(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년07월08일
(11) 등록번호 10-1535361
(24) 등록일자 2015년07월02일

(51) 국제특허분류(Int. Cl.)
H04W 8/20 (2009.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2013-7013622
(22) 출원일자(국제) 2011년10월20일
심사청구일자 2013년05월28일
(85) 번역문제출일자 2013년05월28일
(65) 공개번호 10-2014-0012950
(43) 공개일자 2014년02월04일
(86) 국제출원번호 PCT/US2011/057156
(87) 국제공개번호 WO 2012/058099
국제공개일자 2012년05월03일
(30) 우선권주장
13/079,614 2011년04월04일 미국(US)
61/407,861 2010년10월28일 미국(US)
(56) 선행기술조사문헌
US20100210304 A1*
KR1020100050565 A*
US06836670 B2*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
애플 인크.
미합중국 95014 캘리포니아 쿠퍼티노 인피니트 루프 1
(72) 발명자
셸, 스테판, 브이.
미국 95014 캘리포니아주 쿠퍼티노 엠에스 35-2엠피 인피니트 루프 1
하거티, 데이비드, 티.
미국 95014 캘리포니아주 쿠퍼티노 엠에스 87-2씨지에스 인피니트 루프 1
(74) 대리인
김봉섭, 양영준, 백만기

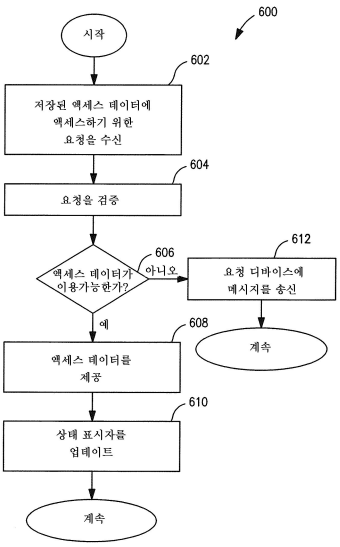
전체 청구항 수 : 총 18 항 심사관 : 이종익

(54) 발명의 명칭 **다중 액세스 제어 엔티티에 대한 관리 시스템**

(57) 요 약

다수의 사용자 액세스 제어 엔티티 또는 클라이언트를 관리하기 위한 방법 및 장치. 예를 들어, 일 실시예에서, eSIM(electronic subscriber identity module)들의 "지갑"은 사용자 디바이스에 저장 및 사용될 수 있고 그리고/또는 다른 디바이스에서의 사용을 위해 다른 디바이스들에 분배될 수 있다. 또 다른 실시예에서, 네트워킹된 서버가 그와 통신하고 있는 복수의 사용자 디바이스에 eSIM을 저장하고 분배할 수 있다. 특정 eSIM에 대한 요청이 프로세싱될 수 있게 하고 그것의 분배에 대한 다양한 규칙들이 구현될 수 있게 하는 이용가능한 eSIM의 데이터베이스가 지갑 엔티티에 그리고/또는 네트워크에 유지된다. 데이터가 사용자와 네트워크 통신 사업자 모두에 특정한 데이터가 네트워킹된 엔티티들 사이에서 전송될 때 그 데이터를 보호하기 위한 보안 예방책들이 구현된다. eSIM 백업 및 복원을 위한 솔루션들도 기술되어 있다.

대 표 도 - 도6


600
시작
602
저장된 액세스 데이터에
액세스하기 위한
요청을 수신
604
요청을 검증
606
액세스 데이터가
이용가능한가?
아니오
612
요청 디바이스에
메시지를 송신
계속
예
608
액세스 데이터를
제공
610
상태 표시자를
업데이트
계속

명 세 서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

eSIM(electronic Subscriber Identity Module)들을 교환(swap)하기 위한 방법으로서,

데이터베이스에 저장된 이용가능(available)한 eSIM들의 선택가능한 리스트를, 모바일 디바이스로, 전송하는 단계;

상기 모바일 디바이스 - 상기 모바일 디바이스는 복수의 eSIM을 저장할 수 있음 - 로부터, 상기 모바일 디바이스에 의해 저장된 제1 eSIM을 상기 eSIM들의 리스트 내의 제2 eSIM과 교환하기 위한 요청을 수신하는 단계;

상기 제2 eSIM이 상기 모바일 디바이스에 이용가능한지 여부를 결정하기 위해서 상기 데이터베이스를 이용(utilize)하는 단계; 및

상기 제2 eSIM이 상기 모바일 디바이스에 이용가능한 경우:

상기 모바일 디바이스로부터 상기 제1 eSIM을 수신하는 단계;

상기 모바일 디바이스로부터 상기 제1 eSIM이 제거되도록 하는 단계;

상기 모바일 디바이스로 상기 제2 eSIM을 전송하는 단계; 및

상기 교환을 반영하기 위하여, 상기 제1 eSIM 및 상기 제2 eSIM의 각각에 대해서, 상기 데이터베이스 내에 포함된 개별 상태 식별자를 업데이트하는 단계

를 포함하는 방법.

청구항 8

삭제

청구항 9

제7항에 있어서,

상기 제2 eSIM이 상기 모바일 디바이스에 이용가능한지 여부를 결정하는 것은 상기 개별 상태 식별자가 업데이

트되기 전에 상기 제2 eSIM에 대한 상기 개별 상태 식별자를 체크하는 것을 포함하는, 방법.

청구항 10

제7항에 있어서,

상기 제2 eSIM이 상기 모바일 디바이스에 이용가능한지 여부를 결정하는 것은 상기 제2 eSIM에 의해 제공되는 서비스 레벨에 대한 액세스를 허용하는 가입(subscription)과 상기 모바일 디바이스가 연관되어 있는지 여부를 결정하는 것을 포함하는, 방법.

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

모바일 디바이스와 통신하도록 구성된 원격 디바이스로서 - 상기 모바일 디바이스는 여러 개의 eSIM들을 저장할 수 있음 - ,

복수의 eSIM을 저장하도록 구성된 저장 장치; 및

프로세서를 포함하고,

상기 프로세서는,

상기 복수의 eSIM에 기초하여, 상기 모바일 디바이스에 의한 사용이 가능한 eSIM들의 리스트를 생성하는 단계;

상기 모바일 디바이스로 상기 eSIM들의 리스트를 전송하는 단계;

상기 모바일 디바이스로부터, 상기 eSIM들의 리스트 내에 포함된 eSIM에 액세스하기 위한 요청을 수신하는 단계;

상기 모바일 디바이스로 상기 eSIM을 전송하는 단계; 및

상기 eSIM이 상기 모바일 디바이스에 의해 저장되었다는 것을 표시하기 위해 상기 eSIM과 연관된 상태 식별자를 업데이트하는 단계를 포함하는 단계들을 수행하도록 구성되는,

원격 디바이스.

청구항 16

제15항에 있어서,

상기 eSIM들의 리스트는 상기 모바일 디바이스에 액세스 가능하고 상기 eSIM들의 리스트 내에 포함된 각 eSIM에 의해 제공되는 서비스 레벨들에 기초하여 생성되는, 원격 디바이스.

청구항 17

제15항에 있어서,

상기 상태 식별자는 상기 eSIM이 다른 모바일 디바이스들에 의한 사용이 가능하지 않다는 것을 표시하기 위해

업데이트되는, 원격 디바이스.

청구항 18

제15항에 있어서,

상기 단계들은,

상기 eSIM을 복귀시키기 위한 요청을 상기 모바일 디바이스로부터 수신하는 단계; 및

상기 eSIM을 복귀시키기 위한 요청의 수신에 응답하여, 상기 eSIM이 다른 모바일 디바이스들에 의한 사용이 가능하다는 것을 표시하기 위해 상기 상태 식별자를 업데이트하는 단계를 더 포함하는, 원격 디바이스.

청구항 19

제15항에 있어서,

상기 단계들은,

상기 eSIM을 복귀시키도록 상기 모바일 디바이스에게 명령하는 단계; 및

상기 eSIM을 복귀시키기 위한 명령에 응답하여, 상기 eSIM이 다른 모바일 디바이스들에 의한 사용이 가능하다는 것을 표시하기 위해 상기 상태 식별자를 업데이트하는 단계를 더 포함하는, 원격 디바이스.

청구항 20

제19항에 있어서,

상기 단계들은,

상기 상태 식별자를 업데이트하는 단계 전에, 상기 모바일 디바이스에서 상기 eSIM의 동작이 디스에이블되었는지를 검증하는 단계를 더 포함하는, 원격 디바이스.

청구항 21

명령어들을 저장하는 비-일시적인(non-transitory) 컴퓨터 판독 가능한 저장 매체로서, 상기 명령어들은, 원격 디바이스 내에 포함된 프로세서에 의해 실행될 때, 상기 원격 디바이스에 의해 관리되는 데이터베이스에 저장된 복수의 eSIM에 모바일 디바이스가 액세스할 수 있게 하기 위하여,

상기 모바일 디바이스에 대해 액세스 가능한 상기 복수의 eSIM 중 하나 이상의 eSIM들의 리스트를 생성하는 단계 - 상기 모바일 디바이스는 여러 개의 eSIM들을 저장할 수 있음 - ;

상기 모바일 디바이스로, 상기 복수의 eSIM 중 하나 이상의 eSIM들의 리스트를 전송하는 단계;

상기 모바일 디바이스로부터, 상기 리스트 내에 포함된 상기 eSIM들 중 적어도 하나의 eSIM에 액세스하기 위한 요청을 수신하는 단계;

상기 모바일 디바이스로, 상기 요청된 적어도 하나의 eSIM을 전송하는 단계; 및

상기 적어도 하나의 eSIM에 대해서, 상기 모바일 디바이스로의 상기 적어도 하나의 eSIM의 상기 전송을 반영하기 위하여 상기 데이터베이스 내에 포함된 개별 상태 식별자를 업데이트하는 단계를 포함하는 단계들을 수행하는,

비-일시적인 컴퓨터 판독 가능한 저장 매체.

청구항 22

제21항에 있어서,

상기 리스트를 생성하는 단계는, 상기 복수의 eSIM 중의 각 eSIM - 상기 각 eSIM의 개별 상태 식별자는 상기 모바일 디바이스가 상기 eSIM에 액세스할 수 있도록 허가된 것을 표시함 - 을 상기 리스트에 더하는 단계를 포함하는, 비-일시적인 컴퓨터 판독 가능한 저장 매체.

청구항 23

제21항에 있어서,

상기 단계들은,

이벤트의 발생에 응답하여:

상기 모바일 디바이스로부터 상기 적어도 하나의 eSIM이 제거되도록 하는 단계; 및

상기 모바일 디바이스로부터 상기 적어도 하나의 eSIM이 제거되는 것을 반영하기 위하여 상기 적어도 하나의 eSIM의 상기 개별 상태 식별자를 업데이트하는 단계를 더 포함하는, 비-일시적인 컴퓨터 판독 가능한 저장 매체.

청구항 24

제21항에 있어서,

상기 단계들은,

제2 모바일 디바이스로부터 상기 요청된 eSIM에 액세스하기 위한 제2 요청을 수신하는 단계; 및

상기 개별 상태 식별자에 적어도 부분적으로 기초하여, 상기 제2 모바일 디바이스에 상기 요청된 eSIM이 제공될 수 있는지 여부를 결정하는 단계를 더 포함하는, 비-일시적인 컴퓨터 판독 가능한 저장 매체.

청구항 25

원격 디바이스와 통신하도록 구성된 모바일 디바이스로서 - 상기 원격 디바이스는 복수의 eSIM을 저장하고 관리하도록 구성됨 - ,

여러 개의 eSIM들을 저장하도록 구성된 저장 장치; 및

프로세서를 포함하고,

상기 프로세서는,

상기 원격 디바이스로부터, 상기 원격 디바이스에 의해 저장된 상기 복수의 eSIM 중 적어도 하나의 eSIM을 포함하는 eSIM들의 리스트를 수신하는 단계 - 상기 적어도 하나의 eSIM은 상기 모바일 디바이스 상의 사용을 위해 다운로드 가능함 - ;

상기 원격 디바이스로, 상기 적어도 하나의 eSIM을 다운로드하기 위한 요청을 전송하는 단계;

상기 원격 디바이스로부터, 상기 적어도 하나의 eSIM을 다운로드하는 단계; 및

상기 원격 디바이스로 하여금, 상기 적어도 하나의 eSIM은 다른 모바일 디바이스들 상의 사용을 위해 다운로드 가능하지 않은 것을 표시하기 위해 상기 적어도 하나의 eSIM과 관련된 정보를 업데이트하도록 하는 단계를 포함하는 단계들을 수행하도록 구성되는,

모바일 디바이스.

청구항 26

제25항에 있어서,

상기 단계들은,

상기 모바일 디바이스의 사용자가 무선 서비스들에 액세스할 수 있게 하도록 상기 적어도 하나의 eSIM을 사용하는 단계를 더 포함하는, 모바일 디바이스.

청구항 27

제25항에 있어서,

상기 단계들은,

상기 원격 디바이스로 상기 적어도 하나의 eSIM을 복귀시키기 위한 요청을 상기 원격 디바이스로 전송하는 단계; 및

상기 원격 디바이스로 하여금, 상기 적어도 하나의 eSIM은 다른 모바일 디바이스들 상의 사용을 위해 다운로드 가능하다는 것을 표시하기 위해 상기 적어도 하나의 eSIM과 관련된 정보를 업데이트하게 하는 단계를 더 포함하는, 모바일 디바이스.

청구항 28

제25항에 있어서,

상기 단계들은,

상기 원격 디바이스로 상기 적어도 하나의 eSIM을 복귀시키기 위한 명령을 상기 원격 디바이스로부터 수신하는 단계; 및

상기 원격 디바이스로 하여금, 상기 적어도 하나의 eSIM을 수신한 때, 상기 적어도 하나의 eSIM이 다른 모바일 디바이스들 상의 사용을 위해 다운로드 가능하다는 것을 표시하기 위해 상기 적어도 하나의 eSIM과 관련된 정보를 업데이트하게 하는 단계를 더 포함하는, 모바일 디바이스.

청구항 29

제28항에 있어서,

상기 원격 디바이스로 상기 적어도 하나의 eSIM을 복귀시키는 것은,

상기 모바일 디바이스에서 상기 eSIM을 디스에이블시키는 것; 또는

상기 eSIM을 상기 원격 디바이스로 전송하고 상기 모바일 디바이스로부터 상기 eSIM을 삭제하는 것을 포함하는, 모바일 디바이스.

발명의 설명

기 술 분 야

[0001] 우선권 및 관련 출원들

[0002] 이 출원은, "MANAGEMENT SYSTEMS FOR MULTIPLE ACCESS CONTROL ENTITIES"라는 명칭으로 2010년 10월 28일에 출원된 미국 가 특허 출원 일련 제61/407,861호에 대한 우선권을 청구하는, "MANAGEMENT SYSTEMS FOR MULTIPLE ACCESS CONTROL ENTITIES"라는 명칭으로 2011년 4월 4일에 출원된 미국 특허 출원 일련 제13/079,614호에 대한 우선권을 청구하며, 이들 각각은 그 전체 내용이 참조로 여기에 포함된다.

