하고 MPIA를 확인할 수 있다. 수락 가능한 경우, 다이제스트 MPIA는 RO에 송신될 수 있다. 엘리먼트(49)에서, TPIA||TPES||MPIA||MPES||목적||RTO를 위한 요청이 송신될 수 있다.

[0190] 도 4a를 참조하고, RTO 프로세스를 지속하면, 엘리먼트(410)에서, TPIA||TPES||MPIA||MPES||목적||RTO 메시지는 타겟 RO(410)에 송신될 수 있다. 엘리먼트(418)에서, 타겟 RO(410)는 예를 들어, 다음, 즉 TPIA, TPES, MPIA, MPES 및 목적을 확인; RIM_{TDRO}에 대해 원래의 도메인의 신뢰성 결정; 수락성(acceptability)을 위한 DP 확인; 또는 완료 도메인 상태를 구축하기 위한 CONFIG 생성 중 하나 이상을 수행할 수 있다.

[0191] 위에 대한 대안은 $TD^*_{Target\_RO}$(408)가 MPIA 및 MPES 대신 ME의 신뢰성에 대한 SDM으로부터의 단순한 표시를 요청하는 것이며; 이 경우 SDM은 TPIA, TPES 및 ME 신뢰성 표시를 제공한다. 그러나 SDM은 여전히 MTE로부터 MPIA 및 MPES를 요청 및 수신한다.

[0192] 도 4a를 계속 참조하면, 엘리먼트(411)에서, 메시지 CONFIG||DP||RIM_{TDRO}||RO가 송신될 수 있다. 엘리먼트(412)에서, CONFIG||DP||RIM_{TDRO}||RO 메시지는 전달될 수 있다. 엘리먼트(428)에서, 도메인은 구축 및 구성될 수 있으며, 무결성은 RIM_{TDRO}에 대하여 확인될 수 있다. 또한, $TD^*_{Target_RO}$의 소유권이 취득될 수 있으며, 이에 따라 $TD^*_{Target_RO}$는 TD_{Target_RO}로 변환된다. 엘리먼트(413)에서, 도메인 완료 메시지가 송신될 수 있다. 엘리먼트(414)에서, 도메인 완료 메시지는 전달될 수 있다.

[0193] 도 5 및 5a는 완전한 입증(예를 들어, 제 4 실시예에 관련됨)을 갖는 원격 소유권-취득을 위한 예시적인 호 흐름도를 예시한다. 예를 들어, 도 5 및 5a는 SDM(502), TD_{DO}(504), ME_{PDM}(506), $ME^*_{Target\_RO}$(508), 및 타겟 RO(510) 중 하나 이상 사이에서의 예시적인 호들을 예시한다. 도 5 및 5a 내의 화살표들은 호의 발신지/수신지를 나타낼 수 있다. 엘리먼트(51)에서, 베이스 코드 부트 완료 메시지가 송신될 수 있다. 이에 응답하여, 엘리먼트(515)에서, THSM은 안전하게 부트하고 SDM을 포함하여 DO의 도메인을 로딩할 수 있다. 엘리먼트(52)에서, THSM 부트 완료 메시지가 송신될 수 있다. 이에 응답하여, 엘리먼트(525)에서, ME는 안전하게 부트할 수 있으며, 이는 이용 가능한 자원들의 확인은 물론 DM의 도메인, 포함된 ME_{PDM}을 로딩하는 것을 포함할 수 있다. ME_{PDM}은 이용 가능한 자원들 및 SDP와 일관되는 도메인 정책을 특정하는 초기 구성을 제공할 수 있다. 엘리먼트(53)에서, ME 내의 이용 가능한 자원들 및 DM의 도메인(정책 정보)을 포함해서, ME 안전한 부트가 완료되었다는 메시지가 송신될 수 있다. 엘리먼트(531)에서, "ME 부트 완료" 메시지는 SDM(502)으로 전달될 수 있다. 엘리먼트(535)에서, SDM(502)은 예를 들어, 시스템-와이드 정책을 평가하고 ME에 대해 허용 가능한 도메인들, 자원들 및 정책 제한들을 결정할 수 있다. 엘리먼트(54)에서, 도메인 정책 제한들 및/또는 허용 가능한 자원들에 관한 정보를 제공하는 메시지가 송신될 수 있다. 엘리먼트(545)에서, 정책 제약은 베이스 정책에 첨부될 수 있으며, 필요한 경우, 자원 리스트가 보정될 수 있다.

[0194] 도 5 및 5a의 엘리먼트(55 내지 511)는 도 4 및 4a에 도시된 엘리먼트(45 내지 414)와 유사할 수 있다. 값들(MPIA 및 MPES)의 평가는 수학식들(14 내지 19)의 것들과 유사할 수 있다. ME는 MTM 가능(capable)일 수 있으며 ME는 단지 원 데이터 MPID가 아니라 스스로 MPIA를 계산하도록 구성될 수 있다. SDM에 의해 전달되는 업데이트된 정책 제한들은 금지된 도메인들 또는 도메인들 정책들이 실현되지 않도록 확인될 수 있다. 정책 검사 및 평가는 ME_{PDM}에 의해 수행될 수 있다.

[0195] 엘리먼트(55)에서, RTO 시작을 위한 요청이 송신될 수 있으며, 이 요청은 타겟 도메인 계획을 포함할 수 있다. 엘리먼트(555)에서, ME_{PDM}에 의해 RTO 요청을 수락 또는 거절할지에 대한 판단이 내려질 수 있다. 엘리먼트(551)에서, RTO가 시작되어야 하는지를 표시하는 메시지가 송신될 수 있다. 대안에서, 엘리먼트(556)에서, RTO를 시작하기 위한 의향(intent)이 ME 타겟을 통해 발신될 수 있다. 엘리먼트(56)에서, RTO 메시지를 시작하기 위한 의향이 보내질 수 있다. 다음은 1) 확장된 도메인 정책; 및/또는 2) 확장된 정책에 따라 이용 가능한 자원들, 수락 가능한 도메인 및 상태들이 확인 및/또는 평가될 수 있다. 엘리먼트(561)에서, RTO의 시작이 수락 가능하다는 것을 표시하는 메시지가 송신될 수 있다. 엘리먼트(57)에서, ME 도메인 세트로부터 MPIA 및 MPES에 대한 요청이 송신될 수 있다. 엘리먼트(575)에서, 도메인 당 PCR들의 범위를 통해 기존의 도메인(MPIA)으로부

터 무결성 입증들의 수집들 및 연계들은 물론, MPES 정보의 수집 및 연계가 수행될 수 있다. 엘리먼트(58)에서, MPIA 및 MPES가 송신될 수 있다. 엘리먼트(59)에서, MPIA||MPES||목적|| RTO 요청이 송신될 수 있다(메시지 무결성 및 비밀성은 증명된 공개/개인 키들로 보호될 수 있음). 엘리먼트(595)에서, 타겟 RO(510)는 예를 들어, MPIA, MPES 및 목적 확인; RIM_{TSIM}에 대해 원래의 도메인의 신뢰성 결정; 수락성에 대한 DP 확인; 또는 완료 도메인 상태를 구축하기 위한 CONFIG 생성 중 하나 이상을 수행할 수 있다. 엘리먼트(514)에서, 메시지 CONFIG||DP||RIM_{TSIM}||RO 가 송신될 수 있다. 엘리먼트(515)에서, 도메인이 구축 및 구성될 수 있고, 무결성이 RIM_{TDRO}에 대해 확인될 수 있다. 또한, $ME^{*}_{Target_RO}$의 소유권이 취득될 수 있으며 이에 따라 $ME^{*}_{Target_RO}$는 ME_{Target_RO}로 변환된다. 엘리먼트(511)에서, 도메인 완료 메시지가 송신(사인되고, 무결성 보호됨)될 수 있다. ME는 도 3 및 3a에서 도시된 것과 같이 어떠한 메시지 전달도 이용되지 않을 수 있고 메시지들의 수가 감소될 수 있도록 타겟 RO와 직접 통신할 수 있다. 원래의 엔진 신뢰성 검증을 위한 RIM 인증서들에 관한 상세들과 함께 ME와 타겟 RO 간의 메시징에서의 공개/개인 키 교환을 위해 요구되는 인증서들에 관한 상세들이도 5에서는 도시되지 않는다.

[0196] 도 6은 THSM의 예시적인 상태 정의들, 천이들, 및 제어 지점 정의들을 예시한다. 예로서, M2M 통신 아이덴티티 모듈(MCIM)(그의 정의 및 기본적인 기능은 PCT 특허 출원 WO 2009/092115(PCT/US2009/031603)에 정의됨)에 대한 수명 주기는 여기서 정의된다. THSM은 MCIM의 상태 정의들 및 천이들을 포함해서, 기능 및 특징들을 개선하고 일반화할 수 있다.

[0197] 상태(601)에서, THSM은 예비-부트 상태에 있을 수 있다. 제 1 사용자는 THSM에 전력을 공급할 수 있고, THSM은 안전하게 부트할 수 있고 THSM은 상태(602)에 있을 수 있다. 상태(602)에서, DM 및 DO는 원래의 상태에 있을 수 있다. DM 도메인은 사전-구성된 파일로부터 구축될 수 있고 THSM은 상태(606)에 있을 수 있다. 상태(606)에서, THSM은 TD_{DM}이 로딩되는 포스트 부트 2 상태에 있을 수 있다. 상태(606)로부터, DO의 도메인은 사전-구성된 또는 다운로드된 파일들로부터 구축될 수 있고, THSM은 상태(605)에 놓여 있게 된다. THSM은 포스트 부트 3 상태에 있을 수 있고, TD_{DO} 도메인이 구축될 수 있지만, TD_{U} 또는 TD_{RO}는 로딩되지 않을 수 있다. 상태(605)로부터, DO의 도메인(SDM)은 사용자의 도메인을 로딩할 수 있으며, THSM은 상태(604)에 있게 된다. 상태(604)에서, THSM은 TD_{U}가 로딩되지만 RO 도메인들은 로딩되지 않을 수 있는 포스트 부트 상태 2a에 있을 수 있다. 상태(605)로부터, 원래의 RO 도메인은 SDP 상에 기초하여 구축될 수 있으며, THSM은 상태(707)에 놓여 있게 된다. 상태(707)에서, THSM은 TD_{RO} 및 TD_{DO}가 로딩되지만 TD_{U}는 로딩되지 않을 수 있는 포스트 부트 상태 7에 있을 수 있다. 상태(607)로부터 TD_{DO}(SDM)는 TD_{U}를 로딩할 수 있고, THSM은 상태(608)에 놓여 있게 된다. 상태(608)에서, THSM은 DO, DU 및 RO 도메인들을 로딩할 수 있다.

[0198] 상태(601)로부터, 사용자는 THSM에 전력을 공급할 수 있고 THSM은 안전하게 부트할 수 있고, THSM은 상태(603)에 놓여 있게 된다. 상태(603)에서, THSM은 저장된 구성이 가장 최근 전력 오프(power off) 이전의 구성이었던 저장된 구성으로 로딩될 수 있다. 상태(603)로부터, 구성을 변경하는 포스트 부트 트랜잭션이 발생할 수 있고, THSM은 상태(610)에 놓여 있게 된다. 상태(610)에서, THSM은 하나 이상의 이전의 활성 상태들이 비활성이 되는 상태에 있을 수 있다. 상태(603)로부터 상태(610)에 도달하는 프로세스와 유사하게, THSM은 THSM이 하나 이상의 활성 도메인들을 갖는 상태(609)에 있을 수 있다. 상태(609)로부터, 구성 변경 이벤트의 결과로서 천이가 발생할 수 있고, THSM은 재차 상태(610)에 놓여 있게 된다.

[0199] 상태들(604, 605, 607 및 608)에서, THSM은 새로운 정책 및/또는 실행 가능한 것들로 재구성될 수 있거나, 또는 비활성 상태로 천이할 수 있다. 또한, 상태(605)에서, SDP는 저장될 수 있다.

[0200] 도메인 관리의 제 1 방법에서, 도메인 소유자로부터의 정책, 즉, 시스템-와이드 도메인 정책(SDP)은 매우 제한적이고 "정적"일 수 있으며, 새로운 도메인 활동들 또는 목적들에 대한 엄격한 규칙들을 가질 수 있다. 이 정책들은 매 새로운 도메인 진입(entry) 또는 기존의 도메인 업데이트들마다 RO들에 통신할 필요성을 완화시키는 경향이 있을 수 있다.

[0201] 도메인 관리의 제 2 방법에서, SDP는 덜 제한적일 수 있고 활동들 및 목적들의 견지에서 더욱 유연할 수 있다. 각각의 새로운 도메인 진입 및 각각의 도메인 변경은 기존의 도메인 소유자들에게 리포트될 수 있다. 이는 정책 시행의 시스템을 보다 동적이 되게 할 수 있으며, 이는 플랫폼과 RO 간의 초기 및 이어지는 협상이 발생할 수 있다.

[0202] 도메인 관리의 제 1 방법을 참조하면, SDP는 사전-구성된 리스트에서 예외없이 허용되는 도메인들을 특정할 수 있다. 이 리스트는 RO들의 타입들 및 (각각의 타입에 대해) 얼마나 많이 허용되는지에 관한 정보를 포함할 수 있다. 리스트는 또한 RO들이 그들의 도메인들을 셋업하면 RO들이 제공할 수 있는 서비스들의 종류를 포함할 수 있다. 장래의(prospective) RO는 리스트에 의해 표시되는 기준들을 충족하는 것일 수 있다. RO는 리스트 및 정책 제약들과 같은 조건들에 관하여 예를 들어, 수학식(9)에 도시된 바와 같이 RTO 프로세스의 부분으로서 경고될 수 있다. RO는, SCARD의 수신 시에 RO가 해당 플랫폼 또는 디바이스 상의 이해관계자가 되고자 하는지를 독립적으로 결정할 수 있다. RO에 송신된 조건들은 다른 RO들의 아이덴티티(identity)들을 보호하기 위해 임의의 다른 RO들의 리스트들의 실제 명칭이 아니라 도메인 타입들 및 그들의 목적들을 포함할 수 있다. RO가 RTO를 끝까지 다하도록 결정하는 경우, RO는 정책으로부터 어떠한 이탈(devation)도 이 RO 또는 플랫폼 상에서 현재 활성인 임의의 다른 RO 또는 미래에 활성이 될 수 있는 임의의 다른 RO에 의해 허용되지 않을 것임을 보장할 수 있다. 그 결과, RO는 발생할 수 있는 후속 RTO들에 대해 경고될 필요가 없을 수 있고 경고되지 않을 수 있다.

[0203] 도메인 관리에 대한 제 2 방법을 참조하면, 단지, 어떤 원격 소유자들이 임의의 특정한 RO 타입들을 식별함 없이 허용될지와 같은 상대적으로 넓은 제한들 및 RO로부터 SDM으로의 보다 많은 정보에 대한 요청들 또는 몇몇 협상들과 같은 보다 많은 상호작용들을 허용하는 정책들은 RTO 프로세스 동안 수행될 수 있다. 또한, 도메인 구성 변경과 같이 모든 RO들과 SDM 간의 진행중인 협력(collaboration)이 존재할 수 있다. 따라서, 초기 및 심지어 이어지는 협상들은 RO/SDM 역학의 부분으로서 발생할 수 있다.

[0204] RTO 프로세스의 부분으로서, RO에는 구성 및 그 신뢰성에 관해, 제 1 방법의 경우와 비교해서 보다 일반적인 정보를 포함할 수 있는, TPIA, TPES 및 SCARD와 같이 RO가 요구하는 입증 및 정책 제어 정보가 주어질 수 있다. 기존의 도메인 구성에 기초하여, 타겟 RO는 RTO를 지속할지 여부를 결정할 수 있다. 타겟 RO가 소유권 취득에 대하여 즉시 결정하지 않는다면, SDM과의 협상 프로세스가 보장될 수 있다. 예를 들어, SDM은 타겟 RO의 도메인이 활성인 동안 어떤 도메인 타입들 및 참석자 서비스들이 활성이 될 수 있는지, 또는 SDM이 반대하는 도메인 타입이 막 활성화되려고 하는 경우 어떤 절차들을 수행할지를 타겟 RO로부터 요구할 수 있다. RO는 예를 들어, 특정한 다른 도메인 타입들 또는 심지어 특정한 다른 RO들에 의해 소유되는 도메인들이 활성화되거나 막 활성화되려고 할 때 그 자신의 도메인이 비활성화되는 것을 요구할 수 있거나, 또는 RO는, RO가 활성을 유지하지만 용량 또는 성능이 감소되는 것을 요구할 수 있다. SDM은 또한 어떤 이벤트 발생들이 RO에게 경고되어야 하는지를 RO로부터 요청할 수 있다. 이러한 이벤트는 RO가 반대하는 도메인 타입들이 활성 또는 비활성이 되는 것을 포함할 수 있다. RO는 다른 도메인 타입들 또는 특정한 다른 소유자에 의해 유지되는 도메인들이 그 자신의 도메인이 활성인 동안 임의의 활동이 완전히 차단되는 것을 요구할 수 있다.

