(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년01월02일
(11) 등록번호 10-1347527
(24) 등록일자 2013년12월26일

(51) 국제특허분류(Int. Cl.)
H04W 8/20 (2009.01) *H04W 12/08* (2009.01)
G06F 15/16 (2006.01) *H04W 88/02* (2009.01)
(21) 출원번호 10-2011-0111627
(22) 출원일자 2011년10월28일
심사청구일자 2011년10월28일
(65) 공개번호 10-2012-0044916
(43) 공개일자 2012년05월08일
(30) 우선권주장
13/111,801 2011년05월19일 미국(US)
61/407,862 2010년10월28일 미국(US)
(56) 선행기술조사문헌
US20090205028 A1*
KR1020080021178 A
*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
마티아스, 아룬 지.
미국 95014 캘리포니아주 쿠퍼티노 엠에스 302-1엔에스 인피니트 루프 1
(뒷면에 계속)
(74) 대리인
백만기, 권강, 정해양, 양영준

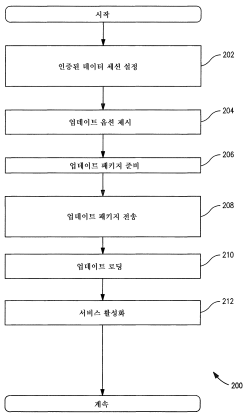
전체 청구항 수 : 총 20 항 심사관 : 복상문

(54) 발명의 명칭 **무선 네트워크를 통해 전자 식별 컴포넌트들을 전달하기 위한 방법 및 장치**

(57) 요 약

본 발명은 무선 장치의 전자 식별 정보의 프로그래밍을 인에이블하는 방법 및 장치에 관한 것이다. 일 실시예에서, 이전에 구입되었거나 사용되었던 무선 장치가 셀룰러 네트워크에 의해 활성화된다. 무선 장치는 액세스 모듈을 이용하여 셀룰러 네트워크에 접속하여 운영 체제 컴포넌트들 및/또는 액세스 제어 클라이언트 컴포넌트들을 다운로드한다. 본 발명의 방법 및 장치는 eSIM(Electronic Subscriber Identity Module) 데이터를 포함하는 다양한 컴포넌트들, 즉 OS 컴포넌트들의 업데이트, 추가 및 대체를 가능하게 한다. 본 발명의 예시적인 일 구현예에서는 디바이스와 셀룰러 네트워크 간의 신뢰된 키 교환을 이용하여 보안을 유지한다.

대 표 도 - 도2



(72) 발명자

본 호크, 제롤드

미국 95014 캘리포니아주 쿠퍼티노 엠에스 111-에이치오엠 인피니트 루프 1

해거티, 데이비드 티.

미국 95014 캘리포니아주 쿠퍼티노 엠에스 87-2씨지에스 인피니트 루프 1

맥라린, 케빈

미국 95014 캘리포니아주 쿠퍼티노 엠에스 302-1엔에스 인피니트 루프 1

주앙, 벤-행

미국 95014 캘리포니아주 쿠퍼티노 엠에스 302-1아이오에스 인피니트 루프 2

리, 리

미국 95014 캘리포니아주 쿠퍼티노 엠에스 302-1아이오에스 인피니트 루프 2

특허청구의 범위

청구항 1

네트워크를 통해 액세스 제어 클라이언트를 수신하는 방법으로서,

제1 세트의 액세스 권한을 갖는 인증된 데이터 세션을 설정하는 단계 - 상기 제1 세트의 액세스 권한은 액세스 제어 클라이언트를 포함하는 하나 이상의 패키지에의 액세스를 가능하게 함 -;

상기 액세스 제어 클라이언트를 포함하는 상기 하나 이상의 패키지를 모바일 디바이스의 보안 요소 내에 다운로드하는 단계 - 상기 액세스 제어 클라이언트는 상기 모바일 디바이스가 상기 액세스 제어 클라이언트와 연관된 네트워크에 인증하는(authenticate) 것을 허용하도록 구성되는 제2 세트의 액세스 권한을 가짐 -;

상기 다운로드된 하나 이상의 패키지에 적어도 부분적으로 기초하여 상기 액세스 제어 클라이언트를 어셈블링하는 단계; 및

상기 어셈블링된 액세스 제어 클라이언트를 이용하여 상기 제2 세트의 액세스 권한의 적어도 일부에 따라 상기 네트워크와 가입자 세션을 설정하는 단계

를 수행하도록 구성되는 적어도 하나의 프로세서를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 인증된 데이터 세션은 상기 네트워크와 수신자 디바이스 간의 상호 검증을 포함하는 방법.