[0003] 이 출원은 또한 공동 소유되고 공동 계류중인, "WIRELESS NETWORK AUTHENTICATION APPARATUS AND METHODS"라는 명칭으로 2010년 11월 22일에 출원된 미국 특허 출원 일련 제12/952,082호, "APPARATUS AND METHODS FOR PROVISIONING SUBSCRIBER IDENTITY DATA IN A WIRELESS NETWORK"라는 명칭으로 2010년 11월 22일에 출원된 제12/952,089호, "VIRTUAL SUBSCRIBER IDENTITY MODULE DISTRIBUTION SYSTEM"이라는 명칭으로 2010년 12월 28일에 출원된 제12/980,232호, 및 "POSTPONED CARRIER CONFIGURATION"라는 명칭으로 2009년 1월 13일에 출원된 제12/353,227호, 및 "METHODS AND APPARATUS FOR ACCESS CONTROL CLIENT ASSISTED ROAMING"이라는 명칭으로 2010년 10월 28일에 출원된 미국 가 특허출원 일련 제61/407,858호, "METHODS AND APPARATUS FOR DELIVERING ELECTRONIC IDENTIFICATION COMPONENTS OVER A WIRELESS NETWORK"라는 명칭으로 2010년 10월 28일에 출원된 제61/407,862호, "METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS"라는 명칭으로 2010년 10월 28일에 출원된 제61/407,866호, "ACCESS DATA PROVISIONING SERVICE"라는 명칭으로 2010년 10월 29일에 출원된 제61/408,504호, "METHODS AND APPARATUS FOR ACCESS DATA RECOVERY FROM A MALFUNCTIONING DEVICE"라는 명칭으로 2010년 11월 3일에 출원된 제61/409,891호, "SIMULACRUM OF PHYSICAL SECURITY DEVICE AND METHODS"라는 명칭으로 2010년 11월 4일에 출원된 제61/410,298호, 및 "APPARATUS AND METHODS FOR RECORDATION OF DEVICE HISTORY ACROSS MULTIPLE SOFTWARE EMULATION"이라는 명칭으로 2010년 11월 12일에 출원된 제61/413,317호에 관련되며, 전술 항목 각각은 그 전체 내용이 여기에 참조로 포함된다.

[0004] 본 발명은 일반적으로 통신 시스템들의 분야에 관련되며, 더 구체적으로는, 일 예시적인 양상에서 사용자 장비로 하여금 액세스 제어 클라이언트들을 사용하여 무선 네트워크들(예를 들어, 셀룰러 네트워크들, WLAN들 등)에

대해 인증하게 하는 무선 시스템들에 관한 것이다.

배 경 기 술

[0005] 대부분의 종래 기술의 무선 라디오 통신 시스템들에서 보안 통신을 위해 액세스 제어가 요구된다. 일 예로서, 한 가지 단순한 액세스 제어 방식은 (i) 통신 파티의 ID(identity)를 검증하는 것, 및 (ii) 검증된 ID에 적합한 액세스의 레벨을 승인하는 것을 포함할 수 있다. 예시적인 셀룰러 시스템(예를 들어, UMTS(Universal Mobile Telecommunications System))의 상황 내에서, 액세스 제어는 물리적 UICC(Universal Integrated Circuit Card) 상에서 실행하는 USIM(Universal Subscriber Identity Module)이라고 불리는 액세스 제어 클라이언트에 의해 관리된다. USIM 액세스 제어 클라이언트는 UMTS 셀룰러 네트워크에 가입자를 인증한다. 성공적인 인증 이후, 가입자에게 셀룰러 네트워크로의 액세스가 허용된다. 하기에서 사용되는 바와 같이, 용어 "액세스 제어 클라이언트"는 일반적으로, 네트워크로의 제1 디바이스의 액세스를 제어하기에 적합한, 하드웨어 또는 소프트웨어 내에 구현되는 논리 엔티티를 나타낸다. 액세스 제어 클라이언트들의 일반적 예들은 전술한 USIM, CSIM(CDMA Subscriber Identity Module), ISIM(IP Multimedia Services Identity Module), SIM(Subscriber Identity Module), RUIM(Removable User Identity Module) 등을 포함한다.

[0006] 통상적으로, USIM(또는 더 일반적으로 "SIM")은, 보안 초기화를 보장하기 위해 적용가능한 데이터 및 프로그램들을 검증하고 암호해독하는, 공지된 AKA(Authentication and Key Agreement) 절차를 수행한다. 구체적으로, USIM은 (i) 네트워크 운영자에게 그의 ID를 제공하기 위해 원격 챌린지에 성공적으로 응답하는 것, 및 (ii) 네트워크의 ID를 검증하기 위한 챌린지를 발행하는 것 모두를 수행해야 한다.

[0007] SIM 카드가 제조될 때, SIM 카드는 해당 SIM 카드의 사용을 특정 통신 사업자(carrier)로 제한하는 통신 사업자-특정 인증 정보를 이용하여 프로그래밍된다. 사용자가 기존의 통신 사업자로부터 새로운 통신 사업자로 서비스들을 변경하기를 원하는 경우, 사용자는 자신의 SIM 카드를 유사한 방식으로, 그러나 상이한 통신 사업자에 대해 프로그래밍된 새로운 SIM 카드로 교체할 필요가 있다.

[0008] 그러나, 기존의 SIM 솔루션들은 다수의 약점들 및 결함들을 가진다. 예를 들어, SIM 소프트웨어는 물리적 SIM 카드 매체에 변경할 수 없게 코딩되고(hard-coded), 결과적으로, 가입자들은 SIM 동작을 변경하려면 새로운 SIM 카드들을 필요로 한다. 카드들을 교환하는 불편함을 감소시키려는 노력으로, 일부 카드들에는 2개의 계정들이 프리로딩된다. 사용자는 카드를 물리적으로 제거하지 않고 2개의 계정들 사이에서 스위칭할 수 있다. 그러나, 이러한 타입의 SIM 카드의 사용자는 새로운 계정들을 추가하려면 여전히 새로운 카드를 필요로 할 것이다.

[0009] 유사하게, 일부 사용자 디바이스들은 다수의 카드 슬롯들을 가지지만, 다수의 카드 리셉터클들을 지원하는 것은 부피가 크며, 그럼에도 불구하고, 동작을 위해서는 실제 SIM 카드를 필요로 한다. 또한, SIM 카드 또는 SIM 카드를 포함하는 디바이스를 분실하는 경우, 사용자는 연관된 계정으로의 액세스를 복원하기 위해서는 새로운 SIM 카드를 획득해야 한다.

[0010] 따라서, 무선 서비스들을 관리하고 이들에 액세스하기 위한 개선된 솔루션들이 요구된다. 이상적으로, 이러한 솔루션들은 액세스 제어를 위해 물리적 카드에 의존하지 않아야 한다. 또한, 개선된 솔루션들은, 예를 들어, 다중 액세스 제어 프로파일들, 다양한 프로파일들의 백업, 액세스 제어 프로파일들의 원격 저장 등과 같은 다른 바람직한 특징들과 호환가능하거나 이들을 지원해야 한다.

발명의 내용

[0011] 본 발명은, 특히, 사용자들에게 통신 및/또는 데이터 서비스들의 제공을 위해 다중 액세스 제어 엔티티들을 관리하기 위한 장치 및 방법들을 제공함으로써 상기 요구들을 해결한다.

[0012] 본 발명의 제1 양상에서, 복수의 사용자 디바이스들에게 복수의 사용자 액세스 제어 클라이언트들을 제공하기 위한 방법이 개시된다. 일 실시예에서, 방법은 서버와 연관된 보안 저장소 내에 복수의 사용자 액세스 제어 클라이언트들을 저장하는 단계; 복수의 사용자 액세스 제어 클라이언트들의 개별 클라이언트들에 대한 복수의 데이터베이스 레코드들을 생성하는 단계; 및 요청 디바이스로부터 복수의 사용자 액세스 제어 클라이언트들의 개별 클라이언트들 중 하나에 액세스하기 위한 요청을 수신하는 단계를 포함한다. 요청이 서비스될 수 있다고 결정되는 경우, 요청된 액세스 제어 클라이언트가 보안 저장소로부터 검색되어, 요청 디바이스에 전송되고, 요청 디바이스에서의 요청된 액세스 제어 클라이언트의 사용을 반영하기 위해 요청된 액세스 제어 클라이언트에 대해 데이터베이스 레코드가 업데이트된다.

[0013] 본 발명의 제2 양상에서, 하나 또는 복수의 eSIM(electronic subscriber identity module)으로의 액세스를 모바일 디바이스에 제공하기 위한 방법이 개시된다. 일 실시예에서, 방법은 복수의 eSIM의 개별 eSIM에 대한 복수의 데이터베이스 레코드들을 이용하여, 모바일 디바이스가 액세스할 수 있는 복수의 eSIM의 서브세트의 리스트를 생성하는 단계; 모바일 디바이스로부터 eSIM의 서브세트 중 하나에 액세스하기 위한 요청을 수신하는 단계; 요청된 eSIM을 요청 디바이스에 전송하는 단계; 및 요청된 eSIM과 연관된 데이터베이스 레코드 내의 상태 식별자를 업데이트하는 단계를 포함한다.

[0014] 본 발명의 제3 양상에서, 복수의 액세스 제어 클라이언트들을 안전하게 제공하기 위한 서버 장치가 개시된다. 일 실시예에서, 장치는: 복수의 인터페이스들; 복수의 액세스 제어 클라이언트를 저장하도록 구성된 저장 장치; 적어도 하나의 컴퓨터 프로그램을 실행하도록 구성된 프로세서를 포함한다. 컴퓨터 프로그램은 일 변형에서, 복수의 레코드들 - 레코드들 각각은 복수의 액세스 제어 클라이언트의 개별 클라이언트와 연관됨 - 을 생성하고; 요청 디바이스로부터 복수의 액세스 제어 클라이언트 중 하나에 액세스하기 위한 요청을 수신하고; 요청 디바이스 및 복수의 액세스 제어 클라이언트 중 요청된 클라이언트의 현재 상태에 적어도 부분적으로 기초하여, 요청이 서비스될 수 있는지의 여부를 결정하도록 구성된다.

[0015] 본 발명의 제4 양상에서, 모바일 디바이스와 통신할 수 있는 사용자 디바이스가 개시된다. 일 실시예에서, 모바일 디바이스는 그것의 사용자에게 전화 통화 및 데이터 서비스들 중 적어도 하나를 제공하기 위한 것이며, 사용자 디바이스는, 적어도 하나의 인터페이스; 저장 장치; 및 적어도 하나의 컴퓨터 프로그램을 실행하기 위한 프로세서를 포함한다. 컴퓨터 프로그램은 모바일 디바이스 상에서 사용가능한 데이터 구조와 관련된 정보를 컴파일하고; 데이터 구조에 액세스하기 위한 요청을 모바일 디바이스로부터 수신하고; 요청된 데이터 구조를 모바일 디바이스에 전송하고; 데이터 구조의 현재 사용을 표시하기 위해 데이터 구조와 관련된 정보를 업데이트하도록 구성되고, 업데이트된 정보는 데이터 구조가 이용가능하지 않음을 표시하는 정보를 포함한다.

[0016] 본 발명의 제5 양상에서, 모바일 디바이스가 개시된다. 일 실시예에서, 모바일 디바이스는 가상 또는 전자 SIM 데이터 구조를 요청하고, 수신하고, 이용하도록 구성된다.

[0017] 본 발명의 제6 양상에서, 컴퓨터 판독가능한 장치가 개시된다. 일 실시예에서, 장치는 실행중인 적어도 하나의 컴퓨터 프로그램을 가지는 저장 매체를 포함하고, 적어도 하나의 프로그램은 가상 또는 전자 SIM들에 대한 요청들을 수신하고, 프로세싱하고, 그것들을 제공하도록 구성된다.

[0018] 본 발명의 제7 양상에서, 사용자들에게 가상 또는 전자 SIM들을 분배하기 위한 시스템이 개시된다. 일 실시예에서, 시스템은 인터넷, 또는 MAN 또는 WLAN과 같은 네트워크를 통한 eSIM들의 전달을 위한 장치를 포함한다.

[0019] 본 발명의 다른 특징들 및 장점들은 하기에 주어진 바와 같은 예시적인 실시예들의 상세한 설명 및 첨부 도면들을 참조하여 당업자에 의해 즉시 인지될 것이다.

도면의 간단한 설명

[0020] 도 1은 종래 기술의 USIM을 사용하는 예시적인 AKA(Authentication and Key Agreement) 절차를 예시한다.

도 2는 본 발명에 따라, eSIM을 클라이언트 지갑에 저장하고 그로부터 검색하기 위한 일 예시적인 방법을 예시한다.

도 3은 본 발명에 따라, eSIM을 클라이언트 서버에 파킹하고 그로부터 검색하기 위한 일 예시적인 방법을 예시한다.

도 4는 본 발명에 따른 eSIM 관리 네트워크 아키텍처의 일 예시적인 실시예를 예시한다.

도 5는 네트워크 데이터베이스, 클라이언트 지갑, 또는 클라이언트 서버에 액세스 제어 클라이언트를 초기에 저장하기 위한 일반화된 방법의 일 실시예를 예시한다.

도 6은 사용자 디바이스들이 액세스 제어 클라이언트를 이용할 수 있게 하기 위한 예시적인 방법을 예시한다.

도 7은 사용자 디바이스로부터 제어 클라이언트를 복귀시키기 위한 예시적인 방법을 예시한다.

도 8은 본 발명의 일 실시예에 따라 상태 표시자들 및 허가된 디바이스들이 연관되어 있는 이용가능한 eSIM의 예시적인 데이터베이스를 예시한다.

도 9는 본 발명에 유용한 SPS의 일 예시적인 실시예를 예시한다.

도 10은 본 발명의 다수의 eSIM 관리 특징들에서 사용하기 위한 예시적인 사용자 디바이스를 예시하는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 이제 동일한 참조 번호가 전반에 걸쳐 동일한 부분들을 나타내는 도면들이 참조된다.

[0022] 개요

[0023] 일 양상에서, 본 발명은 다중 액세스 제어 엔티티들 또는 클라이언트들의 개선된 관리를 허용하는 방법들 및 장치에 관한 것이다. 일 예시적인 실시예에서, 본 발명은 다수의 가상 또는 전자 SIM(eSIM)들의 저장 및 그들 사이의 스위칭을 허용한다. 여기서 더 상세히 기술되는 바와 같이, eSIM들은 백업, 사용자 장비 간의 eSIM들의 전달, 또는 SIM 제공 서버(SPS)에 다시 미사용된 eSIM들을 릴리스할 목적으로, 디바이스에서 떨어져(off-device) 저장될 수 있다.