[0205] SDM은 이러한 조건들을 수락 또는 거절하도록 결정할 수 있다. 정책 요건들의 광범위한 세트(broad set)로 동작중일지라도, SDM은 RO로부터의 요구들을 수락하는 것이 "정적인" 시스템 도메인 정책(SDP)의 의향 또는 레터(letter)에 여전히 따를 수 있는지를 결정하기 위해 의미론적인 성능 및 범위(latitude)를 가질 수 있다.

[0206] 도 7은 RO 도메인들이 달성할 수 있는 예시적인 상태들 및 동적으로 관리되는 환경에서 천이들이 발생할 수 있는 조건들을 예시한다. 상태(701)에서, 예를 들어, RO가 구축되지 않을 수 있는 것과 같은 널(null) 상태가 존재할 수 있다. 상태(701)로부터, 원래의 RO 도메인은 SDP에 따라 구축될 수 있으며, RO 도메인은 상태(702)에 놓여 있게 된다. 상태(702)로부터, RO가 TPIA, TPES 및 SCARD를 획득하는 것을 포함해서, RTO 프로세스가 수행될 수 있다. 또한, RO는 RTO의 조건들을 수락할 수 있고 RO 도메인은 상태(703)에 놓여 있게 된다. 상태(703)로부터, RO는 새로운 활성 도메인과의 정책 충돌이 존재한다는 것을 결정할 수 있고, 이에 응답하여, RO 도메인이 비활성이 되게 하거나 RO 도메인의 성능을 감소시키고 RO 도메인은 상태(704)에 놓여 있게 된다. 또한, 상태(703)로부터, RO 도메인은 업데이트된 정책/구성 변경들을 수신하고, 이는 결과적으로 수정된 구성 및/또는 업데이트된 정책 제한들을 갖는 RO 도메인을 발생시킨다. 상태(706)로부터, RO 도메인은 새로운 활성 도메인과의 정책 충돌이 존재한다고 결정할 수 있고, 이에 응답하여 RO 도메인이 비활성이 되게 하거나 RO 도메인의 기능을 감소시키고 RO 도메인은 상태(704)에 놓여 있게 된다. 또한, 상태(703)로부터, 새로운 소프트웨어 컴포넌트는 다운로드 또는 RTO를 통해 도입될 수 있고, 이는 결과적으로 RO 도메인의 수정된/확장된 상태를 발생시키며 RO 도메인은 상태(705)에 놓여 있게 된다. 상태(705)로부터, RO 도메인은 새로운 활성 도메인과의 정책 충돌이 존재한다고 결정할 수 있고, 이에 응답하여 RO 도메인이 비활성이 되게 하거나 RO 도메인의 기능을 감소시키고, RO 도메인은 상태(704)에 놓여 있게 된다.

[0207] 상태(711)에서 예시되는 바와 같이, 상태(702, 703, 704, 705 또는 706)의 RO 도메인은 예를 들어, DO, RO 등에 의한 삭제를 통해 널(null)이 될 수 있다. 상태(741)에서 예시되는 바와 같이, 비활성/감소된 기능성의 RO

도메인은 예를 들어, RO 도메인이 상태(704)로 이동하게 한 충돌을 해결함으로써 상태(703, 705 또는 706)로 이동할 수 있다. 상태(751)에서 예시되는 바와 같이, 상태(705)의 RO 도메인은 상태(703, 704 또는 706)로 이동할 수 있다. 상태(761)에서 예시되는 바와 같이, 상태(706)의 도메인은 상태(703, 705 또는 706)로 이동할 수 있다.

[0208] RO 도메인의 관리에 관하여, 동적인 도메인 관리의 부분으로서 허용될 수 있는 것은 이벤트들이 전개(unfold)됨에 따라 변경되는 요건들을 협상하기 위한 것이다. 예를 들어, RO는 이전에 반대했을 만한 다른 RO에 의해 제공되는 특정한 서비스는 그것이 그 서비스와 더 이상 경쟁할 필요가 없음을 결정하는 결과로서 이제 허용 가능하다는 것을 결정할 수 있다. 시간이 경과함에 따른 비지니스 모델들에 대한 변경들은 장래의 RO들에 의한 전략들 및 정책들의 협상에 영향을 미칠 수 있다. 동적 정책 구조를 이용하는 SDP는 이러한 전략 변경들을 수용하도록 만들어질 수 있다.

[0209] 스마트-빌링(smart-billing)과 조합된 M2M 지리-추적(geo-tracking)과 같은 서비스들에서(그러나 이것으로 제한되지 않음), RO들의 바람직한 로밍 제휴들 또는 폐쇄 그룹이 형성될 수 있다. 상이한 운용자들이 서로 간에 유사하거나 상이한 서비스 파트너들을 제공하는 이러한 그룹화된 서비스들은 바람직한 폐쇄 그룹을 야기할 수 있다. 이러한 서비스들, 운용자들 또는 둘 다의 바람직한 그룹은 디바이스 사용자에 번들링된 서비스 또는 패키지 딜(package deal)로서 제공될 수 있다.

[0210] 제 1 예에서, 패키지는 패키지가 지구 여기저기를 이동할 때 추적될 수 있다. 이러한 수백만 지리-추적 디바이스들이 활용될 수 있다. 패키지가 대륙을 횡단할 때 패키지에는 상이한 국가들의 상이한 운용자들에 의한 연결이 제공될 수 있다. 따라서, 연결을 획득하기 위해, 사용자는 다수의 로밍 프로파일들(roaming profiles)에 가입하도록 요구될 수 있다. 다양한 원격 운용자들에 걸쳐있는 이 로밍 프로파일들은 각 도메인이 원격 운용자에 의해 소유되고 관리되기 때문에 도메인 간 정책들로서 관리될 것이다. 정책들은 또한 로밍 기반 해결책들을 지원하는 대신, 새로운 서비스 제공자로의 완전한 핸드오버를 지원하도록 시행될 수 있다.

[0211] 제 2 예에서, 스마트 미터링 운용자(smart metering operator)들과 지리-추적 운용자들 간의 제휴가 기술된다. 이 도메인들은 상이한 운용자들에 의해 소유되고 운용될 수 있다. 비지니스 제휴들 또는 사용자 선호도들로 인해, 도메인들은 공동 프로파일(joint profile)을 지원하도록 조합될 수 있다. 노동, 저장, 또는 주차와 같은 자원들의 이용에 기초한 빌링(billing)에 있어서, 스마트 빌링은 패키지들의 추적과 함께 이용될 수 있다. 이와 같이 별개의 카테고리들 내에 있는 서비스들이 공존하는 경우들은 도메인 간 정책 관리의 지원을 이용할 수 있다.

[0212] 도메인 간 정책 관리자(Inter Domain Policy Manager; IDPM)는 도메인들의 그룹 행동을 관리하는 정책들을 관리할 수 있다. 도메인 간 정책들(Inter Domain Policies; IDP)은 RTO 프로세스 동안 각각의 RO에 의해 다운로딩될 수 있다. IDP들은 각각의 RO에 의해 사인되는 인증서에 의해 인증될 수 있다. 이 인증서들은 IDP와 함께 발행될 수 있다. 대안적으로 이 정책들은 외부 서비스 딜러(external service dealer)에 의해 증명되고 다운로드될 수 있다. 바람직한 운용자 리스트를 생성하는데 관심있는 디바이스 사용자들 또는 디바이스 소유자들은 IDP들을 생성할 수 있다. IDPM은 IDP들을 선택하는 우선순위 또는 후보 정책들의 수락 가능한 교차점(acceptabl intersection)을 평가하고 그 후 결과적인 정책을 시행함으로써 이 정책들을 처리할 수 있다.

[0213] IDPM은 그의 기능 중 하나로서 또는 THSM 상에 다운로드되거나 로딩(구축)될 수 있는 개별 엔티티로서 SDM에 대안적으로 부가될 수 있다.

[0214] 입증 프로토콜(attestation protocol)의 부분으로서, TD_{RO}는 TPIA, TPES, 및 SCARD를 전부 송신하는 대신, TPIA, TPES, 및 SCARD의 해시(hash)를 RO에 송신할 수 있다. RO는 스스로 또는 TTP에 의해 이러한 해시들을 검증하고 그에 따라 TDRO 및 주변 시스템들의 시행 가능성(viability)의 평가를 하기 위한 수단을 가질 수 있다. 이 방법은 PCT 특허 출원 WO 2009/092115 (PCT/US2009/031603)에 특정되는 바와 같은 반-자율적인 확인(SemiAutonomous Validation; SAV)과 유사하게 될 수 있다. TPIA, TPES, 및 SCARD 측정들 중 임의의 하나 또는 둘은 입증 단계 동안 송신될 수 있다.

[0215] THSM은 ME의 부분으로서 일체형으로 임베딩될 수 있다. 이러한 디바이스에 대한 RTO 프로세스는 단순화될 수 있는데, 그 이유는 프로세스가 ME와 THSM 간의 인터페이스를 제거할 것이기 때문이다.

[0216] 특징들 및 엘리먼트들이 특정한 조합들로 위에서 기술되었지만, 각각의 특징 또는 엘리먼트는 다른 특징들 및 엘리먼트 없이 단독으로 또는 다른 특징들 및 엘리먼트과의 다양한 조합들로 또는 다른 특징들 및 엘리먼트 없이 이용될 수 있다. 여기서 제공된 방법들 및 흐름도들은 범용 컴퓨터 또는 처리기에 의한 실행을 위해 컴퓨터

-판독 가능한 저장 매체에 통합되는 컴퓨터 프로그램, 소프트웨어, 또는 펌웨어로 구현될 수 있다. 컴퓨터-판독 가능한 저장 매체들의 예들은 판독 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 레지스터, 캐시 메모리, 반도체 메모리 디바이스들, 내부 하드 디스크들 및 제거 가능한 디스크들과 같은 자기 매체들, 자기-광학 매체들, CD-ROM 디스크들, 및 디지털 다용도 디스크들(DVD들)과 같은 광학 매체들을 포함한다.

[0217] 적합한 프로세서들은 예로서, 범용 처리기, 특수 목적 처리기, 종래의 처리기, 디지털 신호 처리기(DSP), 복수의 마이크로처리기, DSP 코어에 연결된 하나 이상의 마이크로처리기, 제어기, 마이크로제어기, 주문형 집적 회로(ASIC)들, 필드 프로그래밍 가능한 게이트 어레이(FPGA) 회로, 임의의 다른 타입의 집적 회로(IC) 및/또는 상태 머신을 포함한다.

[0218] 소프트웨어와 연관되는 처리기는 무선 전송 수신 유닛(WTRU), 사용자 장비(UE), 단말, 기지국, 라디오 네트워크 제어기(RNC), 또는 임의의 호스트 컴퓨터에서 사용하기 위한 라디오 주파수 트랜시버를 구현하는데 이용될 수 있다. WTRU는 모듈들과 함께 이용되고 카메라, 비디오 카메라 모듈, 비디오 전화, 스피커 전화, 진동 디바이스, 스피커, 마이크로폰, 텔레비전 트랜시버, 핸즈 프리 헤드셋들, 키보드, 블루투스® 모듈, 주파수 변조(FM) 라디오 유닛, 액정 디스플레이(LCD) 디스플레이 유닛, 유기 발광 다이오드(OLED) 디바이스 유닛, 디지털 음악 재생기, 미디어 재생기, 비디오 게임 재생기 모듈, 인터넷 브라우저, 및/또는 임의의 무선 근거리 영역 네트워크(WLAN) 또는 초광대역(UWB) 모듈과 같은 하드웨어 및/또는 소프트웨어로 구현된 모듈들과 함께 이용될 수 있다.

[0219] **II. 가입-기반 서비스들에 액세스하기 위한 등록 및 크리덴셜 롤-아웃**

[0220] 디바이스의 사용자는 가입-기반 서비스의 제공자와 가입 제휴를 생성하기를 원할 수 있다. 예를 들어, 도 1의 디바이스(100, 110, 120) 또는 도 2의 UE(200)와 같은 UE의 사용자는 원격 소유자에 의해 제공되는 가입 기반 서비스의 가입된 사용자로서 등록되기를 원할 수 있다. 가입-기반 서비스의 준비(provision)는 제 3 자(예를 들어, 제 3 자는 원격 소유자 대신 사용자에게 가입 기반 서비스를 판매할 수 있음)에 의해 용이하게 될 수 있다. 원격 소유자는 RTO 프로세스에 관련하여 위에서 기술된 바와 같이, 디바이스 상에서 도메인의 소유권을 취득할 수 있으며, 이는 원격 소유자 도메인으로서 지칭될 수 있다. 또한, 사용자는 디바이스 상에서 도메인의 소유권을 취득할 수 있으며, 이는 사용자 도메인으로서 지칭될 수 있다.

[0221] 사용자가 가입 기반 서비스에 액세스하기 위해, 등록 및 크리덴셜 롤-아웃이 발생하도록 요구될 수 있다. 등록 및 크리덴셜 롤-아웃은, 가입-기반 서비스(여기서 이러한 서비스는 원격 소유자 도메인을 통해 원격 소유자에 의해 랜더링될 수 있음)의 가입된 사용자로서 원격 소유자에 사용자를 등록하고, 사용자가 가입된 사용자로서 가입-기반 서비스를 이용하는 것을 가능하게 할 수 있는 크리덴셜들을 원격 소유자로부터 획득하고, 및/또는 원격 소유자 도메인에 크리덴셜들을 저장하는 것 중 하나 이상을 포함할 수 있다. 크리덴셜들은 사용자가 디바이스를 통해 가입-기반 서비스를 이용하는 것을 허용할 수 있다. 용어 크리덴셜은 종래의 크리덴셜들(예를 들어, 키들, ID들, 인증서들 등)을 포함할 수 있다. 용어 크리덴셜은 가입 관리 기 능들을 위해 이용되는 애플릿(applet)들 및 실행 가능한 것들과 같은 다른 문맥-관련 데이터 및 애플리케이션들을 포함할 수 있다.

[0222] 여기서 개시된 시스템들 및 방법들은 디바이스 또는 디바이스들을 통해 사용자가 다수의 가입-기반 서비스들에 액세스할 수 있게 되는 것을 기도(contemplate)한다. 예를 들어, RTO 프로세스에 관해서는 물론 도 1 및 도 2에 관련하여 위에서 기술된 바와 같이, 디바이스는 다수의 원격 소유자들에 의해 소유될 수 있는 다수의 도메인들을 가질 수 있다. 사용자는 다수의 원격 소유자들로부터 다수의 가입-기반 서비스들에 가입할 수 있다.

[0223] 등록 및 크리덴셜 롤-아웃은 원격 소유자가 원격 소유자 도메인의 소유권을 취득한 시간을 한참 지나서 발생할 수 있다. 무선 전화 성능을 구비한 무선 디바이스가 예로서 이용될 수 있다. 다수의 무선 캐리어들은 디바이스 상에서 다수의 도메인들의 소유권을 취득할 수 있다(예를 들어, 각각의 무선 캐리어가 원격 소유자임). 예를 들어, 무선 캐리어 1은 원격 소유자 도메인 1의 소유권을 취득할 수 있고 무선 캐리어 2는 원격 소유자 도메인 2의 소유권을 취득할 수 있다. 그러나, 사용자는 무선 캐리어 2가 아닌 무선 캐리어 1의 가입-기반 서비스(예를 들어, 무선 전화 서비스)에 관련되는 등록 및 크리덴셜 롤-아웃을 개시할 수 있다. 예를 들어, 무선 캐리어 1은 전반적인 무선 전화 서비스들에 관해 무선 캐리어 2보다 양호한 딜(deal)을 사용자에게 제공할 수 있다. 추후의 시간에(예를 들어, 몇일, 몇달, 몇년), 사용자는 무선 캐리어 2의 가입-기반 서비스(예를 들어, 무선 전화 서비스)에 관련되는 등록 및 크리덴셜 롤-아웃을 개시할 수 있다. 예를 들어, 무선 캐리어 2는 장거리 호출에 관하여 무선 캐리어 1보다 양호한 딜을 제공할 수 있다. 사용자는 등록 및 크리덴셜 롤-아웃이 둘 다에

대해서 완료되었기 때문에 둘 다의 가입-기반 서비스들을 이용할 수 있다. 예를 들어, 사용자는 국지적 호들에 대해서 무선 캐리어 1의 무선 전화 서비스를 이용할 수 있고, 장거리 호들에 대해 무선 캐리어 2의 무선 전화 서비스를 이용할 수 있다. 이 예는 원격 소유자가 이러한 어레인지먼트를 금지하는 셋-업 규칙들을 갖지 않는다는 것을 가정한다(예를 들어, RTO 프로세스를 참조). 이 예는 또한 원격 소유자가 원격 소유자 도메인의 소유권을 취득한 시간을 한참 지나서 발생할 수 있다는 것을 예시한다.

[0224] 등록 및 크리덴셜 롤-아웃 프로세스에 포함된 엔티티들은 다음들, 즉 사용자, 사용자 도메인, 원격 소유자, 원격 소유자 도메인, 제 3 자, 또는 반-자율적인 확인을 용이하게 하는 컴포넌트(예를 들어, 시스템-와이드 도메인 관리자) 중 하나 이상을 포함할 수 있다. 등록 및 크리덴셜 롤-아웃에 관련되는 엔티티들은 다음과 같은 속성들을 가질 수 있다.

[0225] 사용자는 가입-기반 서비스와 같은 서비스에 가입하고자 하는 디바이스의 사용자일 수 있다. 이러한 가입-기반 서비스들의 예들은 투자 정보 서비스(financial service)들, 셀룰러 통신 서비스들, 인터넷 연결 서비스들, 음악/비디오/멀티미디어 가입 서비스들, 아이덴티티 서비스들, 위치-기반 서비스들, 이메일/메신저-소셜-네트워킹 서비스들, e-북 서비스들, 게임 서비스들 등을 포함할 수 있지만, 이것으로 제한되지 않는다. 사용자는 또한 디바이스의 소유자일 수 있다. 사용자는 등록 및 크리덴셜 롤-아웃을 개시할 수 있다. 이 개시는 사용자 송신 개인 데이터(user sending personal data) 및/또는 종래의 로그인 정보를 포함할 수 있다. 사용자는 또한 예를 들어, 사용자가 가입된/가입하고 있는 가입-기반 서비스와 연관된 동작들과 관련될 때 가입자로서 지칭될 수 있다.

[0226] 사용자 도메인(TU_U)은 사용자 기능에 관련된 디바이스 상의 도메인일 수 있다. 사용자 도메인은 선택적인 도메인일 수 있다. 사용자 도메인은 여기서 기술되는 바와 같은 THSM의 부분일 수 있으며, 예를 들어, 도 2를 참조한다. 사용자 도메인은 생성되고 플랫폼의 초기 부트 시퀀스 동안 그의 기능이 제공될 수 있다. 소유자 도메인(TD_O)은 사용자 명칭(ID_U), 패스워드(PW_U), 개인 등록 데이터($REGDATA_U$)를 공급함으로써 TD_U에 등록을 개시할 수 있다. TD_U는 사용자 등록의 부분으로서 프로세스 ID(PID_U)를 생성할 수 있다. 이 정보는 등록을 개시하고 크리덴셜 롤-아웃을 요청하는데 이용될 수 있다. 예를 들어, 이 정보는 특정 요청(예를 들어, 특정 등록 및/또는 크리덴셜 롤-아웃 요청)과 연관될 수 있고 등록 및/또는 크리덴셜 롤-아웃에 대한 상이한 세션들 또는 프로세스들을 분별 또는 마크(mark)하는데 이용될 수 있다. 사용자 및 사용자 도메인은 ME를 통해 통신할 수 있다. 사전-준비되는 키들((예를 들어, 비밀성을 위한) K_{temp_C} 및 (예를 들어, 무결성/인증을 위해) K_{temp_I})은 ME/THSM 인터페이스를 통한 메시징을 안전하게 하는데 이용될 수 있다. 비대칭 키 쌍들은 ME/THSM 인터페이스를 통한 메시징을 안전하게 하는데 이용될 수 있다. ME는 도 8에 관련하여 도시되지 않을 수 있다. THSM으로의 사용자 통신은 TD_U를 통해 발생할 수 있다.

[0227] 원격 소유자(RO)는 디바이스를 통해 사용자에게 가입된 서비스를 제공할 수 있다. 원격 소유자는 사용자가 가입된 서비스를 이용하기 위해 요구될 수 있는 크리덴셜들을 제공할 수 있다. 크리덴셜들은 원격 소유자 도메인과 원격 소유자 사이의 강한 비밀로서 역할할 수 있는 인증 키(K)를 포함할 수 있다. 예로서, RO는 다음들, 즉 이메일 서비스 제공자, 인터넷 서비스 제공자, 소셜-네트워킹 서비스 제공자, 디지털 콘텐츠(음악, e-북들, 비디오 등) 제공자, 게임 서비스 제공자, 투자 정보 서비스 제공자, 애플리케이션 서비스 제공자(예를 들어, 모바일 결제의 서비스 제공자, 모바일 티겟팅(mobile ticketing), DRM, 모바일 TV, 위치-기반 서비스들 등) 또는 IMS 서비스 제공자 등 중 하나 이상일 수 있다.

[0228] 원격 소유자 도메인(TD_{RO})은 원격 소유자에 의해 정의된 기능을 제공할 수 있는 디바이스 상의 도메인일 수 있다. 원격 소유자 도메인은 위에서 기술된 바와 같이 THSM의 부분일 수 있으며, 예를 들어, 도 2를 참조한다. 원격 소유자 도메인은 위에서 기술된 RTO 프로세스에 관련하여 기술된 바와 같이 TSIM 기능을 가질 수 있다. 원격 소유자 도메인은 원격 소유자에 의해 제공되는 크리덴셜들을 저장할 수 있다. TD_{RO}는 사용자 도메인으로부터 사용자의 ID 및 프로세스 ID(ID_U, PID_U)를 수신하고 등록 및 크리덴셜 롤-아웃 동안 이 정보를 다양하게 이용할 수 있다.

[0229] POS(point of sale 또는 point of service entity)는 사용자에게로의 가입-기반 서비스의 판매/서비스를 용이하게 하는 제 3 자일 수 있다. POS는 도 8과 관련하여 기술된 바와 같이 티겟들(tickets)을 통해 판매를 용이하게 할 수 있다. 예로서, POS는 원격 소유자의 가입-기반 서비스의 사전 판매 및 사후-판매 고객 서비스 의무들을 판매 및/또는 수행하는 소매점(온라인, 노트와 책(brick and mortar) 등)일 수 있다.

[0230] 시스템 와이드 도메인 관리자(SDM), 예를 들어, 섹션 I에서 개시된 SDM은 등록 및 크리덴셜 롤-아웃의 부분으로서 하나 이상의 플랫폼들에 관련되는 입증 정보를 제공할 수 있다. 예를 들어, 등록 및 크리덴셜 롤-아웃 동안 요청시에, 반-자율적인 무결성 확인이 SDM에 의해 제공될 수 있다. SDM은 도메인의 컴포넌트와 같은 THSM의 부분일 수 있으며, 예를 들어, 도 2를 참조한다.

[0231] 등록 및 크리덴셜 롤-아웃은 다음들 중 하나 이상을 포함할 수 있다:

[0232] · POS는 티켓을 사용자와 연관시킬 수 있다. 티켓은 사용자의 아이덴티티를 설정할 수 있고 크리덴셜에 대한 요청이 원격 소유자에 대해 이루어질 때 제시될 수 있다. 사용자에게 주어진 티켓과 같은 티켓들은 RO에 의해 (예를 들어, 사전-생성된 세트들에서) POS에 분배될 수 있다. 티켓은 등록 및 크리덴셜 롤-아웃 프로세스에서 이용될 정보를 포함할 수 있다. 예를 들어, 정보는 "3개(triple)"을 포함할 수 있으며, 이 3개는 식별자(예를 들어, IMSI), 예를 들어, 크리덴셜들에 대한 요청이 이루어질 때 원격 소유자에게 챌린저 번호(challenge number)로서 역할할 수 있는 난수(RAND), 및 티켓 인증 값(AUTH)을 포함한다.

[0233] · 사용자 대신, 사용자 도메인이 등록을 요청할 수 있다.

[0234] · POS는 사용자의 연관된 개인 등록 데이터와 함께 사용자의 아이덴티티를 원격 소유자(예를 들어, 분배된 티켓은 국제 모바일 가입자 아이덴티티(IMSI)과 같은 식별자를 제공할 수 있음)에 리포트할 수 있다.

[0235] · 사용자는 식별자(예를 들어, IMSI)를 이용하여 크리덴셜 롤-아웃을 요청할 수 있다.

[0236] · 크리덴셜들은 디바이스에, 예를 들어, 가입 서비스에 액세스하는데 이용될 수 있는 원격 소유자 도메인에 전달될 수 있다. 원격 소유자 도메인은 가입 서비스를 관리하는데 있어 TSIM 기능을 제공할 수 있다.

[0237] 등록 및 크리덴셜 롤-아웃은 안전한 방식으로 발생한다. 다음의 사전-조건들 중 하나 이상이 만족될 수 있고 그리고/또는 사용자 등록 및 크리덴셜 롤아웃이 안전한 방식으로 발생한다고 가정될 수 있다.

[0238] · THSM/ME 플랫폼은 신뢰할 수 있는 상태에 있다고 간주될 수 있으며 원격 소유권 취득(RTO) 프로토콜을 통해 도메인이 이전에 구성되었던 원격 소유자에 의한 요청 시에 플랫폼 구성의 상태 또는 그의 부분들을 리포트할 수 있다. 디바이스는 "완전히 신뢰적인" 플랫폼 컴포넌트라고 간주되지 않을 수 있는 ME를 포함할 수 있다. ME의 신뢰성은 THSM에 의해 주기적으로 모니터링될 수 있다. ME 및 THSM에 연결하는 인터페이스는 일반적으로 안전하다고 고려되지 않을 수 있다. ME는 완전한 MTM 성능들을 가지며 그의 무결성을 입증할 수 있다고 가정될 수 있다.

[0239] · 플랫폼의 입증은 다음 방식들 중 하나 이상의 방식으로 구현될 수 있다:

[0240] o TPIA, TPES 및 SCARD의 이용을 포함하는 입증 리포팅, 예를 들어, RTO 프로세스를 참조.

[0241] o 현재 구성의 해시를 RO에 송신하는 것을 포함할 수 있는 원격 확인(remote validation)의 스케일링된 버전. 이러한 타입의 입증은 대량의 데이터의 전달을 방지하고자 할 때 이용될 수 있다.

[0242] o 플랫폼이 안전하다는 확인을 제공하고 내부 무결성 확인의 성능을 포함할 수 있는 반-자율적인 확인(semi-autonomous validation)

[0243] · 크리덴셜들은 원격으로 다운로딩될 수 있다. POS는 원격 소유자에 사용자를 등록하는데 가담할 수 있다. POS와의 통신은 다음 방식들 중 하나 이상의 방식으로 발생할 수 있다 :

[0244] o 사용자가 그의 식별 정보 및 등록 데이터를 송신할 때 사용자는 공중으로(over the air; OTA) 또는 인터넷 링크를 통해 POS와 통신할 수 있다.

[0245] o 사용자가 핸드셋을 통한 등록 로그인 단계를 완료한 후에, 사용자 도메인은 등록 및 크리덴셜 롤-아웃 프로세스에 관련된 POS와 인터넷을 통해 통신할 수 있다.

[0246] · POS는 티켓 분배 기능을 처리하기에 충분히 신뢰할 수 있다고 간주될 수 있다. 이에 따라 POS는 $Cert_{POS}$의 연관된 인증서와 더불어 $K_{POS-Priv}$ 및 $K_{POS-Pub}$로서 표시되는 증명된 키 쌍을 가질 수 있다. 이들은 각각 연관된 인증서들($Cert_{RO}$ 및 $Cert_{TSIM}$)과 더불어, 원격 소유자(K_{RO_Priv}, K_{RO_Pub}) 및 TSIM($K_{TSIM-Priv}$, $K_{TSIM-Pub}$)에 대한 키 세트들과 함께 등록 및 크리덴셜 롤-아웃에서 이용될 수 있다.

[0247] · 사용자와 사용자 도메인 간의 통신은 사용자에 의해 이용하도록 의도된 메시지들이 핸드셋의 스크린 상에 디스플레이되는 중개자(go-between)로서 ME의 이용을 가정할 수 있다. 이 메시지들은 각각 무결성 및 신뢰성 보

호를 위한 임시키들(K_{temp_I} and K_{temp_c})을 이용할 수 있고, ME는 사용자를 위해 해석(예를 들어, 복호화 및/또는 서명 검증)할 수 있다.

[0248] · 등록 및 크리덴셜 롤-아웃은 이것이 동일한 사용자 또는 가능하게는 다수의 사용자들로부터 다수의 등록 및 크리덴셜 요청들을 허용할 수 있는 정도로 유연할 수 있다. 예로서, 각각의 사용자는 주어진 신뢰적인 도메인(TD_{RO})에 대한 하나의(및 오직 하나) 등록을 설정할 수 있지만, 다수의 이러한 도메인들을 통해 다수의 등록들을 설정할 수 있다. 그러나, 다수의 개별 사용자들은 하나의 이러한 도메인에 대해 그들 자신의 등록을 각각 가질 수 있다. 각각의 TD_{RO}는 하나의 RO를 가질 수 있지만, RO는 다수의 등록들을 관리할 수 있으며, 각 등록은 개별 사용자를 위한 것이다. 또한 주어진 RO가 2개 이상의 TD_{RO}를 소유하는 것 또한 가능할 수 있다. 가능하게는 다수의 원격 소유자들에 대응하는 다수의 사용자들 및 신뢰적인 도메인들이 주어지면, 프로세스 ID는 예를 들어, 사용자 도메인, POS 및 원격 소유자에 의해 생성되고 다수의 등록들과 관련하여 모호성(ambiguity)을 방지하기 위해 이용될 수 있다. 주어진 등록 및 크리덴셜 요청을 위해, 가깝게 연관되는 3개의 프로세스 ID들, 즉 PID_U(사용자 도메인에 의해), PID_POS(POS에 의해) 및 PID_RO(원격 소유자에 의해)가 생성될 수 있다. PID_U는 사용자 도메인을 식별하기 위해 POS 또는 원격 소유자 둘 중 하나와 통신할 때 THSM 내의 엔티티들에 의해 이용될 수 있다. 이 ID들은 주어진 등록 프로세스를 고유하게 식별하는데 충분할 수 있다.

[0249] · 신뢰적인 엔티티들 간의 통신들은 공개-개인 키 쌍들을 이용하여 보호될 수 있으며, 여기서 공개 키들은 인증 기관(certificate authority; CA)에 의해 발행된 인증서를 통해 분배될 수 있다.

[0250] · 등록 및 크리덴셜 롤-아웃 동안, 넌스(nonce)들은 리플레이 공격들을 방지하기 위해 이용될 수 있다. 넌스들은 연속적으로 넘버링되거나 또는 다른 방식으로 순차적으로 순서화될 수 있거나, 또는 연속적 또는 다른 방식으로 순차적으로 순서화된 번호들을 포함할 수 있다. 서술적인 넌스 설계(descriptive nonce designation)들이 이용되는 특정한 도메인 간 상호작용들은 연속적으로 넘버링되지 않을 수 있다. 2개의 엔티티들 간의 라운드-트립 통신(round trip communication)에 있어서, 송신된 제 1 넌스는 리턴 메시지(return message)에서 새로운 넌스(보통문으로(in the clear))와 함께 그의 발신 위치에 재차 송신(비-보통문으로)될 수 있다. 리턴 넌스를 수신하는 엔티티는, 값이 초기에 그것에 의해 생성되었고 그에 따라 인지될 수 있으면, 리턴 넌스가 보통문으로 송신될 것을 요구하지 않을 수 있다.

[0251] · 서명들은 예를 들어, 여기서 SHA-X로서 표시될 수 있는 SHA 알고리즘의 미특정된 버전에 의해 계산된 고정 비트 길이의 암호 해시 값들에 적용될 수 있다.

[0252] 등록 및 크리덴셜 롤-아웃을 예시하는 방법이 이제 도 8을 참조하여 설명될 수 있다. 도 8은 등록 및 크리덴셜 롤-아웃 프로세스를 구현하는 예시적인 호 흐름들을 예시한다. 호 흐름들은 수학식으로서 표현될 수 있다. 수학식은 각각의 흐름과 연관될 수 있는 보안 기능들을 포함할 수 있다. 도 8에서 예시되는 호 흐름들은 예시적인 것을 의미한다. 다른 실시예들이 이용될 수 있다는 것이 이해될 것이다. 또한, 흐름들의 순서는 적절하게 변할 수 있다. 또한, 흐름들은 필요 없는 경우 생략될 수 있고 부가적인 흐름들이 부가될 수 있다.