[0024] 본 발명의 일 예시적인 구현예에서, eSIM들은 암호화된 "지갑(wallet)" 형태로 외부 또는 원격 컴퓨터, 또는 다른 디바이스(개인용이든 제3자가 유지하는 것이든)에 저장된다. 예를 들어, 한가지 사용 경우에서, 사용자는 중개인 또는 통신 사업자를 관련시키지 않고 "지갑"으로부터의 eSIM 동작을 복원할 수 있다. 또 다른 실시예에서, eSIM은 클라우드(네트워크) 인프라 구조에 "파킹"될 수 있다. 활성 eSIM을 포함하는 사용자 장비가 그것을 릴리스하고(eSIM의 추가 사용을 중단하고), 클라우드 엘리먼트에 eSIM(또는 그것의 표현)을 저장할 때, eSIM은 파킹된다. 사용자는 이후 클라우드 엘리먼트로부터 동일한 사용자 장비로 eSIM을 검색하거나, 또는 그것을 상이한 사용자 장비에 로딩할 수 있다. 추가로, 클라우드 상의 저장된 비활성 eSIM은 또한 재사용을 위해 (사용자 장비에 이전에 전달되거나 미전달되는지에 관계없이) 통신 사업자에 다시 릴리스될 수 있다.

[0025] 하기에 더 상세히 기술되는 바와 같이, 본 발명의 다양한 양상들은 액세스 제어 클라이언트를 사용자 계정과 연관시키는 것에 관한 것이다. 예를 들어, 사용자는 eSIM들을 클라우드 인프라구조에 저장하고 그로부터 검색할 수 있다. 일부 변형예들에서, 파킹된 eSIM들은 사용자 계정 등과 연관된 임의의 디바이스가 자유롭게 액세스할 수 있는 대체 가능 물품들로서 다루어질 수 있다.

[0026] 예시적인 실시예들의 상세한 설명

[0027] 본 발명의 예시적인 실시예들 및 양상들이 이제 더 상세하게 기술된다. 이들 실시예들 및 양상들이 GSM, GPRS/EDGE, 또는 UMTS 셀룰러 네트워크의 SIM(Subscriber Identity Module)들의 상황에서 주로 논의되지만, 본 발명이 그렇게 제한되지 않는다는 점이 당업자에 의해 인지될 것이다. 실제로, 본 발명의 다양한 양상들은 다중 액세스 제어 엔티티들 또는 클라이언트들의 제공 및 사용으로부터 이득을 얻을 수 있는 임의의 무선 네트워크(셀룰러이든 다른 것이든 간에)에서 유용하다.

[0028] 또한, 용어 "가입자 식별 모듈(subscriber identity module)"이 여기서 사용되지만(예를 들어, eSIM), 이러한 용어가 반드시 (i) 가입자 그 자체에 의한 사용(즉, 본 발명이 가입자 또는 비-가입자에 의해 구현될 수 있음); (ii) 단일 개인의 ID(즉, 본 발명이 가족과 같은 개인들의 그룹 또는 기업과 같은 무형의 또는 가상의 엔티티를 대신하여 구현될 수 있음); 또는 (iii) 임의의 유형의 "모듈" 장비 또는 하드웨어를 내포하거나 요구하지는 않는다는 점이 인지될 것이다.

[0029] **종래 기술의 가입자 식별 모듈(SIM) 동작 -**

[0030] 종래 기술의 UMTS 셀룰러 네트워크들의 상황 내에서, 사용자 장비(UE)는 모바일 디바이스 및 USIM(Universal Subscriber Identity Module)을 포함한다. USIM은 물리적 UICC(Universal Integrated Circuit Card)에 저장되고 이로부터 실행되는 논리적 소프트웨어 엔티티이다. 가입자 정보뿐만 아니라 무선 네트워크 서비스들을 획득하기 위해 네트워크 운영자와의 인증을 위해 사용되는 키들 및 알고리즘들과 같은 다양한 정보가 USIM에 저장된다. USIM 소프트웨어는 Java Card™ 프로그래밍 언어에 기초한다. Java Card는 임베디드 "카드" 타입 디바이스들(예를 들어, 전술한 UICC)에 대해 수정된 Java™ 프로그래밍 언어의 서브세트이다.

[0031] 일반적으로, UICC들은 가입자 분배 이전에 USIM을 이용하여 프로그래밍되며; 사전 프로그래밍 또는 "개인화"는 각각의 네트워크 운영자에 대해 특정적이다. 예를 들어, 배치 이전에, USIM은 IMSI(International Mobile Subscriber Identifier), 고유 ICC-ID(Integrated Circuit Card Identifier) 및 특정 인증 키(K)와 연관된다. 네트워크 운영자는 네트워크 인증 센터(AuC, Authentication Center) 내에 포함된 레지스트리에 상기 연관을 저

장한다. 개인화 이후, UICC는 가입자들에게 분배될 수 있다.

[0032] 이제 도 1을 참조하면, 전술한 종래 기술 USIM을 사용하는 일 예시적인 AKA(Authentication and Key Agreement) 절차(100)가 상세하게 예시된다. 통상의 인증 절차들 동안, UE(102)는 USIM(104)으로부터 IMSI(International Mobile Subscriber Identifier)를 획득한다. UE는 이것을 네트워크 운영자의 서빙 네트워크(SN, Serving Network)(106) 또는 방문한 코어 네트워크에 전달한다. SN은 홈 네트워크(HN)의 AuC에 인증 요청을 포워딩한다. HN은 수신된 IMSI를 AuC의 레지스트리와 비교하고, 적절한 K를 획득한다. HN은 난수(RAND)를 생성하고, 예상된 응답(XRES, expected response)을 생성하기 위한 알고리즘을 사용하여 K를 가지고 이것에 서명한다. HN은 추가로 암호화 및 무결성 보호를 위해 사용하기 위한 암호화 키(CK, Cipher Key) 및 무결성 키(IK, Integrity Key)뿐만 아니라 다양한 알고리즘을 사용하여 인증 토큰(AUTN, Authentication Token)을 생성한다. HN은 RAND, XRES, CK, 및 AUTN로 구성된 인증 벡터를 SN에 송신한다. SN은 오직 일회성 인증 프로세스에서만 사용하기 위해 인증 벡터를 저장한다. SN은 RAND 및 AUTN을 UE에 전달한다.

[0033] 일단 UE(102)가 RAND 및 AUTN를 수신하면, USIM(104)는 수신된 AUTN이 유효한지의 여부를 검증한다. 만약 그러하다면, UE는 수신된 RAND를 사용하여, XRES를 생성한 동일한 알고리즘 및 저장된 K를 사용하여 자신의 고유한 응답(RES)을 계산한다. UE는 RES를 다시 SN에 전달한다. SN(106)는 XRES를 수신된 RES와 비교하고, 이들이 일치하는 경우, SN은 UE에게 운영자의 무선 네트워크 서비스들을 사용하도록 허가한다.

[0034] **예시적 동작 -**

[0035] 본 발명의 다양한 양상들이 이제 일 예시적인 구현예에 대해 논의된다. 본 발명의 예시적인 실시예의 상황에서, 종래 기술에서와 같은 물리적 UICC를 사용하는 대신, UICC는 예를 들어, UE 내의 보안 엘리먼트(예를 들어, 보안 마이크로프로세서 또는 저장 디바이스) 내에 포함되는, 하기에서 eUICC(Electronic Universal Integrated Circuit Card)라고 불리는 소프트웨어 애플리케이션과 같은 가상 또는 전자 엔티티로서 에뮬레이팅된다. eUICC는 하기에서 eSIM(Electronic Subscriber Identity Module)이라고 불리는 다수의 SIM 엘리먼트들을 저장하고 관리할 수 있다. 각각의 eSIM은 통상적인 USIM의 소프트웨어 에뮬레이션이며, 유사한 프로그래밍 및 그와 연관된 사용자 데이터를 포함한다. eUICC는 eSIM의 ICC-ID에 기초하여 eSIM을 선택한다. eUICC가 원하는 eSIM(들)을 선택하면, UE는 eSIM의 대응하는 네트워크 운영자로부터 무선 네트워크 서비스들을 획득하기 위해 인증 절차를 개시할 수 있다.

[0036] 다수의 eSIM들을 관리하기 위한 2개의 다른 방법들이 아래에 기술된다. 일 실시예에서, eSIM은 SPS와 같은 네트워크에 저장(또는 "파킹")된다. 대안적으로, eSIM은 클라이언트 지갑에 저장된다. 그러나, 본 발명이 결코 이들 방법들에 제한되지 않으며, 전술한 내용이 단지 더 넓은 원리들의 예시에 불과하다는 점이 이해될 것이다.

[0037] 예시적인 클라이언트 "지갑" 동작 -

[0038] 도 2는 eSIM을 클라이언트 지갑에 저장하고 그로부터 검색하기 위한 일 예시적인 방법을 예시한다. 하기에서 사용되는 바와 같이, 용어 "지갑"은 하나 이상의 액세스 제어 클라이언트들을 저장하기에 적합한 개인용, 핸드헬드, 또는 랩톱 컴퓨터 또는 개인용 미디어 디바이스(예를 들어, iPod®)를 나타낸다. 예를 들어, 지갑은 로컬 컴퓨터 상에서 실행되는 소프트웨어 애플리케이션(예를 들어, 본원의 양수인에 의해 개발되고 배포되는 iTunes™)을 포함할 수 있고; 대안적으로, 지갑은 가입자의 모바일 디바이스 상에 직접 배치된다. 또한, 클라이언트 지갑은 가입자의 직접 제어 내에 있으며, 가입자의 재량에 따라, 가입자의 디바이스 상에 eSIM을 안전하게 저장하고, 전달하고 그리고/또는 교체할 수 있다.

[0039] 단계(202)에서, 모바일 디바이스는 지갑에 대한 접속을 설정한다. 예를 들어, 사용자는 집 또는 사무실 컴퓨터에 그의 모바일 디바이스를 접속할 수 있다. 모바일 디바이스는 지갑의 사용자 계정에 자신을 식별한다. 사용자 계정은 사용자명, 패스워드 등을 요구할 수 있다. 지갑이 안전이 보장되지 않은 또는 어쩌면 심지어 손상된 컴퓨터-판독가능한 매체(하기에서 더욱 상세하게 논의됨)를 포함할 수 있다는 것을 알 것이다.

[0040] 단계(204)에서, 사용자는 저장, 전달 또는 교체를 위해 하나 이상의 eSIM을 선택한다. 사용자의 사용자 계정은 하나 이상의 eSIM과 연관된다. 사용자는 사용자 계정의 eSIM들 중 임의의 것을 선택하고, 소프트웨어 애플리케이션 내의 그래픽 사용자 인터페이스(GUI)로부터 동작(예를 들어, 저장, 전달, 교체, 추가, 삭제 등)을 요청할 수 있다. 일부 구현예들에서, 이용가능한 eSIM들의 리스팅은 지갑 내에 이전에 저장된 이용가능한 eSIM들(예를 들어, 심지어, 사용자 계정과 이전에 연관되지 않은 eSIM들), 및 모바일 디바이스 내에서 현재 활성이거나 상주하는 eSIM들을 식별하는 추가적인 단계(미도시)를 요구한다.

[0041] 예를 들어, 사용자가 저장을 위해 eSIM을 선택하는 경우, 단계(206)에서, 모바일 디바이스는 그의 eSIM을 암호화한다. 이전에 언급한 바와 같이, 지갑은 안전이 보장되지 않은 또는 손상된 매체를 포함할 수 있다. 결과적으로, 단계(206)는 지갑에 저장된 동안 eSIM에 대한 합당한 정도의 보안을 제공한다. 이러한 보안 조치는 추가적인 무결성 체크 등을 포함할 수 있다. 단계(208)에서, 지갑은 암호화된 eSIM을 저장한다. 지갑은 또한, eSIM이 우발적으로(또는 악의적으로) 복제되거나, 분실되지 않도록 보장하기 위해 자신의 상태를 업데이트할 것이다. 구체적으로, 지갑은 각각의 eSIM의 현재 상태(예를 들어, 활성, 비활성 등)의 내부 상태를 유지한다.

[0042] 유사하게, 사용자가 eSIM이 사용을 위해 디바이스에 전달될 것을 요청하는 경우, 단계(210)에서, 모바일 디바이스는 요청된 eSIM을 다운로드한다. 단계(212)에서, 모바일 디바이스는 eSIM이 예를 들어, 암호해독 및 무결성 체크의 검증에 의해 손상되지 않은 상태로 유지된 것을 검증한다. 성공적 검증까지, eSIM은 사용을 위해 모바일 디바이스로 로드될 수 있고, 지갑은 eSIM의 현재 상태를 업데이트한다.

[0043] 또한, 사용자가 eSIM의 "교환" 또는 교체를 요청하는 경우, 모바일 디바이스는 그의 현재 eSIM을 암호화 및 저장하고(단계 214 및 단계 216), 새로운 eSIM을 검색하여 암호해독한다(단계 218, 220). 성공적 완료까지, 이전 eSIM 및 새로운 eSIM 상태 모두가 그에 따라 업데이트된다.

[0044] 예시적인 네트워크 "파킹" 동작 -

[0045] 도 3은 eSIM을 네트워크 기기에 저장하고 그로부터 검색하기 위한 일 예시적인 방법을 예시한다. 하기에서 사용되는 바와 같이, 용어 "파킹"은 "클라이언트 서버" 내의 저장을 위해 하나 이상의 액세스 제어 클라이언트들을 비활성화하는 것을 나타내고, 여기서 사용되는 바와 같이, 용어 "클라이언트 서버"는 일반적으로 보안 저장 장치를 나타낸다. 보안 저장 장치는 네트워크 기기 또는 다른 "클라우드 컴퓨팅" 구조 내에 위치할 수 있다. 파킹된 eSIM은 가입자의 직접 제어 내에 있지 않은데, 즉 가입자는 동작을 재개하려면 파킹된 eSIM을 활성화시켜야 한다.

[0046] 단계 302에서, 모바일 디바이스는 클라이언트 서버에 대한 접속을 설정한다. 예를 들어, 사용자는 집 또는 사무실 컴퓨터에 그의 모바일 디바이스를 접속시킬 수 있고, 여기서 컴퓨터는 클라이언트 서버에 접속되는 애플리케이션(예를 들어, 본원의 양수인에 의해 개발되고 배포되는 iTunes Store™)을 가진다. 대안적으로, 사용자는 모바일 디바이스(예를 들어, 본원의 양수인에 의해 개발되고 배포되는 App Store™)를 통해 클라이언트 서버에 직접 액세스할 수 있다. 모바일 디바이스는 예를 들어, 사용자명, 패스워드 등에 기초하여, 클라이언트 서버의 사용자 계정에 자신을 식별한다.

[0047] 단계(304)에서, 사용자는 저장, 전달 또는 교체를 위해 하나 이상의 eSIM을 선택한다. 사용자는 파킹을 위해 eSIM을 선택하거나, 또는 파킹된 eSIM을 검색할 수 있다. 사용자가 eSIM 및 원하는 동작을 선택하면, 요청이 클라이언트 서버에 포워딩된다.

[0048] 예를 들어, 사용자가 파킹을 위해 eSIM을 선택하면, 단계(306)에서, 클라이언트 서버는, 모바일 디바이스가 eSIM을 파킹하도록 허가되어 있는지의 여부를 결정한다. 허가는, 사용자 ID, 현재 유지된 eSIM들, 현재 파킹된 eSIM들, 의심되는 사기 행동, 의심되는 우발적 행동(예를 들어, 우발적 파킹 요청) 등과 같은 고려사항들에 기초할 수 있다. 요청이 유효한 경우, 클라이언트 서버는 eSIM을 파킹하고, 이후 eSIM을 비활성화한다(단계 308).

[0049] 유사하게, 사용자가 파킹된 eSIM을 검색하기를 원하는 경우, 단계(310)에서, 클라이언트 서버는, 요청에 기초하여, 모바일 디바이스가 eSIM의 동작을 재개하도록 허가되어 있는지의 여부를 결정한다. 요청이 유효한 경우, 클라이언트 서버는 eSIM을 검색하고, eSIM을 활성화하고, eSIM 상태를 업데이트하고, 모바일 디바이스에 eSIM을 전송한다(단계 312).

[0050] 마지막으로, 사용자가 eSIM의 "교환" 또는 교체를 요청하는 경우, 네트워크는, 모바일 디바이스가 교환을 발행하도록 허가되어 있는지의 여부를 결정하고(단계 314), 현재 eSIM을 파킹하여 현재 eSIM을 비활성화하고, 새로운 eSIM을 검색하여 새로운 eSIM을 활성화하고, 최종적으로 활성화된 새로운 eSIM을 모바일 디바이스에 로딩함으로써 적절한 eSIM들을 교환한다(단계 316).

[0051] **예시적인 eSIM 관리 네트워크 아키텍처 -**

[0052] 이제 도 4를 참조하면, 본 발명의 일 실시예에 따른 일 예시적인 전자 가입자 식별 모듈(eSIM) 관리 네트워크 아키텍처가 예시되어 있다. 도시된 바와 같이, 네트워크는 일반적으로, 통신 네트워크(408)를 통해 복수의 사용자 장비(UE)(404)와 통신하도록 구성된 SIM 제공 서버(SPS, SIM provisioning server)(402)를 포함한다.

SPS는 복수의 모바일 네트워크 운영자(MNO, mobile network operator)들(406)과 추가로 통신한다. 전술한 엔티티들의 간략한 설명이 이제 제공된다.

[0053] 도 4의 실시예에서의 SPS(402)는 서비스 중개자에 의해 관리되는 독립형 엔티티이다. 일 구현예에서, 서비스 중개자는 하나 이상의 MNO들(406)에 대해 파트너가 되는 디바이스 제조자(예를 들어, 본원의 양수인 Apple Inc.™ 등)를 포함할 수 있지만, 다른 배열들이 동일하게 성공적으로 사용될 수 있다. SPS는 네트워크(408)에서 UE(404)에 제공되고 UE(404)에 의해 이용되는 복수의 이용가능한 eSIM들을 저장할 책임이 있다. SPS는 제3자 엔티티와 같은 또 다른 엔티티(미도시)로부터 eSIM들의 "풀(pool)"을 수신할 수 있거나, 또는 대안적으로, 스스로 eSIM들을 생성할 수 있다. 각각의 eSIM은 SPS를 통해 적용가능한 네트워크 운영자에 기초하여 사전 프로그래밍되거나 또는 "개인화"된다.

[0054] 또한 도시된 바와 같이, SPS는 또한 신뢰할 수 있는 서비스 관리자(TSM, Trusted Service Manager)(414) 내에 구현될 수 있고, TSM들의 일반적 예들은 제3자 SIM 벤더 등을 포함한다. TSM은 하나 이상의 MNO들과의 사전 설정된 신뢰 관계를 가진다.

[0055] MNO들(406)은 무선 또는 모바일 통신 사업자들 및 서비스 제공자들을 포함한다. 예시적인 MNO들은 통상적으로, 전화 통화, 단문 메시지 서비스(SMS) 텍스트, 및 데이터 서비스들을 통신 네트워크를 통해 가입자들의 그룹에 제공한다. MNO들의 예들은 예를 들어, AT&T™, Verizon™, Sprint™ 등을 포함한다.

[0056] 통신 네트워크(408)는 전술한 서비스들의 제공을 가능하게 하는 임의의 네트워크일 수 있다. 예를 들어, 통신 네트워크(208)는 유선 또는 무선 통신 네트워크를 포함할 수 있다. 무선 네트워크의 일반적 예들은 GSM(Global System for Mobile Communications), GPRS(General Packet Radio Service), EDGE(Enhanced Data rates for GSM Evolution), UMTS(Universal Mobile Telecommunications System), 다른 네트워크(예를 들어, CDMA2000, 모바일 WiMAX 네트워크들, WLAN 네트워크들 등)와 같은 셀룰러 네트워크들을 포함한다. 유선 네트워크의 일반적 예들은 인터넷 등을 포함한다.

[0057] MNO들(406)로의 액세스는 독립형 SPS(402) 및/또는 TSM들(414)(및 연관된 SPS)의 조합을 통해 제공될 수 있다. 다시 말해, 독립형 SPS는 특정 네트워크들 상의 UE들(404)에 서비스들 및 eSIM들을 제공하기 위해 이용될 수 있는 반면, TSM은 TSM과 연관된 다른 네트워크들 상의 UE들에 서비스들 및 eSIM들을 제공하기 위해 이용된다.

[0058] 예시적인 전자 가입자 식별 모듈(eSIM) 관리 네트워크 아키텍처의 상황 내에서, 예시적인 클라이언트 지갑(410) 및 클라이언트 서버(412)가 이제 더 상세하게 기술된다.

[0059] 도 4에 예시된 바와 같이, 클라이언트 지갑(410)은 통신 네트워크(408)를 통해 또는 직접적인 유선 또는 무선 접속(WLAN/PAN로 도시된 바와 같은)을 통해 복수의 UE(404)와 통신중일 수 있다. 따라서, 지갑은 (예를 들어, 디바이스들의 사용자, 지갑 및 디바이스들과 연관된 가입자, 또는 디바이스들 그 자체에 기초하여) 그것 및/또는 그것의 연관된 디바이스들이 이용할 수 있는 복수의 eSIM들을 저장한다. 지갑은 지갑과 통신중인 임의의 UE에 이들 eSIM 중 하나 이상을 분배할 수 있다.

[0060] 마지막으로, 도 4는 통신 네트워크(408)를 통해 사용자에 의해 액세스 가능한 클라이언트 서버(412)를 예시한다. 따라서, 클라이언트 서버는 하나 이상의 디바이스들(404)에 대한 분배를 위해 복수의 eSIM들을 저장한다. 클라이언트 서버는 필요한 인증 및 계정 정보를 지원하기 위해 MNO와의 접속을 유지한다.

[0061] 도 4의 아키텍처는 특정 가입자, 가입자들의 그룹(예를 들어, 가족, 회사 등), 및/또는 디바이스에 대한 다중 eSIM의 관리를 제공하기 위해 위에서 논의된 바와 같이 사용될 수 있다. 위에서 개시된 아키텍처는 마찬가지로 UE(404)가, 예를 들어, 상이한 eSIM들에 대한 상이한 사용들(예를 들어, 개인, 사업, 여행 등)을 관리하기 위해, 신속하고 효과적으로 eSIM들을 스위칭하기 위한 메커니즘을 제공하기 위해 이용될 수 있다. 사용자는 단순히, 그리고 통신 사업자에 직접 액세스하지 않고, 몇몇 eSIM들 사이에서 스위칭할 수 있다.

[0062] 본 발명의 하나 이상의 양상들을 구현하기 위한 일반화된 방법들 및 장치의 설명이 이제 제시된다.

[0063] **방법-**

[0064] 이제 도 5를 참조하면, 네트워크 데이터베이스, 클라이언트 지갑, 또는 클라이언트 서버에 액세스 제어 클라이언트를 초기에 저장하기 위한 일반화된 방법(500)의 일 실시예가 예시되고 기술된다. 전술한 방법은 처음 액세스 제어 클라이언트가 저장될 때, 액세스 제어 클라이언트가 불필요하게 복제되거나 분실되지 않으며, 적절한 상태가 초기화됨을 보장한다. 하기에서, 도 6 및 7에서 각각 기술된 "사인-아웃" 및 "사인-인" 절차들은 균일

한 액세스 제어 클라이언트 사용을 유지하기 위해 사용될 수 있다.

[0065] 도시된 바와 같이, 단계(502)에 따라, 액세스 제어 클라이언트를 저장하기 위한 요청이 수신된다. 일 실시예에서, 요청이 사용자 또는 사용자 디바이스로부터 수신된다. 대안적으로, 요청은 계정이 설정될 때 계정 관리 엔티티와 같은 네트워크 엔티티로부터 수신될 수 있다. 예를 들어, 사용자는 디바이스를 구매하고, 이후, 디바이스를 통해, 클라이언트 지갑 또는 클라이언트 서버에의 저장을 위해, 해당 가입자 및 디바이스에 대해 특정적인 액세스 제어 클라이언트의 생성 및 제공을 요청할 수 있다. 또 다른 실시예에서, 액세스 제어 클라이언트를 저장하기 위한 요청은 제1 디바이스로부터 수신될 수 있지만, 제어 클라이언트가 제2 디바이스와 연관됨을 표시한다. 또 다른 실시예에서, 액세스 제어 클라이언트를 저장하기 위한 요청은, 액세스 제어 클라이언트가 제1 디바이스에 저장되고, 사용으로부터 제거되거나 비활성화될 것임을 표시하면서, 제1 디바이스로부터 수신될 수 있다.

[0066] 클라이언트 지갑 또는 클라이언트 서버로의 액세스 제어 클라이언트의 전술한 저장은, 동적 데이터의 전송을 더 포함할 수 있다. 동적 데이터는 초기 개인화 이후 액세스 제어 클라이언트에서 변경되고 그리고/또는 생성되는 개인화된 데이터에 관한 것이다. 예를 들어, eSIM이 특정 네트워크, 가입자 및/또는 디바이스로 개인화되는 경우, 개인화된 eSIM은 이후 동적 데이터와 함께 제공된다. eSIM 데이터의 경우와 마찬가지로, 동적 데이터는 수송 동안 안전하게 유지되어야 한다. 동적 데이터 및/또는 eSIM 자체는 원하는 경우, 예를 들어, 공개/개인 키 또는 AES/DES 암호화, 무결성 보호를 위한 암호화 레지듀 또는 해시 등의 사용을 통해 물리적으로 보안될 수 있다.

[0067] 동적 데이터의 한가지 일반적 예는 OTASP(over-the-air-service provisioning) 이후의 eUICC/eSIM 상태이다. 예를 들어, 도 4의 이전 예시적인 네트워크를 참조하면, MNO(406)는 재프로그래밍을 위해 가입자에게 디바이스를 물리적으로 가져오는 것을 요구하는 것 대신 통신 네트워크(408)를 사용함으로써 가입자의 디바이스에 새로운 타입들의 서비스들을 추가하도록 (OTASP)를 수행한다. OTASP의 수행 이후, MNO(406)는 UE(404)에 대한 eUICC 상태를 추적할 수 있다. 추적된 상태는 동적 데이터의 일부분으로서 이동한다. 동적 데이터의 또 다른 일반적 예는 사용자 생성 데이터(예를 들어, 전화번호부 정보 등)이다.

[0068] 단계(504)에 따라, 요청을 수신하는 엔티티(예를 들어, 클라이언트 지갑, 클라이언트 서버 등) 또는 그와 통신하는 다른 엔티티가 요청을 검증한다. 예를 들어, 엔티티는 예를 들어, 요청 디바이스(또는 디바이스와 연관된 가입자)를 인증함으로써, 요청의 소스의 진위를 결정할 수 있다(즉, 요청을 송신한 엔티티가 그렇게 수행하도록 허가되어 있고 그리고/또는 진짜인 디바이스를 대신하는 것임을 보장한다). 요청 디바이스/사용자가 요청을 수행하도록 허가되어 있지 않고 그리고/또는 인증되어 있지 않은 경우, 액세스 제어 클라이언트는 생성되고/되거나 저장되지 않을 것이다.

[0069] 예를 들어, 일 예시적인 허가 또는 인증 단계는: (i) 요청 디바이스가 진짜 디바이스이고, 그리고 (ii) 요청 디바이스가 액세스 제어 클라이언트를 저장하도록 허가되어 있음을 결정한다. 예를 들어, 진위의 검증은 공지된 암호 챌린지(예를 들어, 키 암호법)에 대한 성공적 응답을 요구할 수 있다. 디바이스가 성공적으로 인증되면, 디바이스는 허가를 위해 체크된다(예를 들어, 허가된 디바이스들의 리스트 내에서 발견된다). 디바이스가 성공적으로 검증되는 경우, 프로세스는 단계(506)로 진행한다.

[0070] 대안적으로, 또 다른 예시적인 실시예에서, 검증은 단순한 사용자명 및 패스워드를 포함할 수 있다. 예를 들어, 사용자명 및 패스워드가 사용자 ID를 결정하고 사용자 계정 정보에 액세스하기 위해 사용될 수 있다. 유사하게, 또 다른 예시적인 실시예들에서, 검증은 요청 및 승인을 포함할 수 있다. 예를 들어, 제1 디바이스는 제2 디바이스에 액세스 제어 클라이언트를 요청할 수 있고, 제2 디바이스는 단순한 승인으로 요청을 검증한다. 요청 승인 방식들은 제1 디바이스로부터 제2 디바이스로 액세스 제어 클라이언트를 이동시킬 때 특히 사용된다.

[0071] 대안적으로, 또 다른 예시적인 실시예에서, 검증은 또 다른 엔티티를 이용한 검증을 포함할 수 있다. 예를 들어, 셀룰러 디바이스가 액세스 제어 클라이언트의 저장을 요청할 수 있지만, 액세스 제어 클라이언트는 (예를 들어, 또 다른 신뢰할 수 있는 엔티티에 따라) 무효할 수 있고, 이미 사용중일 수 있고, 손상되었을 수 있고, 등등이다.