[0253] 단계(1)에서, POS(30)는 사용자(32)와 같은 다양한 인가된 사용자들에 분배될 수 있는 사전-생성된 티켓들을 원격 소유자(RO; 40)에게 요청할 수 있다.

[0254]

패키지_0 = 티켓 요청 ‖ ID_{POS} ‖ 넌스 0 POS →RO: 패키지_0 ‖ $Cert_{POS}$ ‖ [SHA-X(패키지_0)]$K_{POS-Pri}$	수학식 1

[0255] 단계(2)에서, RO(40)는 공개 키($K_{POS-Pub}$)(예를 들어, 인증서($Cert_{POS}$)에서 수신됨)를 이용하여 POS 서명의 유효성을 확인하고 사용자(32)와 같은 사용자들을 등록할 때 이용될 수 있는 티켓들의 인덱싱된 세트(indexed set)를 송신함으로써 응답할 수 있다.

패키지_1 = $Ticket_i$ ‖ 넌스 0 ‖ 넌스 1 RO → POS: {티켓$_i$}$K_{POS\text{-}Pub}$ ‖ 넌스 1 ‖ [SHA-X(패키지_1)]K_{RO_Priv} ‖ $Cert_{RO}$	수학식 2

[0256]

[0257] 인덱싱된 세트 내의 각각의 티켓은 3개를 포함할 수 있다:

[0258] $$\text{티켓}_i = (IMSI_i \| RAND_i \| AUTH_i|)$$

[0259] IMSI(international mobile identity subscriber identity)는 예를 들어, 서비스 크리덴셜들을 요청할 때 사용자/가입자의 고유한 식별자로서 역할할 수 있다. RAND 값은 티켓 그 자체의 선도 표시(freshness indication)를 제공할 수 있는 난수이고 AUTH는 티켓의 무결성 및 진정성을 검증할 수 있는 수단이다. 키(K_{RO_Priv})(RO들의 개인 키)를 이용한 패키지_1 해시의 서명은 원격 소유자를 인증하는 동안 메시지의 무결성을 보호할 수 있다.

[0260] 단계(2)에서 송신된 메시지에 대해, POS(30)는 그의 개인 키(K_{POS_Priv})를 이용하여 티켓 세트를 복호화하고 공개키(K_{RO_Pub})(예를 들어, 인증서($Cert_{RO}$)에서 수신됨)를 이용하여 원격 소유자 서명을 검증할 수 있다. 수학식 1 및 수학식 2에서 표시된 바와 같이, 넌스0은 안전한 통신을 위해 요구될 수 있는 라운드 트립(송신자로부터 수신자로 그리고 다시 송신자로)을 형성한다.

[0261] 단계(3)에서, 사용자(32)는 예를 들어, THSM의 사용자 도메인(TD_U; 34)에 등록하고 ID, 패스워드 및/또는 등록 데이터와 같은 정보를 제공할 수 있다.

패키지_2 = ID_U ‖ 패스워드$_U$ ‖ $REGDATA_U$ ‖ 넌스$_U$ 사용자/소유자 → TD_U: ID_U ‖ 넌스$_U$ ‖ $REGDATA_U$ ‖ {패스워드$_U$} K_{temp_C} ‖ [SHA-X(패키지_2)]K_{temp_I}	수학식 3

[0262]

[0263] 단계(3)의 프로세스는 통상적인 로그인 및 등록 절차로서 간주될 수 있다. 메시지의 암호화 및 서명 특징들을 물론, 넌스(넌스$_U$)의 이용은 ME의 암시적인 존재를 반영할 수 있고 사용자에게 투명할 수 있다. 이 투명성은 도 8에서 도시된 방법 전체에 걸쳐서 사용자/소유자와 TD_U간의 다른 통신들과 관련될 수 있다.

[0264] ID_U 및 패스워드$_U$(또한 PW_U로 표시됨)는 그것이 플랫폼 상에서 셋업되는 계정들 각각에 대해 사용자에 의해 생성되는 고유한 사용자 명칭 및 패스워드일 수 있다. ID_U는 특정한 계정에 관하여 사용자를 식별할 수 있고 연관된 패스워드(패스워드$_U$)는 비밀(예를 들어, 다른 사람들이 아닌 인가된 사용자에 의해서만 인지됨)일 수 있으며, 사용자 인가(user authorization)를 위해 이용될 수 있다. $REGDATA_U$는 사용자 개인 정보를 포함할 수 있다.

[0265] 단계(4)에서, TD_U(34)는 단계(3)에서 수신된 메시지에서 정보를 판독하고 이 메시지에 정보를 저장할 수 있고, 프로세스 ID(PID_U)를 생성할 수 있다. K_{temp_C} 및 K_{temp_I}는 사전-준비될 수 있는 비밀성 및 무결성을 각각 나타낼 수 있다. 이는 TD_U(34)가 패스워드(패스워드$_U$)를 복호화하고 패키지_2의 해시된 서명을 검증하는 것을 가능하게 할 수 있다. PID_U는 등록 및 티켓 요청 프로세스를 시작하도록 $REGDATA_U$와 함께 POS(30)에 송신될 수 있다.

패키지_3 = PID_U ‖ $REGDATA_U$ ‖ 넌스3 TD_U → POS: PID_U ‖ 넌스3 ‖ $Cert_{TDU}$ ‖ $REGDATA_U$ ‖ [SHA-X(패키지_3)]$K_{TDU-Priv}$	수학식 4

[0266]

[0267] 단계(5)에서, POS(30)는 PID_U 및 $REGDATA_U$를 수신한 이후 그 자신의 PID(PID_POS)를 생성하고 이것을 PID_U 및 사용자 등록 정보와 연관시킬 수 있다. 플랫폼은 PID_U를 이용하여 POS(30)에 통신할 때, POS(30)는 메시지를 PID_POS에 의해 식별된 등록 프로세스의 부분으로서 간주할 수 있다. 그러므로 다수의 등록 프로세스들은 동시에 발생할 수 있다. PID_POS는 제 2 프로세스 식별자일 수 있다. 인증서($Cert_{TDU}$)와 더불어, POS(30)는 공개키($K_{TDU-Pub}$)를 이용하여 SHA-X(패키지_3)의 서명을 검증할 수 있을 수 있다. POS(30)는 PID_U를 이용하여 PID_POS를 TD_U(34)에 다시(back) 송신함으로써 단계(4)에서 메시지에 응답할 수 있다.

패키지_4 = PID_U ‖ PID_POS ‖ 넌스 3 ‖ 넌스 4 POS → TD_U: PID_U ‖ PID_POS ‖ 넌스 4 ‖ $Cert_{POS}$ ‖ [SHA-X(패키지_4)]$K_{POS-Priv}$	수학식 5

[0268]

[0269] TD_U(34)는 인증서($Cert_{POS}$)로부터 획득된 K_{POS_Pub}를 이용하여 SHA-X(패키지_4)의 서명을 검증할 수 있다. TD_U(34)와 POS(30) 간의 통신은 공중으로 또는 인터넷 경로에서 발생할 수 있다.

[0270] 단계(6)에서, TD_U(34)는 등록 요청을 TD_{RO}(38)에 송신할 수 있다. PID_U 및 PID_POS는 TD_{RO}(38)가 적절한 프로세스 연관들을 형성하는 것을 가능하게 하도록 메시지의 부분으로서 송신될 수 있다. 사용자 식별(ID_U)은 TD_{RO}(38)가 등록 시도를 행하는 특정 사용자의 서비스 프로파일에 대한 확인으로서 이용할 수 있는 메시지 내에 포함될 수 있다. 이 특징은 동일한 도메인에 관하여 다수의 사용자 등록들의 유연성을 제공할 수 있다.

패키지_5: 등록 트리거 ‖ PID_U ‖ PID_POS ‖ ID_U ‖ 넌스 4 ‖ 넌스 $_{TDU1}$ TD_U → TD_{RO}: 패키지_5 ‖ $Cert_{POS}$ ‖ $Cert_{TDU}$ ‖ [패키지_5]$K_{TDU-Priv}$	수학식 6

[0271]

[0272] TD_{RO}(38)는 인증서($Cert_{TDU}$)로부터 획득된 공개 키(K_{TDU_Pub})를 이용하여 TD_U(34)의 서명을 검증할 수 있을 수 있다.

[0273]

[0274] 단계(7)에서, TD_{RO}(38)는 다음의 메시지에서 POS(30)에 티켓 요청을 행할 수 있다. POS(30)는 그것이 메시지 5에서 TD_U(34)에 송신되고 메시지 6에서 TD_{RO}(38)에 전달되었던 넌스4를 예상할 수 있다. 넌스4와 더불어 패키지_6은 개인 키($K_{TSIM-Priv}$)를 이용하여 사인될 수 있다. POS(30)는 프로세스 ID(PID_U)를 이용하여 단계(4)에서 송신된 등록 데이터와 이 요청을 연관시킬 수 있을 수 있다.

패키지_6 = 티켓_요청 ‖ PID_U ‖ 넌스 5 $TD_{RO} \rightarrow POS$: 패키지_6 ‖ $Cert_{TSIM}$ ‖ [SHA-X(패키지_6 ‖ 넌스 4)]$K_{TSIM-Priv}$	수학식 7

[0275]

[0276] POS(30)는 인증서($Cert_{TSIM}$)를 통해 획득할 수 있는 공개 키(K_{TSIM_Pub})를 이용하여 메시지의 서명을 검증할 수 있다. POS(30)는 패키지_6(보통문으로 송신됨) 및 넌스4를 이용하여 SHA-X를 재생성할 수 있다.

[0277] 단계(8)에서, 등록 요청(티켓 요청)이 POS(30)에 의해 수신된 이후, POS(30)는 RO(40)로부터 앞서 수신된 세트로부터 티켓을 페치할 수 있다. POS(30)는 이 티켓을 예를 들어, THSM을 통해 TD_{RO}(38)에 송신할 수 있다. 공개 키($K_{TSIM-Pub}$)는 $티켓_k$를 암호화하는 것을 물론, 이 티켓을 수신자에 대해 은닉(blind)시키는데 이용될 수 있다.

패키지_7 = $티켓_k$ ‖ PID_POS ‖ 넌스 5 ‖ 넌스 6 POS → TD_{RO}: {$ticket_k$}$K_{TSIM-Pub}$ ‖ 넌스 6 ‖ [SHA-X(패키지_7)]$K_{POS-Priv}$ (k 는 RO와 연관된 티켓 세트로부터의 고정된 값임)	수학식 8

[0278]

[0279] TD_{RO}(38)는 그의 개인 키($K_{TSIM-Priv}$)를 이용하여 $티켓_k$를 복호화(은익해제)하고 메시지 6에서 $Cert_{POS}$를 통해 획득했던 K_{POS_Pub}를 이용하여 패키지_7의 서명을 검증할 수 있다. 이 프로세스는 티켓의 무결성을 인증 및 검증하도록 역할할 수 있다. TD_{RO}(38)는 PID_POS를 이용한 정확한 프로세스 연관을 행할 수 있다. 넌스(넌스5)는 TD_{RO}(38)에 리턴될 수 있다.

[0280] 단계(9)에서, TD_{RO}(38)에 송신된 티켓 외에, POS(30)는 또한 $REGDATA_U$를 포함할 수 있고 $티켓_k$로 사용자를 식별할 수 있는 등록 메시지를 RO(40)에 송신할 수 있다. 프로세스 연관을 위해 요구될 수 있는 정보를 RO(40)에 제공하기 위해, PID_POS 및 PID_U가 송신될 수 있다. 이는 RO(40)가 이 등록을 위해 생성한 ID와 수신된 프로세스 ID들을 연관시키는 것을 가능하게 할 수 있다. 이 메시지는 그것을 요청할 수 있는 크리덴셜들을 지정된 사용자에게 제공하기 위해 RO(40)에 의해 요구될 수 있는 정보를 포함할 수 있다.

패키지_8 = ‖ $REGDATA_U$ ‖ 넌스 7 ‖ PID_POS ‖ PID_U POS → RO: {$티켓_k$}K_{RO-Pub} ‖ 패키지_8 ‖ [SHA-X(패키지_8 ‖ $티켓_k$ ‖ 넌스 1)]$K_{POS-Priv}$	수학식 9

[0281]

[0282] 티켓은 메시지 2내의 $Cert_{RO}$에서 POS(30)에 의해 획득되었던 K_{RO-Pub}를 이용하여 암호화될 수 있다. RO(40)는 그의 개인 키($K_{RO-Priv}$)를 이용하여 $티켓_k$를 복호화하고 공개 키($K_{POS-Pub}$)를 이용하여 패키지_8의 서명을 검증할 수 있을 수 있다. 공개 키(K_{RO_Pub})는 RO(40)에 티켓을 바인딩시키는 효과를 가질 수 있다.

[0283] 단계(10)에서, RO(40)는 티켓을 포함해서 등록 정보의 수신을 확인응답할 수 있다. 예를 들어, RO(40)는 다음의 메시지를 TD_U(34)에 송신할 수 있다.

패키지_9 = ACK(등록 데이터 수신됨) ‖ PID_U ‖ PID_RO ‖ 넌스8 RO → TD_U: 패키지_9 ‖ $Cert_{RO}$ ‖ [SHA-X(패키지_9)]$K_{RO-Priv}$	수학식 10

[0284]

[0285] TD_U(34)는 단계(9)에서 메시지를 수신한 이후 RO(40)에 의해 생성된, PID_U 및 PID_RO의 수신과 더불어 RO(40)와의 프로세스 식별을 유지할 수 있다. TD_U(34)는 인증서($Cert_{RO}$)에서 수신된 공개 키(K_{RO_Pub})를 이용하여 패키지_9 해시의 서명의 유효성을 확인할 수 있다.

[0286] 단계(11)에서, 수학식(10)과 연관된 메시지를 수신한 이후, TD_U(34)는 크리덴셜들의 요청에 대한 사용자(32) 허용을 허가하는 스크린 메시지(screen message)를 사용자(32)에 발행할 수 있다.

패키지_10 = 크리덴셜 롤아웃을 요청할 수 있음 ‖ 넌스9 ‖ PID_U ‖ ID_U TD_U → 사용자/소유자 : 패키지_10 ‖ [SHA-X(패키지_10 ‖ 넌스$_U$)]K_{temp_I}	수학식 11

[0287]

[0288] 이 메시지는 메시지 3에서 이용된 사인 및 검증 프로세스와 유사하지만 반대 방향으로, ME 측 상에서의 동일한 키를 이용하여 THSM 상에서 검증되도록 적용될 수 있는 사인키(K_{temp_I})의 이용을 도시한다. 넌스$_U$는 라운드 트립을 수행하는 TD_U(34)에 의해 ME로 리턴될 수 있다. ID_U는 사용자(32)를 식별하도록 ME 및 TD_U(34)에 의해 이용될 수 있는 것은 물론, PID_U를 현재의 등록 및 크리덴셜 롤-아웃과 연관시키고 이는 프로세스 모호성을 방지할 수 있다.

[0289] 사용자는 크리덴셜 롤-아웃을 개시할 수 있으며, 예를 들어, 사용자는 가입자-관련 크리덴셜들을 획득하기 위해 원격 소유자에 적용할 수 있다. 단계(12)에서, 사용자(32)는 단계(11)에서 크리덴셜들에 대한 요청과 관련하여 전달된 메시지에 응답할 수 있다. 패스워드는 공유 암호화키(K_{temp_C})를 이용하여 보호될 수 있다. 넌스$_9$는 TD_U(34)에 리턴될 수 있다.

패키지_11 = 크리덴셜 롤-아웃 요청 ‖ 넌스10 ‖ PID_U ‖ ID_U 사용자/소유자 → TD_U: 패키지_11 ‖ { 패스워드$_U$ }K_{temp_C} ‖ [SHA-X(패키지_11 ‖ 패스워드$_U$ ‖ 넌스9)]K_{temp_I}	수학식 12

[0290]

[0291] TD_U(34)는 공유 암호화 세트를 이용하여 패스워드를 복호화하고 서명을 검증할 수 있을 수 있다. 단계(11)에서 전달된 메시지는 PID_U, 및 ID_U 조합의 이용을 예시한다. 넌스들 및 PID들은 사용자/소유자에게 투명할 수 있고 비-인간 통신 엔티티들에 의해 이용되도록 제한될 수 있다.

[0292] 단계(13)에서, TD_U(34)는 이제 크리덴셜들에 대한 사용자 요청을 TD_{RO}(40)에 전달할 수 있고, 이는 TD_{RO}(40)를 트리거하여 RO(40)에 직접 요청을 행하게 할 수 있다. PID_RO 및 PID_U는 통신 엔티티들과의 프로세스 연관을 가능하게 할 수 있다. TD_{RO}(40)는 이제 3개의 프로세스 ID들을 연관시킬 수 있다.