[0072] 다음으로, 단계(506)에서, 액세스 제어 클라이언트가 검색 또는 수신된다. 이전에 언급한 바와 같이, 제어 클라이언트는 일 실시예에서 eSIM을 포함할 수 있다. eSIM은 전술한 동적 데이터를 더 포함할 수 있다. 일 구현예에서, 액세스 제어 클라이언트는 암호화되어 있거나 다른 방식으로 안전한 형태일 수 있다. 일 변형예에서, 암호화는 수신 디바이스에 의해 암호해독될 수 없다. 이러한 실시예들은 안전할 수 있거나 안전하지 않을 수

있는 클라이언트 지갑 타입 디바이스들에서 특히 유용하다. 예를 들어, eSIM은 오직 사용자 디바이스만 알고 있는 키를 이용하여 암호화될 수 있다. 이후, 지갑이 손상되더라도, eSIM은 암호해독될 수 없다. 다른 변형예들에서, 암호화는 수신 디바이스에 의해 암호해독될 수 있다. 이러한 실시예들은 액세스 제어 클라이언트로부터 다양한 사용자 정보, 예를 들어, eSIM과 연관된 동적 데이터를 검색하기 위해 액세스 제어 클라이언트를 암호해독할 수 있는 클라이언트 서버 실시예들에서 사용될 수 있다. 예를 들어, 사용자가 제1 eSIM을 파킹하고 제2 eSIM을 검색하는 경우, 사용자는 연락처 전화번호부 정보 등과 같은 동적 데이터 컨텐츠들을 검색하기를 원할 수 있다.

[0073] 단계(508)에서, 액세스 제어 클라이언트는 선택적으로 적절한 네트워크에 대해 "개인화"된다. 위에서 논의된 바와 같이, 일 실시예에서, 액세스 제어 클라이언트는 특정 네트워크 운영자, 서비스 제공자, 또는 MNO에 특정적인 정보를 이용하여 개인화되거나 사전프로그래밍된다. 대안적으로, 개인화는 또 다른 엔티티에서 발생할 수 있다. 단계(508)는 액세스 제어 클라이언트를 보안하는 암호화 또는 다른 형태를 더 포함할 수 있다.

[0074] 데이터의 개인화(단계 508)는 또한 액세스 제어 클라이언트에 상태 표시자를 연관시키는 것 및/또는 각각의 액세스 제어 클라이언트에 대응하는 데이터베이스 레코드들을 생성하는 것을 포함할 수 있다. 레코드들은 (상태 표시자를 통해) 액세스 제어 클라이언트의 현재 상태, 뿐만 아니라 데이터와 연관된 가입자, 및 데이터를 사용하도록 허가된 하나 이상의 디바이스들을 식별하기 위한 다른 정보를 예시하기 위해 사용될 수 있다.

[0075] 예를 들어, 일 예시적인 실시예에서, 내부 데이터베이스는 액세스 제어 클라이언트에 대한 상태 표시자를 초기화한다(도 8 및 하기에서 논의되는 연관된 논의를 참조하라). 상태 표시자는 액세스 제어 클라이언트가 현재 사용중인지(예를 들어, "사용중"), 현재 사용될 수 없는지(예를 들어, "유지됨"), 즉시 사용을 위해 이용가능한지(예를 들어, "이용가능함"), 그리고 사용을 위해 이용가능하지 않은지(예를 들어, "이용가능하지 않음")를 표시한다.

[0076] 방법(500)의 단계(510)에 따라, 액세스 제어 클라이언트가 저장된다. 일 실시예에서, 액세스 제어 클라이언트(예를 들어, eSIM 및 연관된 동적 데이터)는 클라이언트 지갑, 클라이언트 서버, 또는 전술 항목 중 하나와 통신하는 다른 엔티티에서 데이터 베이스 내에 저장된다. 추가로, 액세스 제어 클라이언트의 내부 상태는 현재 저장을 반영하도록 업데이트된다.

[0077] 이제 도 6을 참조하면, 사용자 디바이스들이 액세스 제어 클라이언트를 이용할 수 있게 하기 위한 예시적인 방법(600)이 예시된다.

[0078] 도시된 바와 같이, 단계(602)에 따라, 하나 이상의 저장된 액세스 제어 클라이언트들에 대한 요청이 수신된다. 예를 들어, 클라이언트 서버는 사용자 디바이스로부터 하나 이상의 액세스 제어 클라이언트들에 대한 요청을 수신한다. 또 다른 예에서, 클라이언트 지갑은 액세스 제어 클라이언트를 요청하는 사용자 또는 모바일 디바이스로부터의 요청을 수신한다.

[0079] 일 예시적인 실시예에서, UE의 사용자가 사용자의 디바이스의 사용자 인터페이스를 통해, 지갑 또는 클라이언트 서버에 의해 제공되는 이용가능한 eSIM의 리스트로부터 이용가능한 eSIM 데이터 중 특정 데이터를 선택하는 경우, 요청이 생성된다. 예를 들어, 지갑 디바이스는 모바일 디바이스가 이용할 수 있는 eSIM들의 리스트 또는 디렉토리를 생성하고, 사용자는 그에 응답하여 하나를 선택한다.

[0080] 또한 전술한 단계(602)가 "요청/응답" 모델을 이용하지만, 방법(600)은 또한 "푸시" 모델을 사용하여 동작하도록 구성될 수 있고, 이에 의해, 네트워크 디바이스(예를 들어, SPS 또는 TSM 등)는 요청의 수신 없이 이용가능한 eSIM의 리스트 및/또는 eSIM의 전달을 개시한다는 점이 이해될 것이다. 이는 미리 결정된 길이의 시간 동안 사용자 디바이스에 활성 eSIM이 없는 것이 검출되는 경우, 그리고/또는 계정 설정 시에, 또는 또 다른 환경 또는 방식(예를 들어, 규정된 주기로 또는 이벤트-구동 방식으로 클라이언트 디바이스들의 폴링) 하에서 발생할 수 있다.

[0081] 다음으로, 단계(604)에서, 요청을 수신하는 엔티티(예를 들어, 클라이언트 지갑, 클라이언트 서버)는 요청을 검증한다. 요청 디바이스/서버가 요청을 하도록 허가되어 있지 않고/않거나 인증되어 있지 않은 경우, 액세스 제어 클라이언트 데이터는 승인되지 않을 것이다.

[0082] 단계(606)에서, 요청 엔티티가 검증되면, 요청된 액세스 제어 클라이언트의 상태 표시자가 검토되고, 액세스 제어 클라이언트가 이용가능한지의 여부가 결정된다. 특정 요청 디바이스 및/또는 사용자에 의한 사용을 위한 액세스 제어 클라이언트의 이용가능성은 이용가능한 액세스 제어 클라이언트들의 데이터베이스를 조회함으로써 결정된다. 예를 들어, 지갑 및/또는 클라이언트 서버 또는 통신 중인 다른 엔티티(예를 들어, SPS, TSM 등)은

eSIM이 동작을 위해 이용가능함을 검증한다.

[0083] 예를 들어, 내부 상태 데이터베이스(예를 들어, 지갑)는 각각의 eSIM에 대한 상태 표시자를 제공한다(도 8 및 하기에 논의되는 연관된 논의를 참조하라). 상태 표시자는 요청되는 eSIM이 현재 사용중인지(예를 들어, "사용중"), 현재 사용될 수 없는지(예를 들어, "유지됨"), 즉시 사용을 위해 이용가능한지(예를 들어, "이용가능"), 그리고 사용을 위해 이용가능하지 않은지(예를 들어, "이용가능하지 않음")를 표시한다. 단계(606)에서, 요청된 액세스 제어 클라이언트가 이용가능하다고 결정되는 경우, 제어 클라이언트는 요청 엔티티에 송신된다(단계 608). 위에서 언급한 바와 같이, 전송들의 보안성을 보장하기 위한 하나 이상의 메커니즘들이 이용될 수 있다는 것을 알 것이다. 추가로 동적 데이터가 요청된 액세스 제어 클라이언트와 함께 제공될 수 있다는 것을 알 것이다.

[0084] 액세스 제어 클라이언트가 이용가능하며 요청 디바이스에 제공된다고 결정되는 경우, 액세스 제어 클라이언트의 상태가 이러한 새로운 사용을 반영하기 위해 데이터베이스에서 업데이트된다(단계 610). 위에서 논의한 바와 같이, eSIM 및 연관된 동적 데이터가 저장되는 경우, 레코드는 그와 연관된 상태 표시자와 연관된다. 이들은 액세스 제어 클라이언트를 제공하기 위한 엔티티(예를 들어, 클라이언트 서버 또는 지갑)와 통신하는 데이터베이스에 저장된다. 표시자는 eSIM 데이터의 새로운 사용(또는 중단된 사용)을 예시하기 위해 업데이트된다.

[0085] 단계(606)에서, 요청된 액세스 제어 클라이언트가 이용가능하지 않다고 결정된 경우(그것이 "사용중", "유지됨" 또는 "이용가능하지 않음"이므로), 단계(612)에 따라, 메시지가 요청 디바이스에 제공된다. 메시지는 요청된 액세스 제어 클라이언트가 이용가능하지 않음을 표시할 수 있고, 또한, 이용가능하지 않은 것에 대한 이유를 제공할 수 있다(예를 들어, 디바이스가 로밍 중인 동안 eSIM이 이용가능하지 않지 않음, 또 다른 eSIM이 해당 동일한 디바이스 상에서 사용중인 동안 eSIM이 이용가능하지 않음 등).

[0086] 일 실시예에서, 오리지널 eSIM 데이터가 클라이언트 서버 또는 지갑에서 유지되는 반면, 그 사본이 요청 엔티티에 제공된다(전송 이후 eSIM을 제거하는 것에 반해). 본원의 다른 곳에서 논의되는 바와 같이, 이러한 실시예는 특히 eSIM 백업을 제공하기에 유용하다. 데이터베이스는 제어 클라이언트가 사용중이며 다시 송신될 수 없음을(비록 그것이 저장소 내에 지속하더라도) 반영하기 위해 업데이트된다. 이러한 방식으로, 동일한 eSIM이 임의의 한 시점에 하나 초과의 디바이스에 제공되는 것이 방지된다. 그러나, 원할 경우, 주어진 eSIM이 하나 초과의 디바이스에서의 전달 및 동시 사용을 위해 마킹될 수 있다는 것을 알 것이다(이러한 기능은 데이터베이스 내의 eSIM의 상태 표시자에 의해 보여짐).

[0087] 많은 경우들에서, eSIM 데이터가 또 다른 디바이스에서의 후속 사용을 위해 이용가능하게 되도록 하기 위해 eSIM 데이터는 제공 엔티티(예를 들어, 클라이언트 서버 또는 지갑)에서 복원되어야 한다. 그러나, 단일 eSIM이 다수의 디바이스들에서 이용될 수도 있다는 것을 알 것이다. 한번에 하나 또는 하나 초과의 디바이스에서 사용될 수 있는 특정 eSIM의 능력이 하기에 논의되는 상태 표시자에서 예시된다.

[0088] 또한, 전술한 방법들 및 장치는 사용자 또는 네트워크 운영자로 하여금 분실된 또는 제대로 기능하지 않는 eSIM의 경우 디바이스로 eSIM들을 복원하게 한다. 예를 들어, 사용자는 지갑에서 이전에 저장된 백업으로부터 디바이스를 복원시킴으로써 고장난 또는 손상된 eSIM 프로파일을 복원시킬 수 있다. 이러한 방식으로, 백업 및 복원은 중개인 또는 통신 사업자의 도움 없이 유리하게 수행될 수 있다. 클라이언트 서버로부터의 백업이 수행될 수도 있지만, 클라이언트 서버는 중개인 또는 통신 사업자 엔티티에 의한 추가적인 검증 정보 및/또는 허가를 요구할 수 있다.

[0089] 위에서 논의한 바와 같이, 액세스 제어 클라이언트가 디바이스에 의해 요청되거나 디바이스에 제공되는 경우, 데이터의 물리적 사본은, 일 실시예에서, 제공 디바이스(예를 들어, 클라이언트 서버 또는 지갑)에 유지되고, 디바이스에는 (예를 들어, eSIM 및 동적 데이터를 포함하는) 데이터의 사본이 제공된다. 또한 위에서 언급한 바와 같이, 제공 디바이스에 상주하는 사본의 후속 사용은 데이터베이스에 표시된 상태의 영향을 받는다. 예를 들어, "이용가능하지 않은" 상태는, 제2 사본이 다른 곳에서 이용가능하지 않으며, 상주하는 사본이 추가적인 디바이스들에서의 사용을 위해 이용가능하지 않음을 표시한다. 이러한 실시예에 따라, 클라이언트 서버 또는 지갑 디바이스에서의 사용을 위해, 또는 도 7에 예시된 바와 같이 또 다른 디바이스(예를 들어, UE)로의 후속 전송을 위해, 또는 클라이언트 서버 또는 지갑 디바이스에서 한 번 더 제어 클라이언트를 이용할 수 있게 하기 위한 방법이 필요하다. eSIM이 필요하지 않고/않거나 디바이스에 의해 사용되지 않는 경우, 도 7의 방법을 통해 eSIM이 또한 제공 엔티티에 복귀될 수도 있다는 점에 유의한다.

[0090] 이제 도 7의 방법을 참조하면, 제어 클라이언트를 복귀시키는 것(또는 "사인 인"하는 것)은 디바이스로부터 액

세스 제어 클라이언트를 클리어하기 위한 사용자 선택 이전에 또는 사용자 선택과 동시에 수행될 수 있다. 다시 말해, 디바이스의 사용자가 (예를 들어, 상이한 eSIM을 사용하기 위해) 그의 디바이스로부터 eSIM을 삭제하는 경우, 도 7의 방법이 수행되지 않는 한 eSIM은 제거되지 않을 것이다. 대안적으로, eSIM은, 예를 들어, SPS, TSM 또는 다른 네트워크 엔티티로부터의 명시적인 명령의 수신 시에 명시적으로 제거될 수 있다.

[0091] 도시된 바와 같이, 방법의 단계(702)에 따라, 액세스 제어 클라이언트를 복귀시키기 위한 명령이 수신된다. 명령은 미리 결정된 기간 이후, 또는 또 다른 방식에 따라 자동으로 생성될 수 있다. 예를 들어, 특정 eSIM은 그것이 복귀되어야할 만료 시간/날짜를 가질 수 있다. 대안적으로, 복귀 명령은 사용자가 선택된 eSIM을 복귀시키기 위한 기능을 인스턴스화(instantiate)하는 경우 생성될 수 있다.

[0092] 클라이언트 지갑 실시예에서, 단계(702)의 복귀 명령은 UE로부터 지갑 또는 서버로 무선으로 송신될 수 있다. 대안적으로, 복귀 명령은 예를 들어, (예컨대, USB, IEEE-1394 등을 통한) 도킹 또는 다른 접속 동안, 디바이스들의 서로에 대한 유선 접속 시에 인스턴스화될 수 있다.