패키지_12: 크리덴셜 롤-아웃 요청(TSIM) ‖ 넌스$_{TDU2}$ ‖ PID_U ‖ PID_RO $TD_U \rightarrow TD_{RO}$: 패키지_12 ‖ $Cert_{RO}$ ‖ [SHA-X(패키지_12)]$K_{TDU-Priv}$	수학식 13

[0293]

[0294] 메시지 검증은 단계(6)에서 전달된 메시지에서 수신되는 $Cert_{TDU}$에서 수신되는 $K_{TDU-Pub}$를 이용하여 달성될 수 있다.

[0295] 단계(14)에서, TD_{RO}는 SDM(36)에 대해 반-자율적인 무결성 검증을 위한 요청을 행할 수 있다. 반-자율적인 무결성 검증은 키 무결성 표시자들(예를 들어, TPIA, TPES 및 SCARD)의 해시 값의 이용으로 제한될 수 있다.

패키지_13 = 반-자율적인 무결성 검증 요청 ‖ PID_U ‖ 넌스$_{TDRO}$ $TD_{RO} \rightarrow SDM$: 패키지_13 ‖ $Cert_{TSIM}$ ‖ [SHA-X(패키지_13)]$K_{TDRO-Priv}$	수학식 14

[0296]

[0297] 인증서($Cert_{TSIM}$)는 SDM(36)이 패키지_13 해시의 서명 검증을 위해 공개 키($K_{TDRO-Pub}$)를 획득하는 것을 허용하도록 송신될 수 있다. 프로세스 ID 연관은 PID_U를 이용하여 유지될 수 있다. SDM(36)은 PID_U 이상 필요한 것은 아닐 수 있는데 그 이유는 SDM(36)은 외부 엔티티, 예를 들어, THSM 외부의 엔티티들과 통신할 수 없을 수 있기 때문이다.

[0298] 단계(15)에서, SDM(36)은 예를 들어, RTO 프로세스 이래로 발생했을 수 있는 구성 변경들에 관한 업데이트된 입증 정보를 수집할 수 있다. TPIA, TPES, 및 SCARD는 필요에 따라 업데이트될 수 있으며 무결성 데이터는 단일 값 IV(무결성 검증 값)내로 해시될 수 있다. PID_U 및 IV는 리턴 메시지에서 TD_{RO}(34)에 송신될 수 있다. 넌스(넌스$_{TDRO}$)는 리턴될 수 있다.

패키지_14 = IV ‖ PID_U ‖ 넌스$_{SDM}$ $SDM \rightarrow TD_{RO}$: 패키지_14 ‖ $Cert_{SDM}$ ‖ [SHA-X(패키지_14 ‖ 넌스$_{TDRO}$)]$K_{SDM-Priv}$	수학식 15

[0299]

[0300] 서명은 인증서($Cert_{SDM}$)에서 획득된 공개키($K_{SDM-Pub}$)로 검증될 수 있다.

[0301] 단계(16)에서, TD_{RO}(38)는 RO(40)에 대해 크리덴셜 롤-아웃에 대한 요청을 행할 수 있다. 단계(16)에서 송신된 메시지에서, 식별자($IMSI_k$)는 단계(13)의 메시지의 인증서($Cert_{RO}$)에서 TD_{RO}(40)에 의해 수신된 공개키(K_{RO-Pub})를 이용하여 암호화되어 RO(40)에 송신될 수 있다. 무결성 값(IV)은 신뢰 검증의 목적을 위해 송신될 수 있으며, 프로세스 ID(PID_U)는 단계(9)의 메시지 내의 정보와의 프로세스 연관을 가능하게 하도록 송신될 수 있다.

패키지_15 = 크리덴셜 롤-아웃 요청 ‖ ID_U ‖ IV ‖ PID_U ‖ 넌스11 TD_{RO} → RO: {$IMSI_k$}$K_{RO\text{-}Pub}$ ‖ 패키지_15 ‖ $Cert_{TDRO}$ ‖ [SHA-X(패키지_15 ‖ $IMSI_k$)]$K_{TDRO\text{-}Priv}$	수학식 16

[0302]

[0303] RO(40)는 그의 개인 키($K_{RO\text{-}Priv}$)를 이용하여 $IMSI_k$를 복호화하고 인증서($Cert_{TDRO}$)에서 RO(40)에 의해 획득된 공개키($K_{TDRO\text{-}Pub}$)를 이용하여 서명을 검증할 수 있다.

[0304] 단계(17)에서, 크리덴셜들은 RO(40)에 의해 TD_{RO}(38)에 송신될 수 있다. 크리덴셜들은 단계(16)의 $Cert_{TDRO}$로부터 획득된 공개키 $K_{TDRO\text{-}Pub}$를 이용하여 암호화될 수 있다. 이는 크리덴셜들을 TD_{RO}(38)에 바인딩할 수 있다. TD_{RO}(38)는 그의 개인 키($K_{TDRO\text{-}Priv}$)를 이용하여 크리덴셜들을 바인딩해제(unbind)할 수 있다. 넌스(넌스11)는 라운드 트립을 수행할 수 있다.

패키지_16 = PID_RO ‖ 넌스 12 RO → TD_{RO}: {$Cred_{TSIM}$}$K_{TDRO\text{-}Pub}$ ‖ 패키지_16 ‖ [SHA-X(패키지_16 ‖ 넌스11 ‖ $Cred_{TSIM}$)]$K_{RO\text{-}Priv}$	수학식 17

[0305]

[0306] TD_{RO}(38)는 단계(13)의 관련 인증서에서 수신된 공개키(K_{RO_Pub})를 이용하여 서명을 검증할 수 있다. 이 프로세스 ID(PID_RO)는 정확한 프로세스 연관을 제공한다.

[0307] 크리덴셜 키들은 예를 들어, 단계(17)에서 표시된 바와 같은 크리덴셜들의 수신 시에 SDM(36)에서 제공된 보안 정책에 따라 또는 보호된 메모리에서 저장될 수 있다. 정책은 RTO 프로세스 동안 정의되었을 수 있다. 단계(18)에서, 일단 롤-아웃이 완료되면, 확인응답 메시지(acknowledgement message)가 RO(40)에 송신될 수 있다.

패키지_17 = 롤-아웃 완료 ACK ‖ PID_U ‖ 넌스13 TD_{RO} → RO: 패키지_17 ‖ [SHA-X(패키지_17 ‖ 넌스 12)]$K_{TDRO\text{-}Priv}$	수학식 18

[0308]

[0309] 넌스(넌스12)는 리턴될 수 있으며 프로세스 모호성은 PID_U를 이용하여 방지될 수 있다. RO(40)는 단계(16)에서 획득된 공개키($K_{TDRO\text{-}Pub}$)를 이용하여 서명을 검증할 수 있을 수 있다.

[0310] 단계(19)에서, TD_{RO}(38)는 롤아웃 완료 확인응답 메시지를 TD_U(34)에 송신할 수 있다. 넌스(넌스$_{TDU2}$(13 참조) 및 넌스$_{TDU1}$(16 참조))는 리턴될 수 있으며, 프로세스 모호성은 PID_U를 이용하여 방지될 수 있다.

패키지_18 = 롤-아웃 완료 ‖ PID_U $TD_{RO} \rightarrow TD_U$: 패키지_18 ‖ $Cert_{TDRO}$ ‖ [SHA-X(패키지_18 ‖ 넌스 $_{TDU1}$ ‖ 넌스 $_{TDU2}$)]$K_{TDRO-Priv}$	수학식 19

[0311]

[0312] 서명은 인증서($Cert_{TDRO}$)에서 획득된 공개키($K_{TDRO-Pub}$)를 이용하여 TD_U(34)에 의해 검증될 수 있다.

[0313] 단계(20)에서, 사용자(32)에는 크리덴셜들이 수신되고 구성되었음을 표시하는 스크린 메시지가 TD_U(34)로부터 제공될 수 있다. 크리덴셜들은 이제 사용자(32)가 인가된 안전한 서비스들에 대해 이용 가능하게 될 수 있다. 넌스(넌스10)는 리턴될 수 있다(12 참조)

패키지_19 = 크리덴셜 설치됨 ‖ ID_U ‖ PID_U ‖ 넌스14 $TD_U \rightarrow$ 사용자/소유자 : 패키지_19 ‖ [SHA-X(패키지_19 ‖ 넌스10)]K_{temp_I}	수학식 20

[0314]

[0315] 서명 검증은 3, 11 및 12과 관련하여 기술된 바와 같이 달성될 수 있다. PID_U 및 ID_U 조합의 이용은 단계(11)과 관련하여 기술된 바와 같이 달성될 수 있다.

[0316] 단계(21)에서, 티켓$_k$가 이제 사용되고 다른곳에 분배되지 말아야 한다는 것을 표시하는 메시지가 POS(30)에 송신될 수 있다.

패키지_20 = 티켓$_k$ 이제 사용함 ‖ PID_POS ‖ PID_RO ‖ 넌스15 RO → POS: 패키지_20 ‖ [SHA-X(패키지_20)]$K_{RO-Priv}$	수학식 21

[0317]

[0318] POS(30)는 단계(2)에서 수신된 인증서($Cert_{RO}$)에서 획득된 공개 키(K_{RO_Pub})를 이용하여 서명을 검증할 수 있을 수 있다. PID_RO는 프로세스 연관을 가능하게 할 수 있다.

[0319] 도 8에서 예시된 호 흐름들과 관련하여 3개의 넌스들이 하나의 트립을 형성하는 것으로 도시되었다. 즉, 이들은, 이들이 먼저 통신되었던 때 이후의 메시지에서 리턴되지 않을 수 있다. 3개의 이러한 넌스들은 단계(10)의 넌스8, 단계(15)의 넌스$_{SDM}$ 및 단계(21)의 넌스(15)이다. 호 흐름 설명에서 표시되진 않았지만, 3개의 넌스들 각각에 대해서, 넌스를 포함하는 ACK가 수신자에 의해 대응하는 송신자에게 송신(리턴)된다. 따라서, 예를 들어, 넌스8은 단계(10)에서 메시지의 수신에 이어서 TD_U(34)에 의한 ACK 메시지를 통해 RO(40)에 리턴될 수 있다.

[0320] 단계들 1, 2, 9 및 21에 관련된 메시지들은 대역외(out of band)로서 지정될 수 있다.

[0321] 도 9는 하나 이상의 개시된 실시예들이 구현될 수 있는 예시적인 통신 시스템(900)의 도면이다. 통신 시스템(900)은 음성, 데이터, 비디오, 메시징, 브로드캐스트 등과 같은 콘텐츠를 다수의 무선 사용자들에게 제공하는 다중 액세스 시스템일 수 있다. 통신 시스템(900)은 무선 대역폭을 포함해서, 시스템 자원들의 공유를 통해 이러한 콘텐츠에 다수의 무선 사용자들이 액세스하는 것을 가능하게 할 수 있다. 예를 들어, 통신 시스템(900)은

코드 분할 다중 액세스(CDMA), 시분할 다중 액세스(TDMA), 주파수 분할 다중 액세스(FDMA), 직교 FDMA(OFDMA), 단일-캐리어 FDMA(SC-FDMA) 등과 같은 하나 이상의 채널 액세스 방법들을 이용할 수 있다.

[0322] 도 9에서 도시된 바와 같이, 통신 시스템(900)은 무선 전송/수신 유닛들(WTRU들)(902a, 902b, 902c, 902d), 라디오 액세스 네트워크(RAN)(904), 코어 네트워크(906), 공개 교환 전화 네트워크(PSTN)(908), 인터넷(910), 및 다른 네트워크(912)를 포함할 수 있지만, 개시된 실시예들은 임의의 수의 WTRU들, 기지국들, 네트워크들, 및/또는 중계 노드들, 게이트웨이들, 펨토 셀 기지국들, 셋-톱 박스들 등을 포함(그러나 이것으로 제한되지 않음)할 수 있는 네트워크 엘리먼트들을 기도(contemplate)한다는 것이 인지될 것이다. WTRU들(902a, 902b, 902c, 902d)은 무선 환경에서 동작하고 그리고/또는 통신하도록 구성된 임의의 타입의 디바이스일 수 있다. 예로서, WTRU들(902a, 902b, 902c, 902d)은 무선 신호들을 전송 및/또는 수신하도록 구성될 수 있고 사용자 장비(UE), 모바일국, 고정식 또는 이동식 가입자 유닛, 호출기, 셀룰러 전화, 개인 휴대 정보 단말(PDA), 스마트폰, 랩톱, 넷북, 테블릿, 개인용 컴퓨터, 무선 센서, 소비자 전자제품 등을 포함할 수 있다.

[0323] 통신 시스템(900)은 또한 기지국(914a) 및 기지국(914b)을 포함할 수 있다. 기지국들(914a, 914b) 각각은 코어 네트워크(906), 인터넷(910) 및/또는 네트워크들(912)과 같은 하나 이상의 통신 네트워크들에 대한 액세스를 용이하게 하도록 WTRU들(902a, 902b, 902c, 902d) 중 적어도 하나와 무선으로 인터페이스하도록 구성된다. 예로서, 기지국들(914a, 914b)은 베이스 트랜시버 스테이션(base transceiver station; BTS), 노드-B, e노드 B, 홈 노드 B, 홈 e노드 B, 사이트 제어기, 액세스 포인트(AP), 무선 라우터, 무선-가능 셋-톱 박스, 무선-가능 홈 게이트웨이, 중계 노드 등일 수 있다. 기지국들(914a, 914b)이 단일의 엘리먼트로서 각각 도시되었지만, 기지국들(914a, 914b)은 임의의 수의 상호연결된 기지국들 및/또는 네트워크 엘리먼트들을 포함할 수 있다는 것이 인지될 것이다.

[0324] 기지국(914a)은 다른 기지국들 및/또는 기지국 제어기(BSC), 라디오 네트워크 제어기(RNC), 중계 노드들 등과 같은 네트워크 엘리먼트들(도시되지 않음)을 또한 포함할 수 있는 RAN(904)의 부분일 수 있다. 기지국(914a) 및/또는 기지국(914b)은 셀(도시되지 않음)로서 지칭될 수 있는 특정 지리적인 영역 내에서 무선 신호들을 전송 및/또는 수신하도록 구성될 수 있다. 셀은 셀 섹터들로 추가로 분할될 수 있다. 예를 들어, 기지국(914a)과 연관된 셀은 3개의 섹터들로 분할될 수 있다. 따라서, 일 실시예에서, 기지국(914a)은 3개의 트랜시버들(즉, 셀의 각 섹터에 대해 하나)을 포함할 수 있다. 다른 실시예에서, 기지국(914a)은 다중-입력 다중 출력(MIMO)을 이용할 수 있고 그러므로 셀의 각 섹터에 대해 다수의 트랜시버들을 활용할 수 있다.

[0325] 기지국들(914a, 914b)은 임의의 적합한 무선 통신 링크(예를 들어, 라디오 주파수(RF), 마이크로파, 적외선(IR), 자외선(UV), 가시광 등)일 수 있는 공중 인터페이스(916)를 통해 WTRU들(902a, 902b, 902c, 902d) 중 하나 이상과 통신할 수 있다. 공중 인터페이스(916)는 임의의 적합한 라디오 액세스 기술(RAT)을 이용하여 설정될 수 있다.

[0326] 보다 구체적으로, 위에서 언급한 바와 같이, 통신 시스템(900)은 다중 액세스 시스템일 수 있고 CDMA, TDMA, FDMA, OFDMA, SC-FDMA 등과 같은 하나 이상의 채널 액세스 방식들을 이용할 수 있다. 예를 들어, RAN(904)의 기지국(914a) 및 WTRU들(902a, 902b, 902c)은 광대역 CDMA(WCDMA)를 이용하여 공중 인터페이스(916)를 설정할 수 있는, 범용 모바일 전기통신 시스템(Universal Mobile Telecommunications System; UMTS) 지상 라디오 액세스(UTRA)와 같은 라디오 기술을 구현할 수 있다. WCDMA는 고속 패킷 액세스(High-Speed Packet Access; HSPA) 및/또는 이볼브드(Evolved) HSPA(HSPA+)와 같은 통신 프로토콜들을 포함할 수 있다. HSPA는 고속 다운링크 패킷 액세스(High-Speed Downlink Packet Access; HSDPA) 및/또는 고속 업링크 패킷 액세스(High-Speed Uplink Packet Access; HSUPA)를 포함할 수 있다.

[0327] 다른 실시예에서, 기지국(914a) 및 WTRU들(902a, 902b, 902c)은 롱 텀 에볼루션(Long Term Evolution; LTE) 및/또는 LTE-어드밴스드(LTE-Advanced; LTE-A)를 이용하여 공중 인터페이스(916)를 설정할 수 있는, 이볼브드 UMTS 지상 라디오 액세스(E-UTRA)와 같은 라디오 기술을 구현할 수 있다.