[0093] 또 다른 실시예에서, 복귀 프로세스는 지갑, SPS 및/또는 다른 네트워크 엔티티로부터 수신되는 신호에 응답하여 인스턴스화될 수 있다. 예를 들어, 사용자로부터 발신된 특정 eSIM에 대한 요청이 지갑, 클라이언트 서버, SPS, TSM 또는 다른 신뢰할 수 있는 네트워크 엔티티에서 수신될 수 있다. 요청에 응답하여, 요청된 eSIM이 (또 다른 디바이스에 배치되어 있거나 그것에 의해 의해 사용중이므로) 현재 이용가능하지 않다고 결정되는 경우, 지갑, 클라이언트 서버 등은 (예를 들어, 무선 전송 메커니즘을 통해) 요청된 eSIM을 현재 사용하고 있는 디바이스에 전송되는 메시지를 생성한다. 메시지는 또 다른 사용자 또는 디바이스가 제어 클라이언트로의 액세스를 요청하고 있음을 표시하며, 여기서 논의된 복귀 프로세스(도 7)를 자동으로 시작하거나, 또는 디바이스의 사용자로 하여금 복귀 프로세스를 시작하거나 액세스를 거절하도록 선택하게 할 수 있다.

[0094] 다음으로, 방법은 단계(704)로 진행하며, 여기서, 마커(상태 표시자)는 액세스 제어 클라이언트가 현재 이용가능하거나 더 이상 사용중이 아님을 반영하도록 업데이트된다. 일 실시예에서, 상태 표시자를 업데이트하기 전에, 지갑, 클라이언트 서버, SPS, TSM, 네트워크 엔티티 등은 우선 복귀 프로세스가 요청된 특정 액세스 제어 클라이언트가 현재 사용중이 아닌 것으로서 데이터베이스에서 보여지는지의 여부를 결정한다는 것을 알 것이다. 일반적으로, 상태의 임의의 불일치는 제어 클라이언트의 이전 사용이 잠재적으로 불법적이거나, 은밀했을 수 있거나, 제어 클라이언트에 대한 사용/재생 규칙에 따르지 않음을 나타낼 수 있다. 따라서, 일부 실시예들에서, 상태 에러들은 네트워크 관리자 또는 다른 관할 엔티티(cognizant entity)에 보고된다.

[0095] 마지막으로, 단계(706)에서, 액세스 제어 클라이언트는 디바이스에서의 저장소로부터 제거된다. 이러한 제거는 (i) 완전한 제거 또는 소거, 또는 대안적으로 (ii) 제어 클라이언트를 액세스할 수 없고 그리고/또는 복사할 수 없도록 그것을 디스에이블시키고, 가능한 추후의 재활성화를 위해 클라이언트에 디스에이블된 사본을 남기는 것, 또는 (iii) 정확한 암호해독 키를 가지는 허가된 엔티티에 의해서만 액세스가 허용되는 암호화를 포함할 수 있다.

[0096] 여기서 논의된 복귀 프로세스는 UE에 저장된 액세스 제어 클라이언트의 버전을 삭제하고 클라이언트 서버 또는 지갑에 저장된 액세스 제어 클라이언트의 오리지널 버전의 상태를 복원하는 것을 포함하지만, 또 다른 실시예에서, 오리지널 제어 클라이언트가 이들 엔티티들 사이에 다시 복사될 수 있으며, 상주하는 사본이 단순히 디스에이블된다는 것을 알 것이다.

[0097] 본 발명의 또 다른 양상에서, 예를 들어, SPS, 클라이언트 서버, UE, 지갑, 또는 다른 위치에 배치된 추가적인 컴퓨터 프로그램들이 운영 규칙들을 호출하기 위해 이용된다. 운영 규칙들은, 예를 들어, 네트워크 최적화 및 신뢰성 목표, 증가된 유지보수 간격들, 증가된 가입자 또는 사용자 만족, 증가된 가입 기반, 더 높은 이익 등을 포함하는 운영 또는 사업에 관련된 하나 이상의 목표들(예를 들어, 이익)을 달성하기 위해 사용된다.

[0098] 예를 들어, 본 발명의 일 실시예에서, 액세스 제어 클라이언트들에 대한 경쟁 사용들 또는 요청들에 대한 다양한 논리 규칙들이 구현될 수 있다. 예를 들어, "우선 도달 우선 서빙" 패러다임이 사용될 수 있으며, 여기서, 제1 사용자(예를 들어, 위의 예에서 제1 UE)에게 우선순위 및 제2 또는 후속하는 요청들을 거절하는 권한이 주어진다. 대안적으로, 사용자 또는 디바이스 프로파일이 우선순위를 설정하는 기반으로서 사용될 수 있는데, 예를 들어, 위의 예에서의 제2 (요청) 사용자는 더 높은 특권을 가지는 사용자를 포함할 수 있고, 이 경우, 콘텐츠가 제1 디바이스로부터 체크 아웃되어 제2 클라이언트에 제공된다. 또 다른 대안으로서, 액세스 제어 클라이언트를 사용할 시에 사용자의 경험을 간섭하지 않기 위해, 복귀가 수행되기 전에 진행중인 서비스의 완료를 허용하도록, 복귀 프로세스가 지연될 수 있다. 또 다른 모델로서, 요청들의 시간 또는 횟수에 대해 할당의 균형

을 맞추기 위해 "라운드 로빈" 또는 다른 공유 방식이 사용될 수 있다.

[0099] 또 다른 이러한 예에서, eSIM, 동적 데이터, 또는 여기서 논의된 바와 같은 다른 액세스 제어 클라이언트의 분배 또는 이들로의 액세스(그리고, 일부 경우들에서, 예를 들어, 클라이언트 서버, SPS, 지갑, 및/또는 UE의 동작)를 제어하도록 적응된 하나 이상의 소프트웨어 루틴들이 사용된다. 규칙들은 별도의 엔티티 또는 프로세스를 포함할 수 있거나, 또는 다른 프로세싱 엔티티들(예를 들어, SIM 제공 애플리케이션, eSIM 지갑 애플리케이션 및/또는 클라이언트 eSIM 관리 애플리케이션) 내에 완전히 통합될 수 있다.

[0100] 액세스 제어 클라이언트들(예를 들어, eSIM)의 분배 및 사용이 특정 운영 프로토콜들 또는 결정 프로세스들(위에서 논의된 바와 같은), 네트워크 내에 존재하는 실제 또는 예상되는 조건들 등에 따라 발생할 수 있다는 것을 알 것이다. 예를 들어, 위에서 논의된 실시예들에서, 특정 eSIM이 이용가능하고(일부 경우들에서, 또 다른 디바이스 상에서 이미 사용 중이 아니고) 요청 디바이스가 그 eSIM을 사용하도록 허가되어 있는 경우 그 eSIM이 그 디바이스에 제공될 것이다. 그러나, 이러한 결정 프로세스들은, 레이턴시 감소, 이익 또는 시스템 신뢰성의 최대화와 같은, 더 높은 레벨의 사업 또는 운영 목표들과 항상 일치하는 것은 아닐 수 있다. 따라서, 사업/운영 규칙들은, 시행되는 경우, 다수의 디바이스들에 걸쳐 액세스 제어 클라이언트의 분배 및/또는 사용을 동적으로(또는 수동으로) 제어하기 위해 사용될 수 있다.

[0101] 구현되는 한 가지 규칙은 가입자 클래스에 따라 특정 UE로 eSIM의 전달 및/또는 사용을 가능하게 하는 것을 포함할 수 있다. 다시 말해, 제1 클래스의 가입자는 이용가능한 eSIM 중 특정한 것들만 수신하도록 허용될 수 있고, 그리고/또는 제1 클래스의 가입자와 연관된 지갑은 제한된 개수의 추가 디바이스들에만 eSIM을 전송하도록 허용될 수 있다. 그러나, 더 높은 클래스의 가입자는 모든 eSIM 또는 업그레이드된 eSIM(하기에 논의됨)을 수신할 자격을 부여받을 수 있고, 그리고/또는 더 높은 클래스의 가입자와 연관된 지갑은 제한되지 않은 개수 및 타입의 디바이스들에 eSIM을 전달할 수 있다.

[0102] 유사하게, 요청된 eSIM의 전송은 오직 특정 조건을 만족시키는 디바이스들 및/또는 가입자들만을 대상으로 제어될 수 있다. 예를 들어, 요청 디바이스가 업그레이드된 eSIM을 사용하기 위해 필수적인 기능성을 소유하지 않는 경우, 이는 업그레이드된 eSIM으로의 액세스를 거절당할 수 있다. 대안적으로, 디바이스 또는 가입자 제한들을 만족시키는 eSIM이 액세스의 거절 시에도 제공될 수 있다.

[0103] 또 다른 실시예에서, 특정 eSIM에 만료 날짜/시간이 주어지는 규칙이 구현될 수 있다. 말하자면, 주어진 eSIM이 특정 디바이스에 얼마나 상주할 수 있는지에 대해 제한이 설정될 수 있고, 그리고/또는 특정 시간 기간 동안 특정 eSIM(및 다른 기간들에서 상이한 eSIM)을 갖는 스케줄이 사전-설정될 수 있다. 시간 제한 또는 스케줄링된 시간이 만료되면, eSIM은 디바이스로부터 자동으로 삭제될 수 있고, eSIM 복귀 프로세스(도 7 참조)가 개시된다.

[0104] 추가적인 실시예에서, 업그레이드된 또는 "스마트" eSIM이 제공될 수 있다. 스마트 eSIM은 eSIM을 사용하는 가입자의 가입 레벨 및/또는 디바이스의 타입에 기초하여 사용자(들)에게 제공되는 서비스들을 조정할 수 있다. 예를 들어, 스마트 eSIM은 그 eSIM이 예컨대 스마트폰으로부터 소위 "피처 폰(feature phone)"으로 이동되는 경우 특정 기능들 또는 서비스들이 인에이블/디스에이블되도록 할 수 있고, 소위 "덤 폰(dumb phone)"으로 이동되는 경우 훨씬 더 많은 기능들이 디스에이블되도록 할 수 있다.

[0105] 예를 들어, eSIM 배포자를 위한 이익을 생성하기 위한, 사업 규칙들이 구현될 수도 있다. 특히, 위에서 언급한 바와 같이, 독립형 클라이언트 서버는 서비스 중개자에 의해 관리될 수 있고, 이러한 서비스 중개자는 하나 이상의 MNO들에 대해 파트너가 되지만, SPS로부터 분배되는 eSIM으로의 액세스를 위해 할증금을 명령하는 디바이스 제조자를 포함할 수 있다. 예를 들어 각각의 가입자가 그것에 액세스가 주어지는 각각의 eSIM에 대해 할증금을 지불해야 하는 경우, 가격 책정 구조들은, 예를 들어, eSIM마다 기반으로 유도될 수 있다. 하나 초과의 디바이스에서 사용될 수 있는 eSIM, 하나 초과의 디바이스에서 동시에 사용될 수 있는 eSIM, 및/또는 스마트 eSIM과 같은 더 고급의 eSIM은 다른 eSIM보다 더 높은 할증금으로 제공될 수 있다는 것을 알 것이다. 추가로 지갑 UE 특징과 같은, 여기서 논의된 특정 특징들은 고급 또는 업그레이드된 가입들을 요구하도록 구성될 수 있다는 것을 알 것이다.

[0106] 추가로, eSIM에 기초하여 가입자 청구서를 분할하거나 결합하기 위한 규칙들이 구현될 수 있다. 다시 말해, 가입자는 모든 디바이스들에서 모든 eSIM에 대한 사용에 대한 단일 청구서를 수신하기로 선택할 수 있다. 대안적으로, 가입자는, 각각의 청구서가 eSIM이 사용된 디바이스와 무관하게 가입자에 연관된 단일 eSIM에 대한 사용을 나타내는, 다수의 청구서들을 수신하기로 선택할 수 있다.

[0107] 추가로, 클라이언트 서버는 전술한 서비스 중개자(예를 들어, 디바이스 제조자)에 의해 관리되고, eSIM 액세스에 대한 메커니즘들 및 사업 규칙들을 제공할 수 있다는 것을 알 것이다. 일 실시예에서, 사용자는 UE를 구매하고, 이후, 인터넷 또는 다른 통신 네트워크를 통해, eSIM으로의 사후- 또는 사전-지불 액세스를 요청할 수 있다. 서비스 중개자는 이러한 실시예에 따라 (예를 들어, 과금 관리 등에 의해) MNO의 기능들 중 다수를 수행한다.

[0108] **eSIM 데이터베이스-**

[0109] 이제 도 8을 참조하면, 상태 표시자들 및 허가된 디바이스들이 연관되어 있는 이용가능한 eSIM의 예시적인 데이터베이스가 도시되어 있다. 예시된 바와 같이, 하나 초과의 eSIM은 단일 가입자에 연관될 수 있다. 예를 들어, [eSIM 1], [eSIM 2] 및 [eSIM 3]은 각각 가입자 1에 연관된다. 도시된 바와 같이, [eSIM 1]은 디바이스 A상에서 현재 사용중인 반면, [eSIM 2] 및 [eSIM 3]은 "유지됨" 상태이다. "유지됨" 상태는 [eSIM 2] 및 [eSIM 3]이, 비록 또 다른 eSIM의 사용과 동시에 사용되는 것은 아니지만, 디바이스 A에 의해 사용될 수 있는 대체 eSIM이라는 것을 표시한다.

[0110] 도 8은 단일 가입자가, 각각의 디바이스가 하나 이상의 eSIM을 가지는 하나 초과의 디바이스와 연관될 수 있음을 추가로 예시한다. 예를 들어, [eSIM 4] 및 [eSIM 5]은 모두 가입자 2와 연관된다. 그러나, [eSIM 4]은 디바이스 B에만 허가되어 있고, [eSIM 5]은 디바이스 C에만 허가되어 있다. 도 8의 [eSIM 5]의 상태는 현재 "이용가능하지 않음"이다. 이 상태는, 이 시간에 특정 eSIM을 사용하는 것이 바람직하거나 가능하지 않음을 표시한다. 이것은, 예를 들어, 디바이스가 로밍중이고, 특정 eSIM이 로밍 동안 사용될 수 없는 경우 발생할 수 있다.

[0111] 또한, 도 8에 예시된 바와 같이, 단일 디바이스는 한번에 하나 초과의 eSIM을 수용하고 사용할 수 있다. 예를 들어, 데이터베이스는 [eSIM 6] 및 [eSIM 7]이 모두 (가입자 3에 의해 동작되는) 디바이스 D에서의 사용을 위해 이용가능함을 표시한다. 도 8은 또한, 단일 eSIM이 동시에 다수의 디바이스들에서 사용중일 수 있음을 예시한다(즉, [eSIM 6]은 현재 디바이스 D 및 E에서 "사용중"이다).

[0112] **클라이언트 서버-**

[0113] 도 9는 본 발명에 유용한 클라이언트 서버(412)의 일 예시적인 실시예를 예시한다. 위에서 논의된 바와 같이, 클라이언트 서버는 독립형 엔티티를 포함할 수 있거나, 다른 네트워크 엔티티들(예를 들어, SPS, TSM 등)과 통합될 수 있다. 도시된 바와 같이, 클라이언트 서버(412)는 일반적으로 통신 네트워크(408)와 인터페이싱하기 위한 네트워크 인터페이스(902), 프로세서(904), 저장 장치(908), 및 다양한 백 엔드 인터페이스들을 포함한다. MNO 인터페이스(910)가 예시되어 있지만, 이러한 인터페이스는 생략되거나, 교체되거나 복제될 수 있다는 것을 알 것이다. 다른 인터페이스들이 또한 이용될 수 있으며, 전술 항목은 단지 예시적이다. MNO 인터페이스(910)는 클라이언트 서버(412)로 하여금 하나 이상의 MNO(406)와 통신할 수 있게 한다.

[0114] 예시된 실시예에서, 클라이언트 서버(412)는 적어도 그의 프로세서에서 실행하는 SIM 데이터베이스(906)를 포함한다. 클라이언트 서버에서 실행하는 단일 애플리케이션으로서 예시되어 있지만, 전술한 데이터베이스 기능은 서로 데이터 통신하는 복수의 엔티티들에서 실행하는 분산된 애플리케이션을 포함할 수 있다는 것을 알 것이다.

[0115] 데이터베이스 애플리케이션은, (i) 특정 eSIM이 저장될 것을 요청하는 통신, (ii) 저장된 하나 이상의 eSIM으로의 액세스를 요청하는 통신 및/또는 (iii) 특정 UE(404)에 이전에 전송된 eSIM의 복귀를 요청하는 통신과 같은 통신들을 UE(404)로부터 수신한다. 데이터베이스 애플리케이션은 또한 위의 요청들이 허가된 엔티티들로부터 수신되며 어떠한 보안 우려도 존재하지 않음을 보장하기 위해 위의 요청들을 검증할 책임이 있다.

[0116] 데이터베이스 애플리케이션은 이용가능한 eSIM들의 데이터베이스를 저장하도록 구성된다. 도 8에 예시된 바와 같이, 데이터베이스는 특정 eSIM과 연관된 가입자, eSIM을 사용하도록 허가된 디바이스들, 및 eSIM의 현재 상태에 관련된 정보를 제공할 수 있다. 추가적인 정보들이 또한 유지될 수 있다. 마찬가지로, 데이터베이스 애플리케이션은 데이터베이스에 저장된 정보를 변경하거나 업데이트하도록 구성된다. 예를 들어, 애플리케이션은 특정 eSIM이 "이용가능함", "사용중", "이용가능하지 않음" 등임을 반영하도록 현재 상태 정보를 업데이트하는 데 사용될 수 있다. 허가된 가입자들, 허가된 디바이스들 등에 대한 변경들도 데이터베이스 애플리케이션에 의해 데이터베이스에서 이루어질 수 있다.

[0117] 사용자 또는 디바이스가 클라이언트 서버(412)로부터 eSIM을 요청하는 경우, 데이터베이스 애플리케이션은 요청된 eSIM의 현재 상태뿐만 아니라, 요청된 eSIM이 제공될 수 있는지의 여부를 결정할 책임이 있다. eSIM이 이용

가능하며 제공될 수 있는지의 여부에 대한 결정은 요청 가입자 또는 디바이스, 및/또는 요청된 eSIM에 대해 특정적일 수 있다. 예를 들어, 데이터베이스 애플리케이션은 네트워크 엔티티들(예를 들어, 과금 엔티티들 등)에 조회하여 요청 사용자 또는 디바이스에 대한 서비스 레벨 또는 계층을 결정하도록 구성될 수 있다. 이러한 정보는 이후, 요청 사용자 또는 디바이스가 요청된 eSIM에 액세스할 수 있는지의 여부를 결정하기 위해 이용될 수 있다. 대안적으로, 데이터베이스 애플리케이션은 조회에 응답하여 또는 자동적으로, 별도의 엔티티(예를 들어, eSIM을 생성하는 엔티티, 또는 전술한 결정들을 수행할 책임이 있는 또 다른 네트워크 엔티티)로부터 각각의 eSIM에 대한 규칙들을 단순히 수신할 수 있다.

[0118] 추가로, 데이터베이스 애플리케이션은 그와 통신 중인 각각의 디바이스에 대해 특정적인 이용가능한 eSIM의 리스트를 생성하기 위해 사용될 수 있다. 일 실시예에서, 이는 단순히, 특정 가입자, 디바이스 등에 대해 이용가능한 eSIM의 데이터베이스의 조회를 수행하고, 이 조회의 결과들을 선택가능한 리스트의 형태로 요청 디바이스에 제공함으로써 달성될 수 있다.

[0119] 마지막으로, 데이터베이스 애플리케이션은 선택적으로, eSIM의 불법적 또는 허가되지 않은 사본이 생성되고 그리고/또는 배포되었다고 생각되는 경우, 시스템 관리자에 대한 통지들을 생성할 수 있다.

[0120] **사용자 장비(UE) -**

[0121] 도 10은 여기서 논의되는 다수의 eSIM 관리 특징들에서 사용하기 위한 예시적인 사용자 디바이스(404)를 예시하는 블록도이다. 위에서 논의된 바와 같이, UE(404)는, 일부 실시예들에서, 내부 지갑 디바이스를 포함할 수 있다.

[0122] 예시된 바와 같이, 도 10의 예시적인 UE(404)는 통신 네트워크(408)(및 클라이언트 서버를 포함하는 그의 엔티티들)와 통신하기 위한 네트워크 인터페이스(1002)를 포함한다. UE(404)는 또한, 네트워크 인터페이스(1002)를 통해 클라이언트 서버와 통신할 수 있다. 일 실시예에서, UE는 이러한 인터페이스를 통해 eSIM들을 요청하고 수신한다. UE는 디지털 프로세서(1004) 및 연관된 저장소(1010)를 더 포함하고, 디지털 프로세서는 그것에서 다양한 애플리케이션들을 실행하도록 구성된다. 복수의 백-엔드 인터페이스들이 또한 예시되어 있다. 사용자 인터페이스(1012) 및 디바이스 인터페이스(1014)가 예시되어 있지만, 이들 중 어느 하나 또는 둘 모두가 생략되거나, 교체되고, 복제될 수 있다는 것을 알 것이다. 대안적인 인터페이스들이 또한 이용될 수 있다. 사용자 인터페이스는 UE로 하여금, 예를 들어, 메시지들을 디스플레이하고 사용자에게 서비스들을 제공하기 위해 디바이스의 사용자와 통신할 수 있게 해준다. 일 실시예에서, 선택적 디바이스 인터페이스는 디바이스로 하여금 또 다른 디바이스, 예를 들어, 지갑 또는 클라이언트 서버와 통신할 수 있게 해주는 유선 또는 무선 인터페이스를 포함한다.

[0123] 프로세서(1004)는 (i) 포괄적 SIM 기능 애플리케이션(1006), (ii) eSIM 지갑 애플리케이션(1008) 중 하나 이상을 실행하도록 구성된다.

[0124] 포괄적 SIM 기능 애플리케이션(1006)은, 일 실시예에서, 네트워크 엔티티로부터 제공되는 복수의 "포괄적" SIM 또는 다른 데이터를 수신하고 UE에게 이를 저장하도록 지시할 책임이 있다. 포괄적 SIM 기능 애플리케이션은 (i) 포괄적 액세스 제어 클라이언트를 요청하고, (ii) 포괄적 액세스 제어 클라이언트를 수신하고, (iii) 포괄적 액세스 제어 클라이언트의 저장을 지시하고, 그리고/또는 (iv) 포괄적 액세스 제어 클라이언트의 특정 클라이언트들의 사용을 지시하기 위해 이용될 수 있다.

[0125] 디바이스가 지갑 디바이스(410)를 포함하는 경우, eSIM 지갑 애플리케이션(1008)은 액세스 제어 클라이언트(eSIM)를 수신하고, 저장하고, 복수의 UE(404)에 제공하기 위해 이용될 수 있다. 지갑 애플리케이션(1008)은 각각의 eSIM의 현재 상태 및 허가된 디바이스들에 관한 정보를 포함할 수 있는 이용가능한 eSIM의 데이터베이스를 생성하기 위해 사용될 수 있다.

[0126] 지갑 애플리케이션(1008)은 다양한 UE(404)로부터 eSIM의 개별 eSIM으로의 액세스에 대한 요청을 더 수신할 수 있다. 지갑 애플리케이션은 특정 eSIM 데이터에 대한 요청이 요청 디바이스, 요청 디바이스와 연관된 사용자, 및 특정 eSIM 내에 포함되거나 특정 eSIM과 연관되는 정보에 적어도 부분적으로 기초하여 서비스될 수 있는지의 여부를 결정하기 위해 사용될 수 있다. 지갑 애플리케이션(1008)은, 예를 들어, 요청된 컨텐츠의 상태에 대해, 컨텐츠가 유지되어 있는 저장 엔티티에 조회함으로써 이를 수행할 수 있다.

[0127] eSIM이 제공되는 경우, 지갑 애플리케이션(1008)은 UE(404)에서 데이터베이스 내의 데이터와 연관된 상태 표시자를 업데이트한다. 대안적으로, 지갑 또는 eSIM 애플리케이션들은 클라이언트 서버(412) 등과 같은 외부 엔티

티에서 eSIM의 상태를 업데이트하기 위한 메시지를 송신할 수 있다.

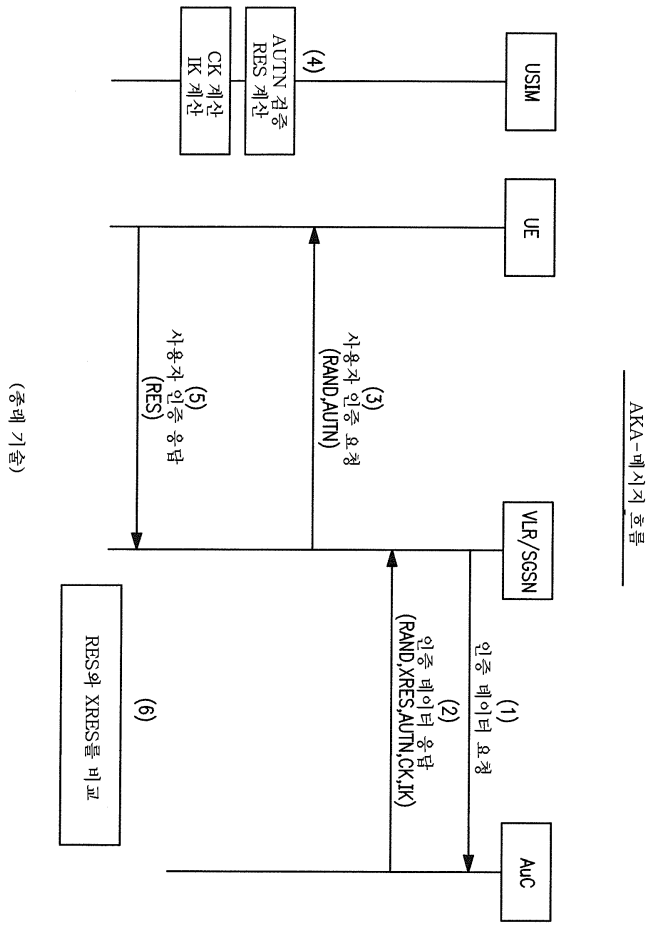
[0128] UE(404)의 저장 디바이스(1010)는, 위에서 참조된 동적 데이터를 포함하여, 복수의 이용가능한 액세스 제어 클라이언트를 저장하도록 구성될 수 있다. 저장 디바이스(1010)는 프로세서(1004)에서 실행되는 전술한 컴퓨터 애플리케이션들을 더 저장할 수 있다. 저장 디바이스(1010)는 예를 들어, 랜덤 액세스 메모리(RAM), 하드 디스크 드라이브, 광학 드라이브(예를 들어, CD-ROM 또는 DVD), NAND/NOR 플래시 메모리, 또는 이들의 어떤 조합을 포함할 수 있다.

[0129] 본 발명의 특정 양상들이 방법의 단계들의 특정 순서의 관하여 기술되지만, 이들 기술들은 단지 본 발명의 더 광범위한 방법들을 예시하는 것일 뿐이며, 특정 응용에 의해 요구되는 경우 수정될 수 있다는 것을 인지할 것이다. 특정 단계들은 특정 환경들에서 불필요하거나 선택적이 될 수 있다. 추가로, 특정 단계들 또는 기능이 개시된 실시예들에 추가될 수 있거나, 또는 둘 이상의 단계들의 수행 순서가 치환될 수 있다. 모든 이러한 변형예들은 여기서 청구되고 개시된 본 발명 내에 포함되는 것으로 간주된다.

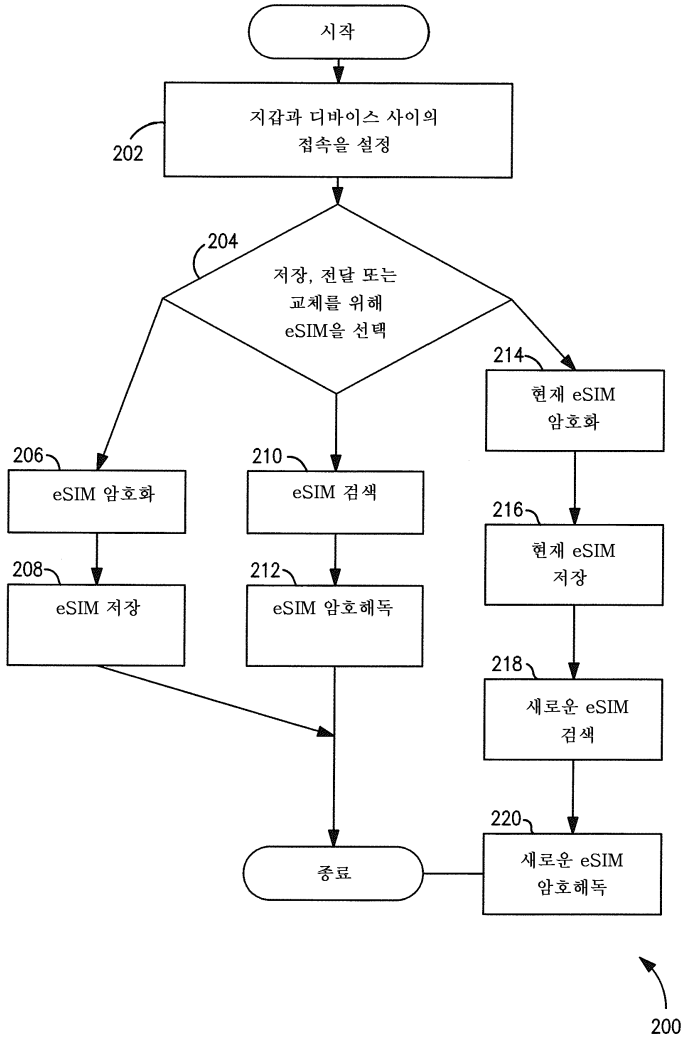
[0130] 위의 상세한 설명이 다양한 실시예들에 적용된 본 발명의 신규한 특징들을 도시하고, 기술하고, 지정하였지만, 예시된 디바이스 또는 프로세스의 세부 사항 및 및 형태에서 다양한 생략, 교체 및 변경들이 본 발명으로부터 벗어나지 않고 당업자에 의해 이루어질 수 있다는 것을 이해할 것이다. 전술한 기재는 본 발명을 수행하는 현재 고려되는 최적의 방식이다. 이러한 기재는 결코 제한적인 것으로 의도되는 것이 아니라, 오히려 본 발명의 일반적 원리들을 예시적인 것으로서 간주되어야 한다. 본 발명의 범위는 청구항들을 참조하여 결정되어야 한다.