[0328] 다른 실시예들에서, 기지국(914a) 및 WTRU들(902a, 902b, 902c)은 IEEE 802.16(즉, WiMAX(Worldwide Interoperability for Microwave Access)), CDMA2000, CDMA2000 1X, CDMA2000 EV-DO, IS-2000(Interim Standard 2000), IS-95(Interim Standard 95), IS-856(Interim Standard 856), GSM(Global System for Mobile communications), EDGD(Enhanced Data rates for GSM Evolution), GERAN(GSM EDGE) 등과 같은 라디오 기술을 구현할 수 있다.

[0329] 도 9의 기지국(914b)은 예를 들어, 무선 라우터, 홈 노드 B, 홈 e노드 B, 또는 액세스 포인트일 수 있으며, 사

업소, 가정, 차량, 캠퍼스 등과 같은 국지화된 영역에서 무선 연결을 용이하게 하기 위한 임의의 적합한 RAT를 활용할 수 있다. 일 실시예에서, 기지국(914b) 및 WTRU들(902c, 902d)은 무선 근거리 영역 네트워크(WLAN)를 설정하기 위해 IEEE 802.11과 같은 라디오 기술을 구현할 수 있다. 다른 실시예에서, 기지국(914b) 및 WTRU(902c, 902d)는 무선 개인 영역 네트워크(WPAN)를 설정하기 위해 IEEE 802.15와 같은 라디오 기술을 구현할 수 있다. 또 다른 실시예에서, 기지국(914b) 및 WTRU들(902c, 902d)은 피코셀 또는 펨토셀을 설정하기 위해 셀룰러-기반 RAT(예를 들어, WCDMA, CDMA2000, GSM, LTE, LTE-A 등)를 활용할 수 있다. 도 9에서 도시된 바와 같이, 기지국(914b)은 인터넷(910)으로의 직접 연결을 가질 수 있다. 따라서, 기지국(914b)은 코어 네트워크(906)를 통해 인터넷(910)에 액세스하도록 요구되지 않을 수 있다.

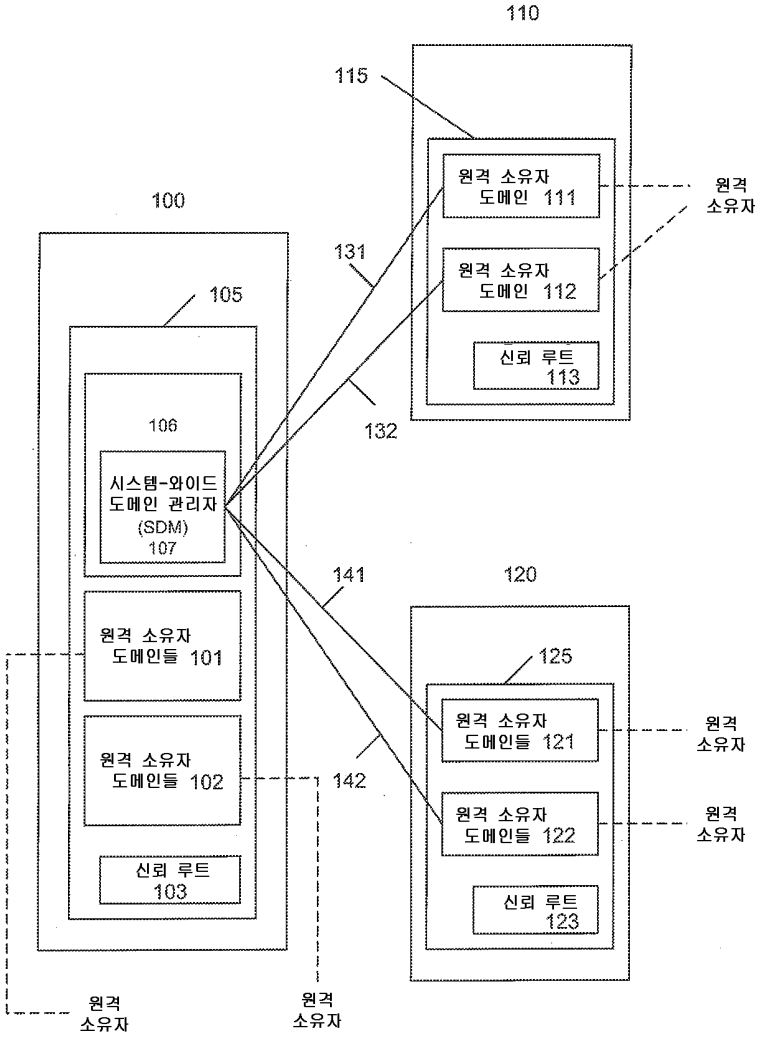
[0330] RAN(904)은 음성, 데이터, 애플리케이션, 및/또는 VoIP(voice over internet protocol) 서비스들을 WTRU들(902a, 902b, 902c, 902d) 중 하나 이상에 제공하도록 구성된 임의의 타입의 네트워크일 수 있는 코어 네트워크(906)와 통신할 수 있다. 예를 들어, 코어 네트워크(906)는 호 제어, 빌링 서비스(billing service)들, 모바일 위치-기반 서비스들, 사전-지불 전화걸기(pre-paid calling), 인터넷 연결, 비디오 분배 등을 제공할 수 있고 그리고/또는 사용자 인증과 같은 고-레벨 보안 기능들을 수행할 수 있다. 도 9에서 도시되지 않았지만, RAN(904), 및/또는 코어 네트워크(906)는 RAN(905)와 동일한 RAT 또는 상이한 RAT를 이용하는 다른 RAN들과 직접 또는 간접 통신할 수 있다는 것이 인지될 것이다. 예를 들어, E-UTRA 라디오 기술을 활용할 수 있는 RAN(904)에 연결되는 것 외에, 코어 네트워크(906)는 GSM 라디오 기술을 이용하는 다른 RAN(도시되지 않음)와도 통신할 수 있다.

[0331] 코어 네트워크(906)는 또한 PSTN(908), 인터넷(910) 및/또는 다른 네트워크들에 액세스하기 위해 WTRU들(902a, 902b, 902c, 902d)에 대한 게이트웨이로서 역할할 수 있다. PSTN(908)은 POTS(plain old telephone service)를 제공하는 회선-교환 전화 네트워크들을 포함할 수 있다. 인터넷(910)은 TCP/IP 인터넷 프로토콜 수트(internet protocol suite)의 전송 제어 프로토콜(TCP), 사용자 데이터그램 프로토콜(UDP), 및 인터넷 프로토콜(IP)과 같이 공통 통신 프로토콜들을 이용하는 상호연결된 컴퓨터 네트워크들 및 디바이스들의 전역 시스템을 포함할 수 있다. 네트워크들(912)은 다른 서비스 제공자들에 의해 소유 및/또는 운용되는 유선 또는 무선 통신 네트워크들을 포함할 수 있다. 예를 들어, 네트워크들(912)은 RAN(904)와 동일한 RAT 또는 상이한 RAT를 이용할 수 있는 하나 이상의 RAN들에 연결된 다른 코어 네트워크를 포함할 수 있다.

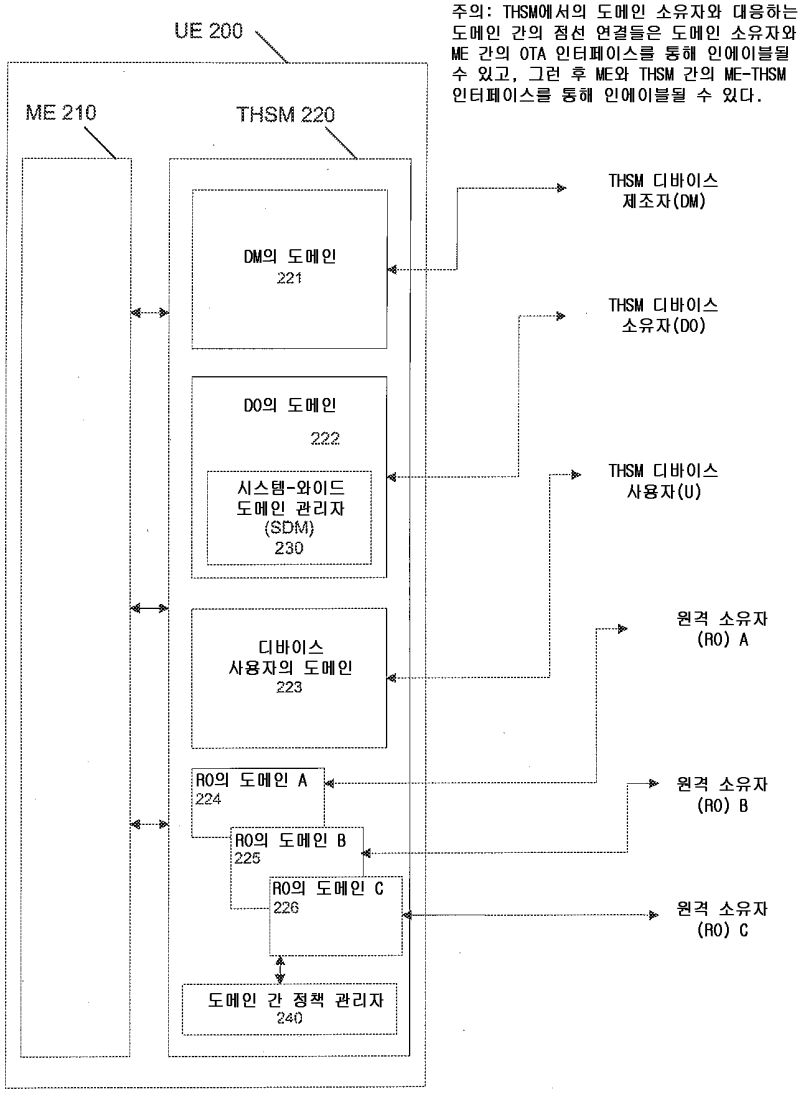
[0332] 통신 시스템(900) 내의 WTRU들(902a, 902b, 902c, 902d) 중 일부 또는 모두 다는 다중-모드 성능을 포함할 수 있는데, 즉, WTRU들(902a, 902b, 902c, 902d)은 상이한 무선 링크들을 통해 상이한 무선 네트워크들과 통신하기 위해 다수의 트랜시버들을 포함할 수 있다. 예를 들어, 도 9에 도시된 WTRU(902c)는 셀룰러-기반 라디오 기술을 이용할 수 있는 기지국과, 그리고 IEEE 802 라디오 기술을 이용할 수 있는 기지국과 통신하도록 구성될 수 있다.

도면

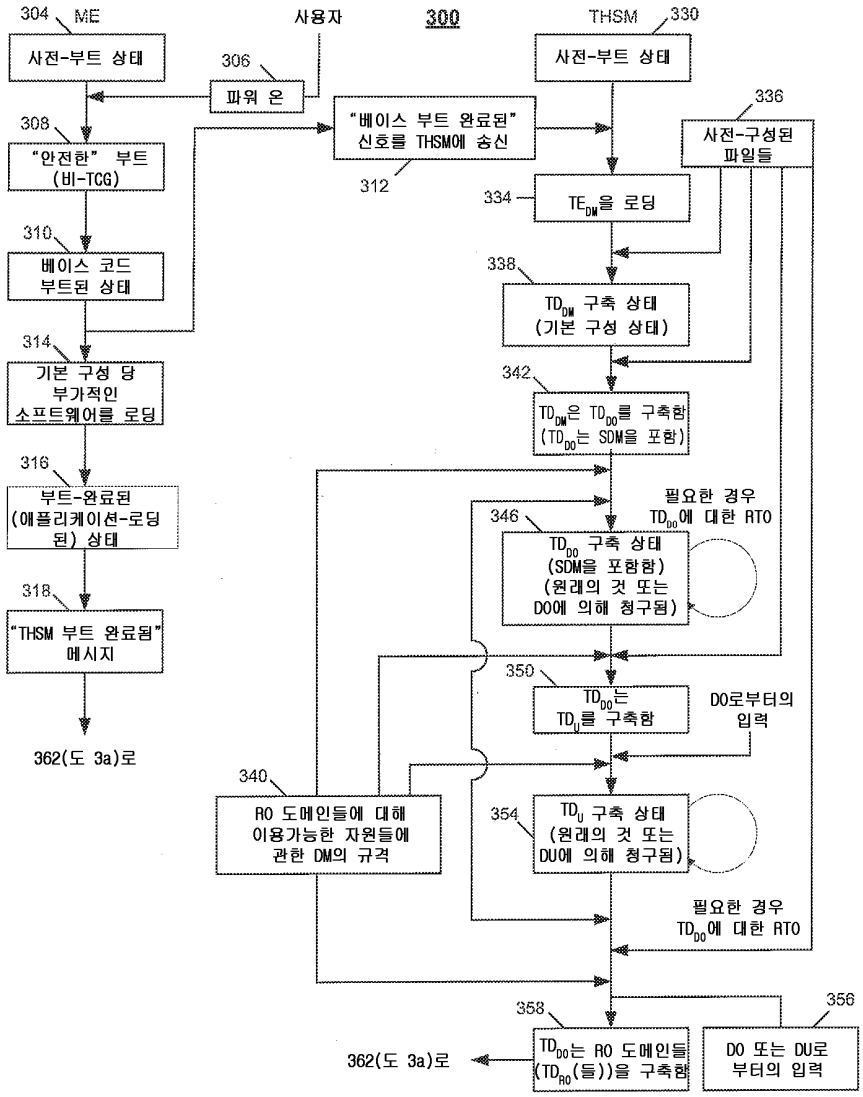
도면1


110
115
원격 소유자 도메인 111
원격 소유자
원격 소유자 도메인 112
신뢰 루트 113
131
132
100
105
106
시스템-와이드 도메인 관리자 (SDM) 107
원격 소유자 도메인들 101
원격 소유자 도메인들 102
신뢰 루트 103
141
142
120
125
원격 소유자 도메인들 121
원격 소유자
원격 소유자 도메인들 122
원격 소유자
신뢰 루트 123
원격 소유자
원격 소유자

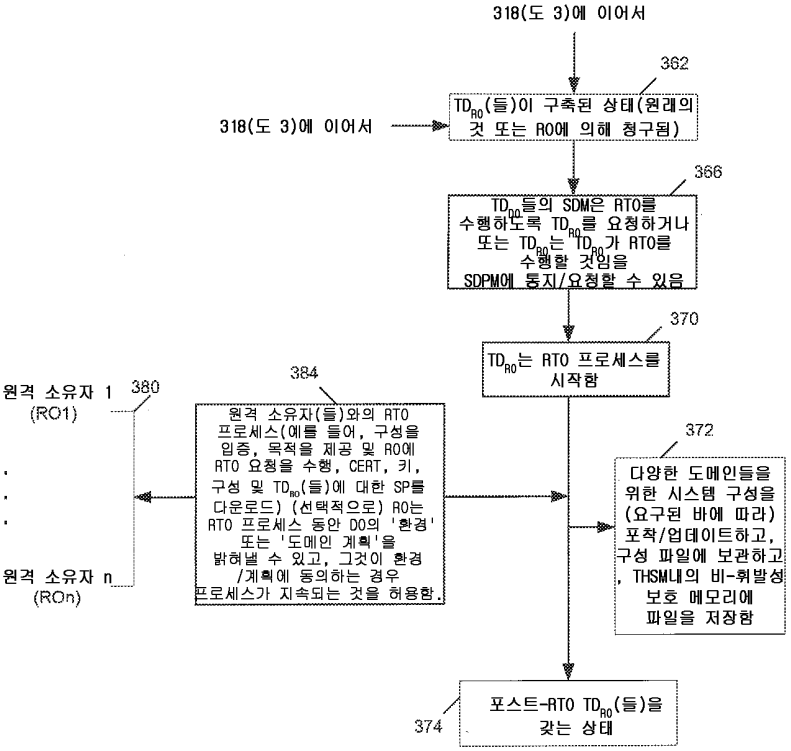
도면2


주의: THSM에서의 도메인 소유자와 대응하는 도메인 간의 점선 연결들은 도메인 소유자와 ME 간의 OTA 인터페이스를 통해 인에이블될 수 있고, 그런 후 ME와 THSM 간의 ME-THSM 인터페이스를 통해 인에이블될 수 있다.
UE 200
ME 210
THSM 220
DM의 도메인
221
DO의 도메인
222
시스템-와이드 도메인 관리자 (SDM)
230
디바이스 사용자의 도메인
223
RO의 도메인 A
224
RO의 도메인 B
225
RO의 도메인 C
226
도메인 간 정책 관리자
240
THSM 디바이스 제조자(DM)
THSM 디바이스 소유자(DO)
THSM 디바이스 사용자(U)
원격 소유자 (RO) A
원격 소유자 (RO) B
원격 소유자 (RO) C

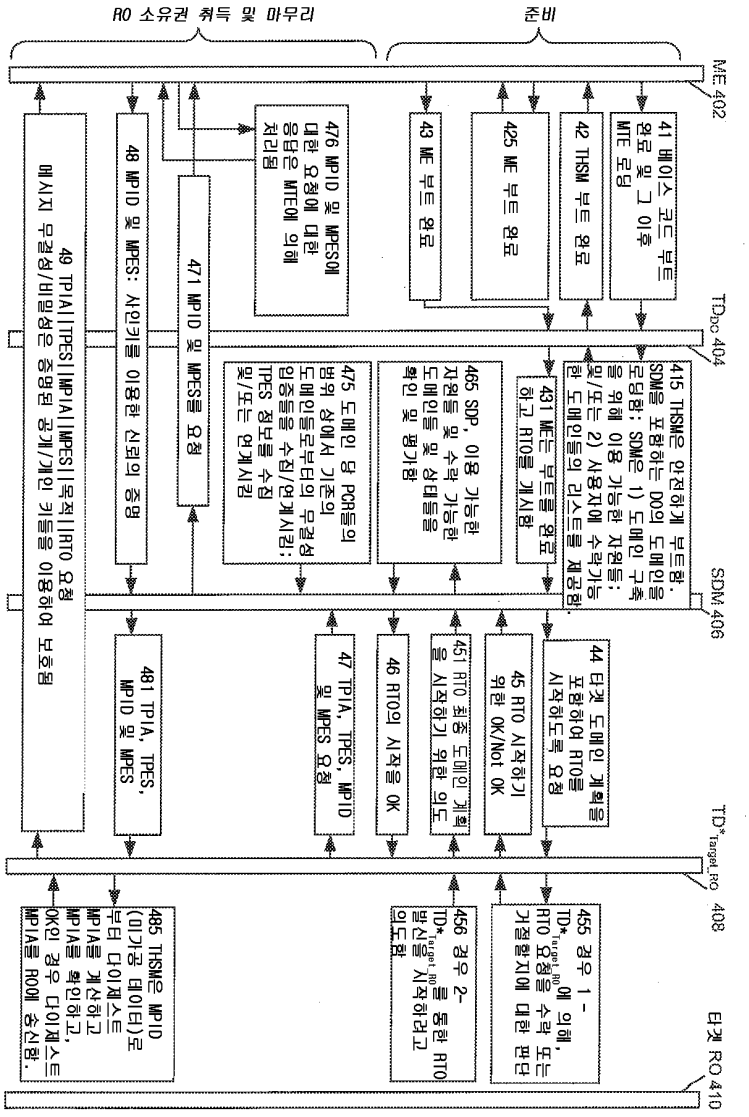
도면3


304
ME
사전-부트 상태
306
파워 온
사용자
300
THSM
330
사전-부트 상태
336
사전-구성된 파일들
308
"안전한" 부트 (비-TCG)
"베이스 부트 완료됨" 신호를 THSM에 송신
312
334
TE_DM을 로딩
310
베이스 코드 부트된 상태
338
TD_DM 구축 상태 (기본 구성 상태)
314
기본 구성 당 부가적인 소프트웨어를 로딩
342
TD_DM은 TD_DO를 구축함 (TD_DO는 SDM을 포함)
316
부트-완료된 (애플리케이션-로딩된) 상태
필요한 경우 TD_DO에 대한 RTO
346
TD_DO 구축 상태 (SDM을 포함함) (원래의 것 또는 DO에 의해 청구됨)
318
"THSM 부트 완료됨" 메시지
350
TD_DO는 TD_U를 구축함
DO로부터의 입력
362(도 3a)로
340
RO 도메인들에 대해 이용가능한 자원들에 관한 DM의 규격
354
TD_U 구축 상태 (원래의 것 또는 DU에 의해 청구됨)
필요한 경우 TD_DO에 대한 RTO
358
356
362(도 3a)로
TD_DO는 RO 도메인들 (TD_RO(들))을 구축함
DO 또는 DU로부터의 입력

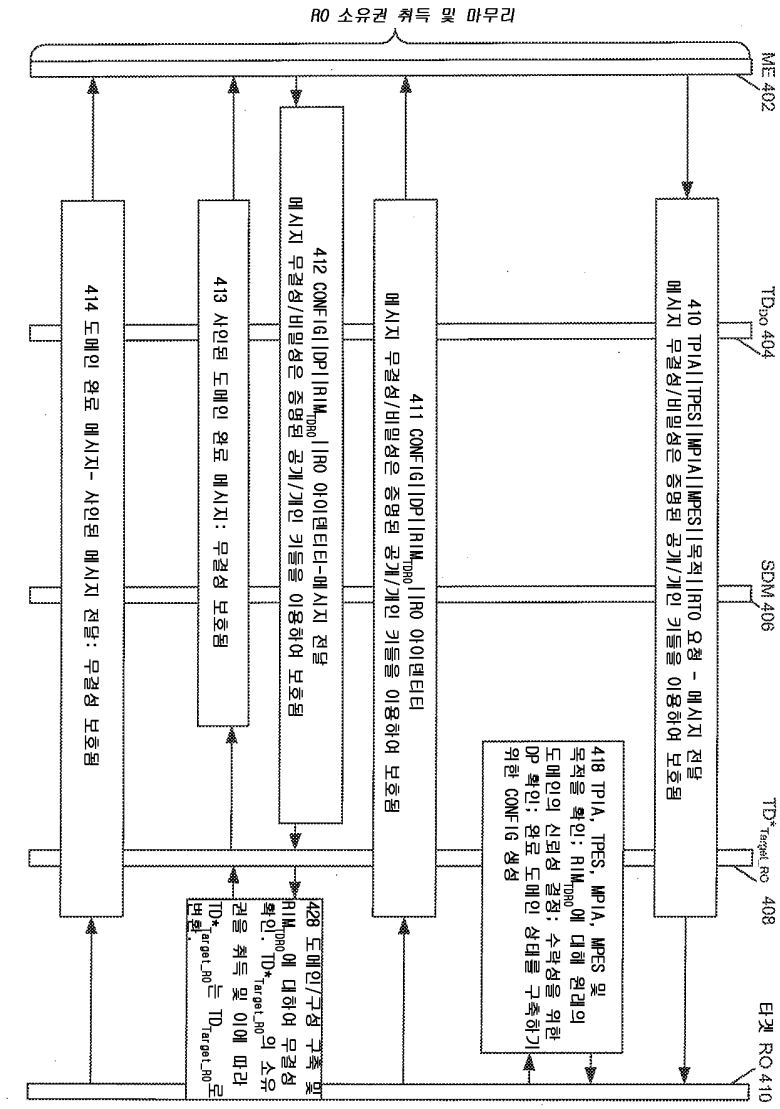
도면3a


318(도 3)에 이어서
362
TDRO(들)이 구축된 상태(원래의 것 또는 RO에 의해 청구됨)
318(도 3)에 이어서
366
TDRO들의 SDM은 RTO를 수행하도록 TDRO를 요청하거나 또는 TDRO는 TDRO가 RTO를 수행할 것임을 SDPM에 통지/요청할 수 있음
370
TDRO는 RTO 프로세스를 시작함
372
다양한 도메인들을 위한 시스템 구성을 (요구된 바에 따라) 포착/업데이트하고, 구성 파일에 보관하고, THSM내의 비-휘발성 보호 메모리에 파일을 저장함
384
원격 소유자(들)와의 RTO 프로세스(예를 들어, 구성을 입증, 목적을 제공 및 RO에 RTO 요청을 수행, CERT, 키, 구성 및 TDRO(들)에 대한 SP를 다운로드) (선택적으로) RO는 RTO 프로세스 동안 DO의 '환경' 또는 '도메인 계획'을 밝혀낼 수 있고, 그것이 환경/계획에 동의하는 경우 프로세스가 지속되는 것을 허용함.
380
원격 소유자 1 (RO1)
원격 소유자 n (ROn)
374
포스트-RTO TDRO(들)을 갖는 상태

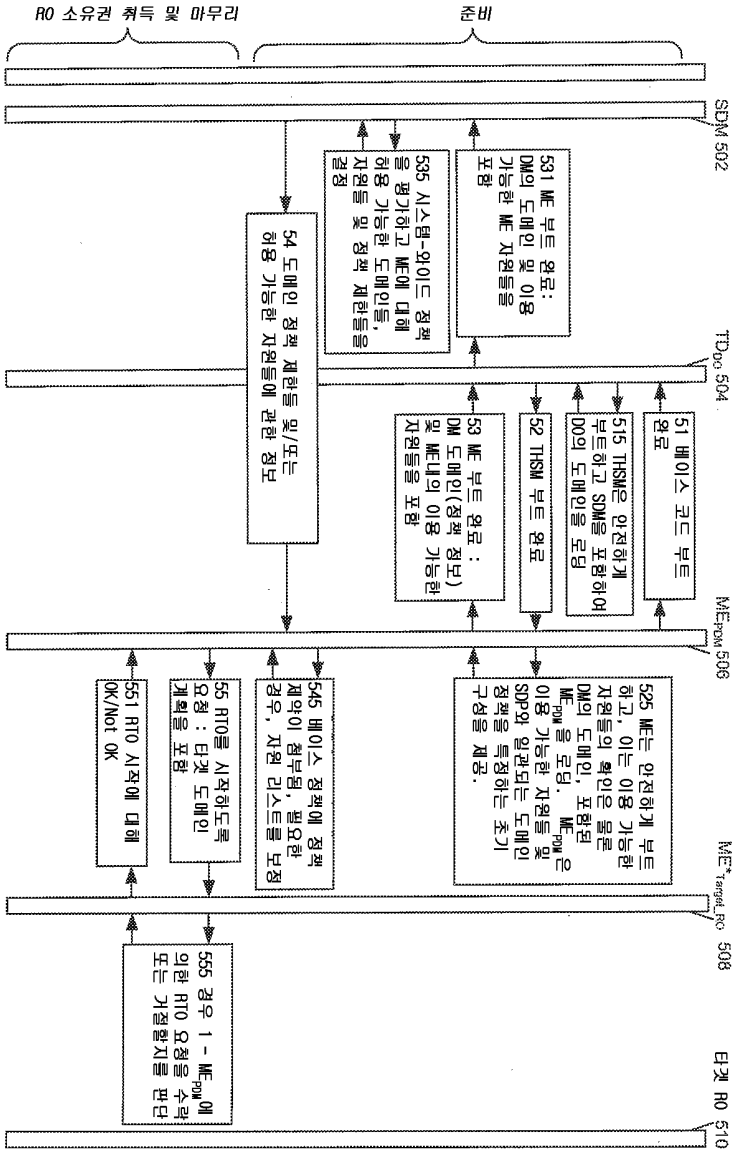
도면4


RO 소유권 취득 및 마무리
준비
ME 402
TD_DC 404
SDM 406
TD*_Target_RO 408
타겟 RO 410
41 베이스 코드 부트 완료 및 그 이후 MTE 로딩
42 THSM 부트 완료
425 ME 부트 완료
43 ME 부트 완료
476 MPID 및 MPES에 대한 요청에 대한 응답은 MTE에 의해 처리됨
48 MPID 및 MPES: 사인키를 이용한 신뢰의 증명
471 MPID 및 MPES를 요청
49 TPIA||TPES||MPIA||MPES||묵적||RTO 요청
메시지 무결성/비밀성은 증명된 공개/개인 키들을 이용하여 보호됨
415 THSM은 안전하게 부트함; SDM을 포함하는 DD의 도메인을 로딩함; SDM은 1) 도메인 구축을 위해 이용 가능한 자원들; 및/또는 2) 사용자에 수락가능한 도메인들의 리스트를 제공함.
431 ME는 부트를 완료하고 RTO를 개시함
475 도메인 당 PCR들의 범위 상에서 기초의 도메인들로부터의 무결성 인증들을 수집/연계시킴; TPES 정보를 수집 및/또는 연계시킴
465 SDP, 이용 가능한 자원들 및 수락 가능한 도메인들 및 상태들을 확인 및 평가함
44 타겟 도메인 계획을 포함하여 RTO를 시작하도록 요청
45 RTO 시작하기 위한 OK/Not OK
451 RTO 최종 도메인 계획을 시작하기 위한 의도
47 TPIA, TPES, MPID 및 MPES 요청
46 RTO의 시작을 OK
481 TPIA, TPES, MPID 및 MPES
455 경우 1 - TD*Target_RO에 의해, RTO 요청을 수락 또는 거절할지에 대한 판단
456 경우 2- TD*Target_RO를 통한 RTO 발신을 시작하려고 의도함
485 THSM은 MPID (미가공 데이터)로부터 다이제스트 MPIA를 계산하고 MPIA를 확인하고, OK인 경우 다이제스트 MPIA를 ROOM 송신함.

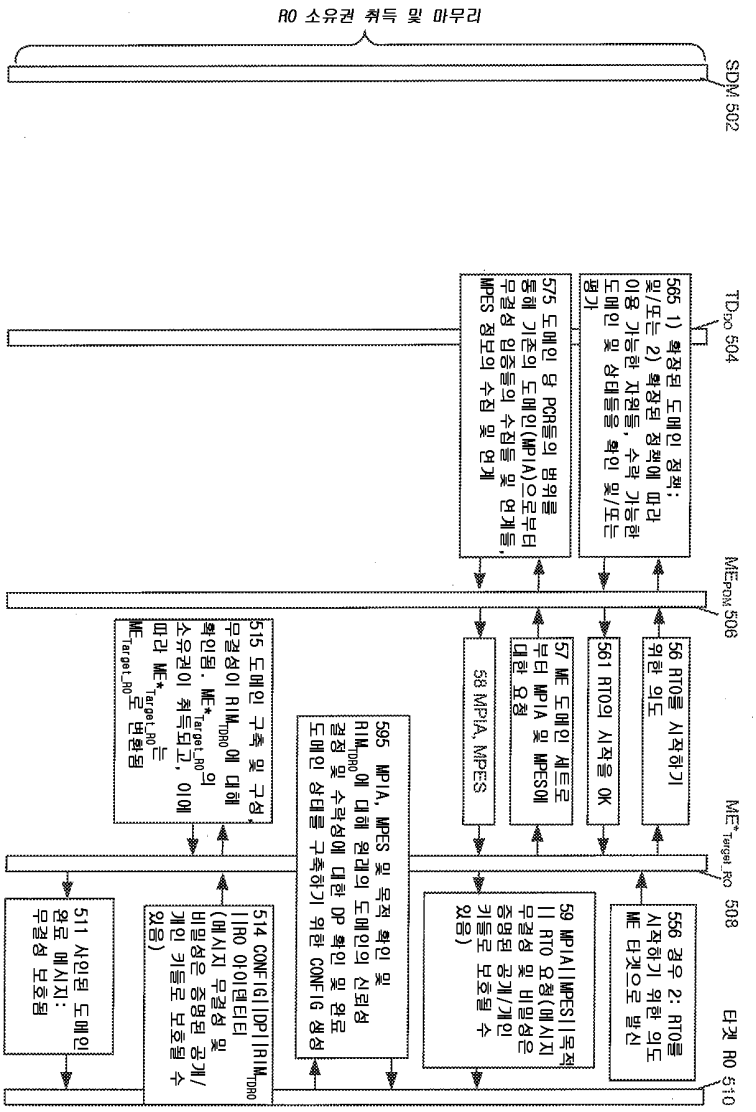
도면4a


RO 소유권 취득 및 마무리
ME 402
TD_DO 404
SDM 406
TD*_Target_RO 408
타겟 RO 410
410 TPIA | TPES | MPIA | MPES | 목적 | RTO 요청 - 메시지 전달
메시지 무결성/비밀성은 중앙된 공개/개인 키들을 이용하여 보호됨
411 CONFIG | DP | RIM_DRO | RO 아이덴티티
메시지 무결성/비밀성은 중앙된 공개/개인 키들을 이용하여 보호됨
412 CONFIG | DP | RIM_DRO | RO 아이덴티티-메시지 전달
메시지 무결성/비밀성은 중앙된 공개/개인 키들을 이용하여 보호됨
413 사인된 도메인 완료 메시지: 무결성 보호됨
414 도메인 완료 메시지- 사인된 메시지 전달: 무결성 보호됨
418 TPIA, TPES, MPIA, MPES 및 목적을 확인; RIM_DRO에 대해 원래의 도메인의 신뢰성 결정; 수락성을 위한 DP 확인; 완료 도메인 상태를 구축하기 위한 CONFIG 생성
428 도메인/구성 구축 및 RIM_DRO에 대하여 무결성 확인. TD*_Target_RO의 소유권을 취득 및 이에 따라 TD*_Target_RO는 TD_Target_RO로 변환.