도면

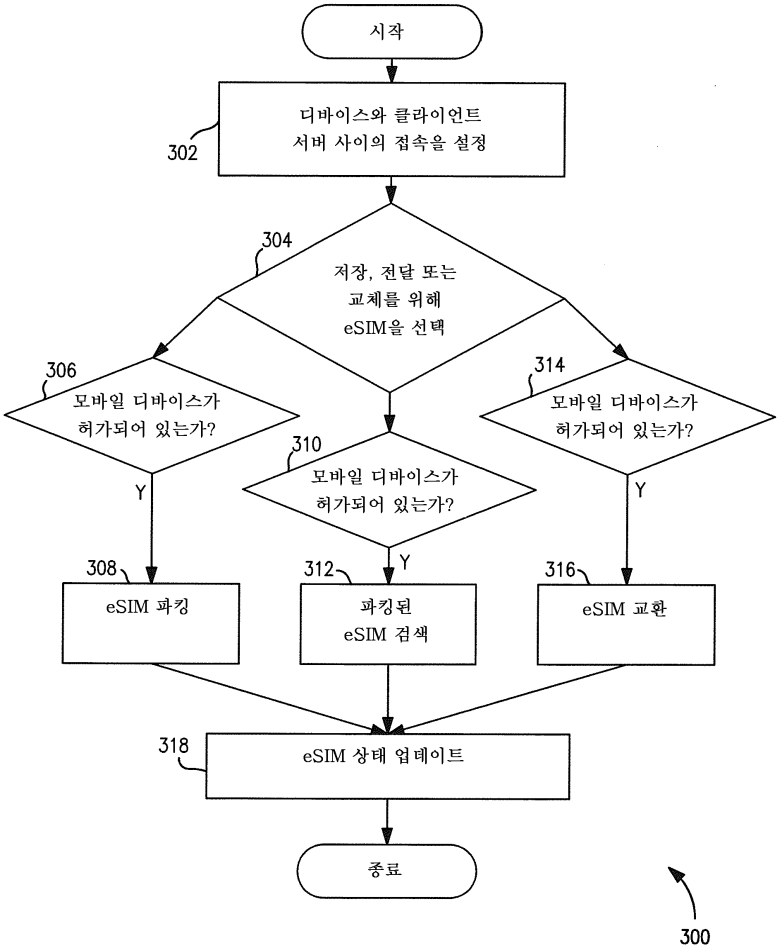
도면1



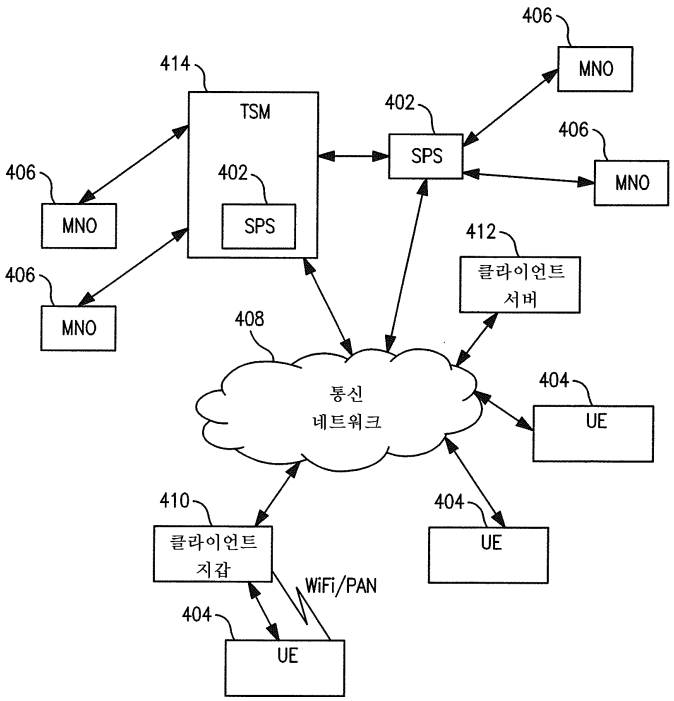
도면2


시작
지갑과 디바이스 사이의 접속을 설정
202
204
저장, 전달 또는 교체를 위해 eSIM을 선택
206
eSIM 암호화
208
eSIM 저장
210
eSIM 검색
212
eSIM 암호해독
214
현재 eSIM 암호화
216
현재 eSIM 저장
218
새로운 eSIM 검색
220
새로운 eSIM 암호해독
종료
200

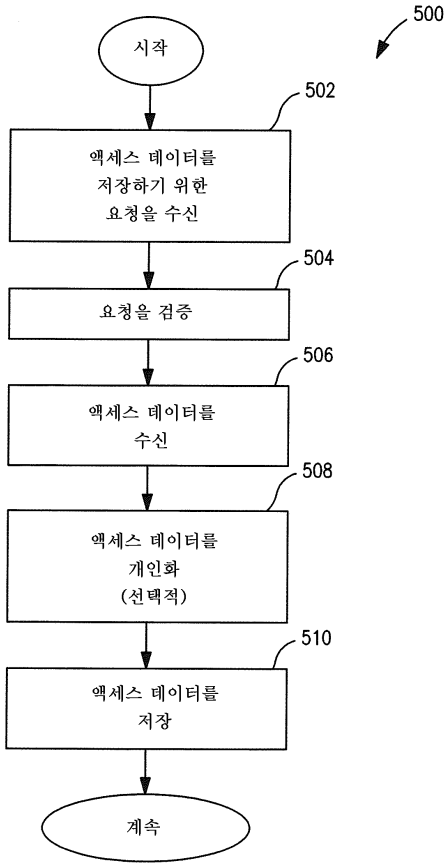
도면3


시작
디바이스와 클라이언트
서버 사이의 접속을 설정
302
304
저장, 전달 또는
교체를 위해
eSIM을 선택
306
모바일 디바이스가
허가되어 있는가?
310
모바일 디바이스가
허가되어 있는가?
314
모바일 디바이스가
허가되어 있는가?
Y
Y
Y
308
eSIM 파킹
312
파킹된
eSIM 검색
316
eSIM 교환
318
eSIM 상태 업데이트
종료
300

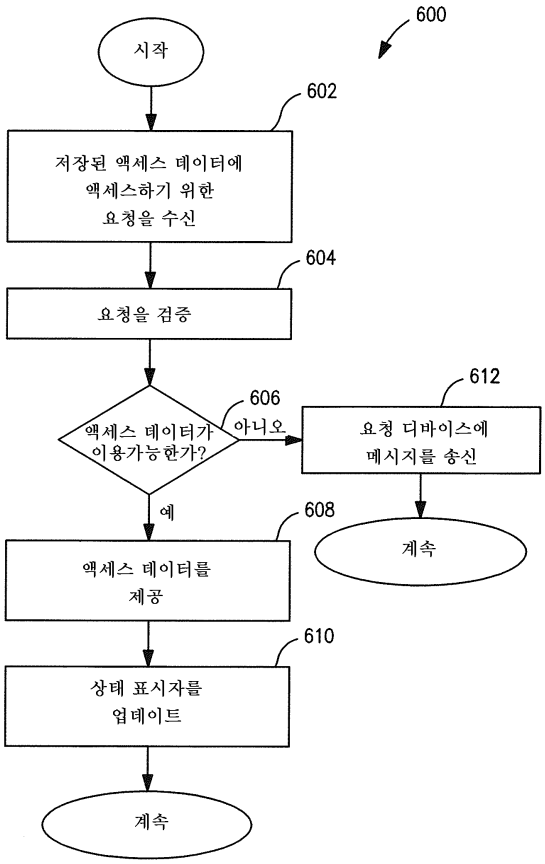
도면4


406
MNO
414
TSM
402
SPS
406
MNO
406
MNO
402
SPS
406
MNO
412
클라이언트
서버
408
통신
네트워크
404
UE
410
클라이언트
지갑
404
UE
WiFi/PAN
404
UE

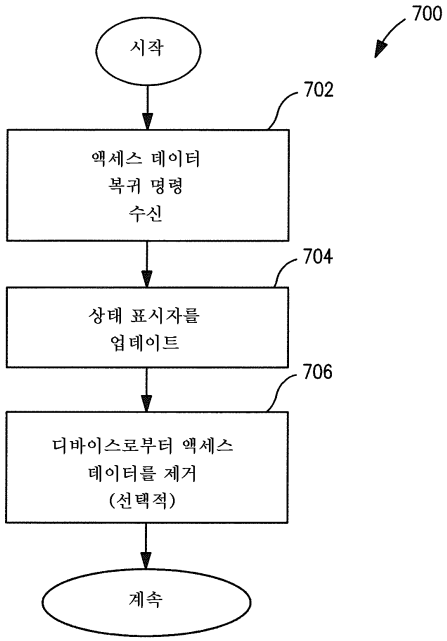
도면5


500
시작
502
액세스 데이터를
저장하기 위한
요청을 수신
504
요청을 검증
506
액세스 데이터를
수신
508
액세스 데이터를
개인화
(선택적)
510
액세스 데이터를
저장
계속

도면6


600
시작
602
저장된 액세스 데이터에
액세스하기 위한
요청을 수신
604
요청을 검증
606
액세스 데이터가
이용가능한가?
아니오
612
요청 디바이스에
메시지를 송신
계속
예
608
액세스 데이터를
제공
610
상태 표시자를
업데이트
계속

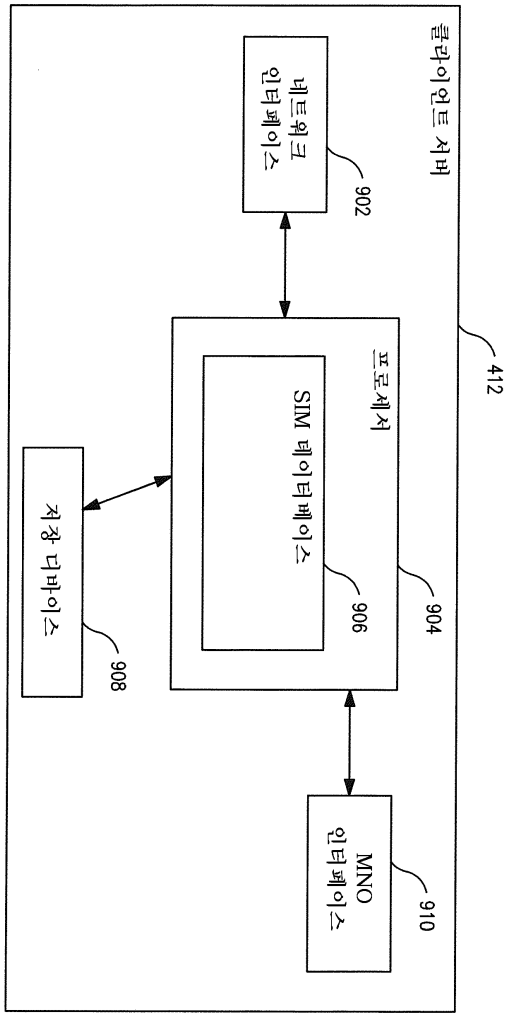
도면7


700
시작
702
액세스 데이터
복귀 명령
수신
704
상태 표시자를
업데이트
706
디바이스로부터 액세스
데이터를 제거
(선택적)
계속

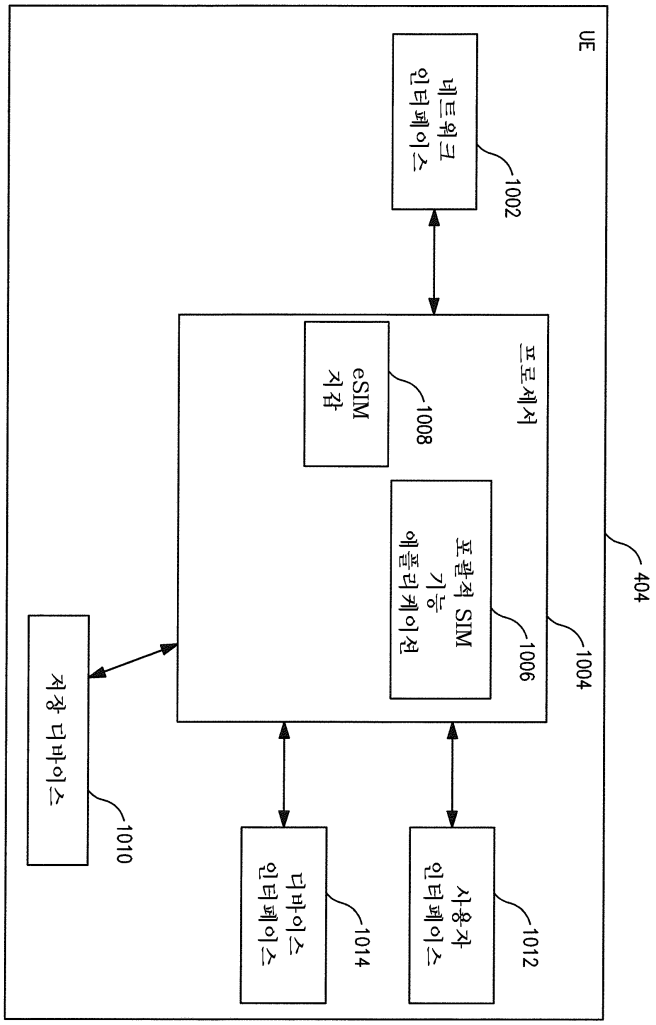
도면8

설명	가입자	상태 표시자	허가된 디바이스(들)
[eSIM 1]	가입자 1	사용중	디바이스 A
[eSIM 2]	가입자 1	유지됨	디바이스 A
[eSIM 3]	가입자 1	유지됨	디바이스 A
[eSIM 4]	가입자 2	사용중	디바이스 B
[eSIM 5]	가입자 2	이용가능하지 않음	디바이스 C
[eSIM 6]	가입자 3	사용중 사용중	디바이스 D 디바이스 E
[eSIM 7]	가입자 3	이용 가능함	디바이스 D

도면9


클라이언트 서버
412
네트워크 인터페이스
902
프로세서
904
SIM 데이터베이스
906
저장 디바이스
908
MNO 인터페이스
910

도면10


UE
네트워크 인터페이스
1002
프로세서
eSIM 지갑
1008
포괄적 SIM 기능 애플리케이션
1006
1004
404
저장 디바이스
1010
디바이스 인터페이스
1014
사용자 인터페이스
1012