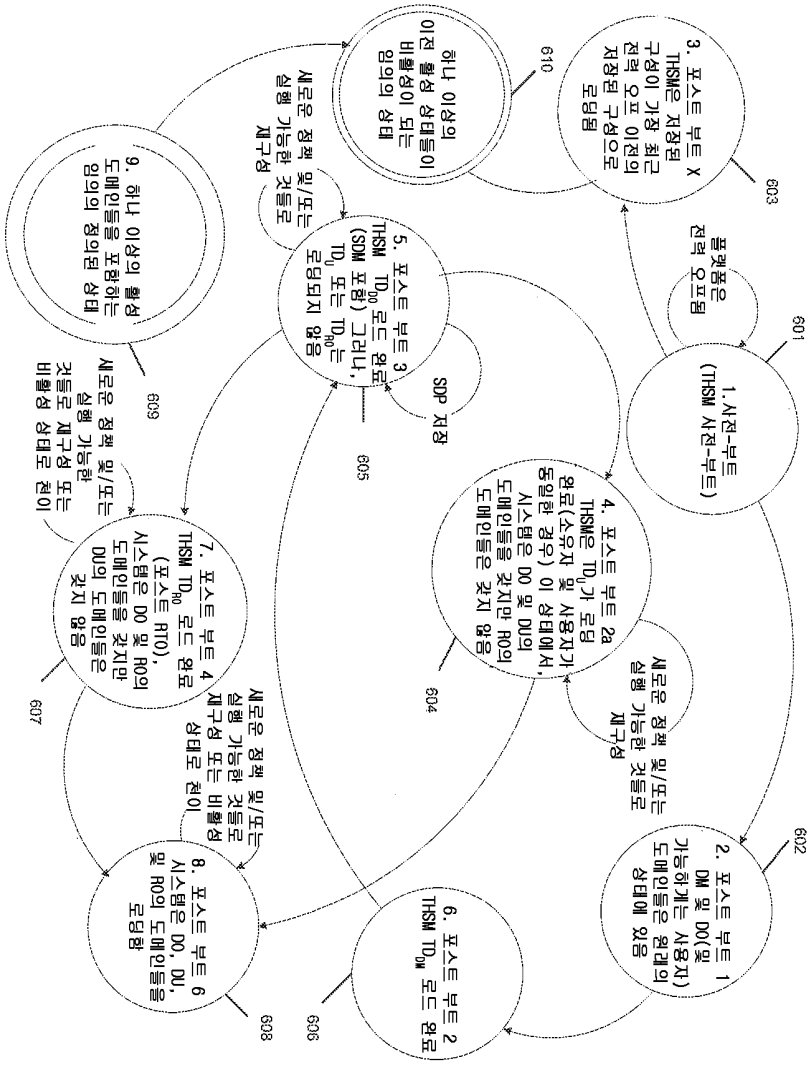
도면5


RO 소유권 취득 및 마무리
준비
SDM 502
TDDC 504
MEPDM 506
METarget_RO 508
타겟 RO 510
531 ME 부트 완료: DM의 도메인 및 이용 가능한 ME 자원들을 포함
535 시스템-와이드 정책을 평가하고 ME에 대해 허용 가능한 도메인들, 자원들 및 정책 제한들을 결정
54 도메인 정책 제한들 및/또는 허용 가능한 자원들에 관한 정보
51 베이스 코드 부트 완료
515 THSM은 안전하게 부트하고 SDM을 포함하여 DD의 도메인을 로딩
52 THSM 부트 완료
53 ME 부트 완료 : DM 도메인(정책 정보) 및 ME내의 이용 가능한 자원들을 포함
525 ME는 안전하게 부트하고, 이는 이용 가능한 자원들의 확인을 돕고 DM의 도메인, 포함된 MEPDM 을 로딩. MEPDM 은 이용 가능한 자원들 및 SDF와 일관되는 도메인 정책을 특정하는 초기 구성을 제공.
545 베이스 정책에 정책 제약이 철부됨, 필요한 경우, 자원 리스트를 보정
55 RTO를 시작하도록 요청 : 타겟 도메인 계획을 포함
551 RTO 시작에 대해 OK/Not OK
555 경우 1 - MEPDM 에 의한 RTO 요청을 수락 또는 거절할지를 판단

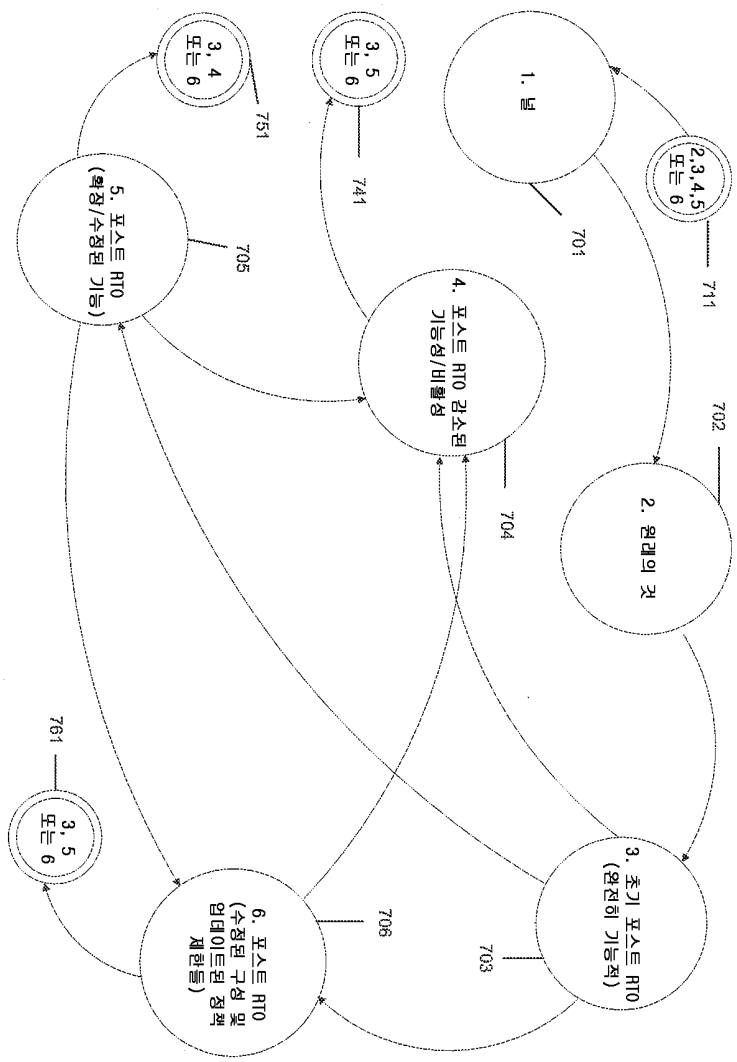
도면5a


RO 소유권 취득 및 마무리
SDM 502
TDpo 504
MEPDM 506
ME*Target_RO 508
타겟 RO 510
565 1) 확장된 도메인 정책; 및/또는 2) 확장된 정책에 따라 이용 가능한 자원을, 수락 가능한 도메인 및 상태들을 확인 및/또는 평가
575 도메인 당 PDR들의 범위를 통해 기준의 도메인(MPIA)으로부터 무결성 입증들의 수집들 및 연계들, MPES 정보의 수집 및 연계
56 RTO를 시작하기 위한 의도
561 RTO의 시작을 OK
57 ME 도메인 세트로부터 MPIA 및 MPES에 대한 요청
58 MPIA, MPES
556 경우 2: RTO를 시작하기 위한 의도 ME 타겟으로 발신
59 MPIA||MPES||목적||RTO 요청(메시지 무결성 및 비밀성은 증명된 공개/개인 키들로 보호될 수 있음)
595 MPIA, MPES 및 목적 확인 및 RIM_TDPO에 대해 원래의 도메인의 신뢰성 결정 및 수락성에 대한 DP 확인 및 완료 도메인 상태를 구축하기 위한 CONFIG 생성
515 도메인 구축 및 구성; 무결성이 RIM_TDPO에 대해 확인됨. ME*_Target_RO의 소유권이 취득되고, 이에 따라 ME*_Target_RO는 ME_Target_RO로 변환됨
514 CONFIG||DPI||RIM_TDPO||RO 아이덴티티 (메시지 무결성 및 비밀성은 증명된 공개/개인 키들로 보호될 수 있음)
511 사인된 도메인 용료 메시지: 무결성 보호됨

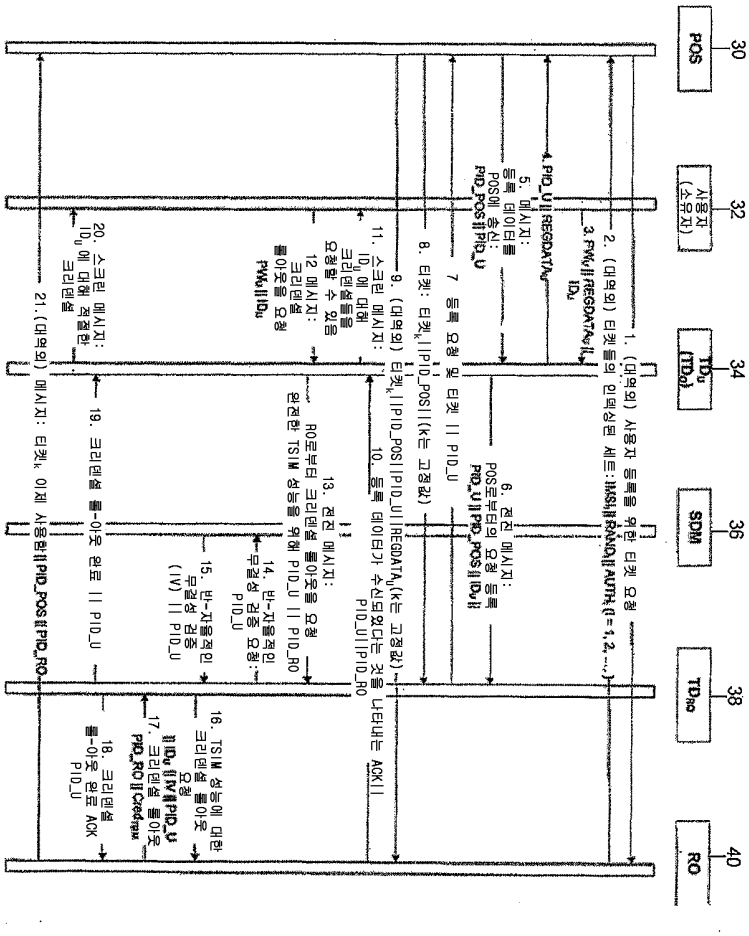
도면6


1.사전-부트
(THSM 사전-부트)
601
2. 포스트 부트 1
DM 및 DO(및 가능하게는 사용자) 도메인들은 원래의 상태에 있음
602
3. 포스트 부트 X
THSM은 저장된 구성이 가장 최근 전력 오프 이전의 저장된 구성으로 로딩됨
603
4. 포스트 부트 2a
THSM은 TDi가 로딩 완료(소유자 및 사용자가 동일한 경우) 이 상태에서, 시스템은 DO 및 DU의 도메인들을 갖지만 RO의 도메인들은 갖지 않음
604
5. 포스트 부트 3
THSM TDPB (SDM 포함) TDi 로딩되지 않음
605
6. 포스트 부트 2
THSM TDPB 로드 완료
606
7. 포스트 부트 4
THSM TDPB 로드 완료
(포스트 RTO), 시스템은 DO 및 RO의 도메인들을 갖지만 DU의 도메인들은 갖지 않음
607
8. 포스트 부트 6
시스템은 DO, DU, 및 RO의 도메인들을 로딩함
608
9. 하나 이상의 활성 도메인들을 표현하는 임의의 정의된 상태
609
하나 이상의 비활성 상태들이 되는 임의의 상태
610
플랫폼은 전력 오프됨
SDP 저장
새로운 정책 및/또는 실행 가능한 것들로 재구성
새로운 정책 및/또는 실행 가능한 것들로 재구성
새로운 정책 및/또는 실행 가능한 것들로 재구성 또는 비활성 상태로 천이
새로운 정책 및/또는 실행 가능한 것들로 재구성 또는 비활성 상태로 천이

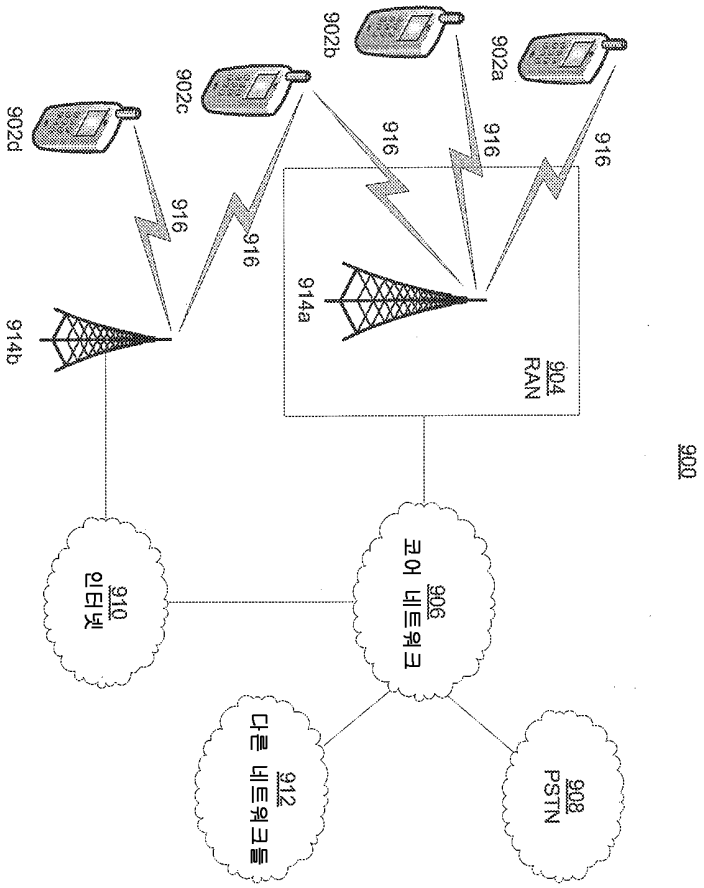
도면7


1. 널
2. 원래의 것
3. 초기 포스트 RTO (완전히 기능적)
4. 포스트 RTO 감소된 기능성/비활성
5. 포스트 RTO (확장/수정된 기능)
6. 포스트 RTO (수정된 구성 및 업데이트된 정책 제한들)
2,3,4,5 또는 6
3, 5 또는 6
3, 4 또는 6
3, 5 또는 6
701
702
703
704
705
706
711
741
751
761

도면8


POS
30
사용자 (소유자)
32
TD_U (TD_0)
34
SDM
36
TD_RO
38
RO
40
1. (대역외) 사용자 등록을 위한 티켓 요청
2. (대역외) 티켓 들의 인덱싱된 세트: {AS_i || RANDA_i || AUTH_i (i = 1, 2, ...)}
3. FW_0 || REGDATA_0 || ID_U
4. PID_U || REGDATA_0
5. 메시지: 등록 데이터를 POS에 송신: PID_POS || PID_U
6. 전진 메시지: POS로부터의 요청 등록 PID_U || PID_POS || ID_U ||
7 등록 요청 된 티켓 || PID_U
8. 티켓: 티켓_k || PID_POS || (k는 고정값)
9. (대역외) 티켓_k || PID_POS || PID_U || REGDATA_0 (k는 고정값)
10. 등록 데이터가 수신되었다는 것을 나타내는 ACK ||
PID_U || PID_RO
11. 스크린 메시지: ID_0 에 대해 크리덴셜들을 요청할 수 있음
12 메시지: 크리덴셜 롤아웃을 요청 FW_0 || ID_U
13. 전진 메시지: RO로부터 크리덴셜 롤아웃을 요청
완전한 TSIM 성능을 위해 PID_U || PID_RO
14. 반-자율적인 무결성 검증 요청: PID_U
15. 반-자율적인 무결성 검증 (V) || PID_U
16. TSIM 성능에 대한 크리덴셜 롤아웃 요청
17. ID_0 || IV || PID_U || 크리덴셜 롤아웃 PID_RO || Cred_FEM
18. 크리덴셜 롤-아웃 완료 ACK PID_U
19. 크리덴셜 롤-아웃 완료 || PID_U
20. ID_0 에 대해 적절한 크리덴셜 스크린 메시지:
21.(대역외) 메시지: 티켓_k 이제 사용됨 || PID_POS || PID_RO

도면9


902a
902b
902c
902d
916
916
916
916
916
914a
914b
904
RAN
900
910
인터넷
906
코어 네트워크
912
다른 네트워크들
908
PSTN