청구항 3

제2항에 있어서,

상기 상호 검증은 암호 키 프로토콜을 포함하는 방법.

청구항 4

제3항에 있어서,

상기 암호 키 프로토콜은 하나 이상의 비대칭 RSA(Rivest Shamir and Adelman) 공용 및 개인 키들에 기초하는 방법.

청구항 5

제1항에 있어서,

상기 제2 세트의 액세스 권한은 하나 이상의 고객 서비스를 가능하게 하는 방법.

청구항 6

제5항에 있어서,

상기 네트워크는 무선 네트워크를 포함하고, 상기 하나 이상의 고객 서비스는 음성 호출을 발신 또는 수신하는 것을 포함하는 방법.

청구항 7

제5항에 있어서,

상기 하나 이상의 고객 서비스는 상기 네트워크에 액세스하는 것을 포함하는 방법.

청구항 8

제5항에 있어서,

상기 하나 이상의 고객 서비스는 미디어 파일에 액세스하는 것을 포함하는 방법.

청구항 9

제5항에 있어서,

상기 제1 세트의 액세스 권한은 고객 서비스에 대해 이용가능하게 되어 있지 않은 방법.

청구항 10

네트워크를 통해 디바이스 운영 체제를 변경하는 방법으로서,

모바일 디바이스가 하나 이상의 업데이트 요청을 수행하기 위해서 네트워크에 액세스하는 것을 허용하도록만 구성되는 제1 세트의 액세스 권한을 갖는 인증된 데이터 세션을 설정하는 단계;

상기 인증된 데이터 세션을 통해 업데이트 요청을 수신하고, 그에 응답하여 제1 키로 암호화된 적절한 업데이트 패키지를 생성하는 단계; 및

상기 인증된 데이터 세션을 통해 하나 이상의 업데이트 패키지 및 상기 모바일 디바이스의 보안 요소에 특정된 제2 키로 암호화된 상기 제1 키를 송신하는 단계

를 수행하도록 구성되는 적어도 하나의 프로세서를 포함하고,

상기 하나 이상의 업데이트 패키지는 액세스 제어 클라이언트와 동작하도록 구성되고, 상기 액세스 제어 클라이언트는 제2 세트의 액세스 권한을 갖는 방법.

청구항 11

제10항에 있어서,

상기 네트워크는 무선 네트워크를 포함하고, 상기 인증된 데이터 세션은 상기 무선 네트워크와 상기 디바이스 간의 상호 검증을 포함하는 방법.

청구항 12

제10항에 있어서,

상기 제1 세트의 액세스 권한은 실질적으로 업데이트 패키지들을 교환하는 것에 제한되어 있는 방법.

청구항 13

제10항에 있어서,

상기 제2 세트의 액세스 권한은 하나 이상의 가입자 세션을 인에이블하는 방법.

청구항 14

제10항에 있어서,

상기 제1 세트의 액세스 권한은 상기 제2 세트의 액세스 권한의 서브세트인 방법.

청구항 15

제10항에 있어서,

상기 제2 세트의 액세스 권한은 하나 이상의 사용자 선택에 기초하여 선택되는 방법.

청구항 16

제15항에 있어서,

상기 업데이트 요청은 상기 하나 이상의 사용자 선택을 포함하는 방법.

청구항 17

제10항에 있어서,

하나 이상의 업데이트 옵션을 상기 디바이스에 제시하는 단계를 더 포함하는 방법.

청구항 18

무선 장치로서,

하나 이상의 무선 네트워크에 접속하도록 구성된 하나 이상의 무선 인터페이스;

복수의 사용자 액세스 데이터 요소를 저장하도록 구성된 보안 요소 - 사용자 액세스 데이터 요소 각각은 상기 무선 장치가 상기 사용자 액세스 데이터 요소와 연관된 대응하는 네트워크와 인증하는 것을 허용하도록 구성됨 -;

프로세서; 및

상기 프로세서와 데이터 통신하는 저장 디바이스

를 포함하며,

상기 저장 디바이스는, 상기 프로세서에 의해 실행될 때,

제2 세트의 액세스 권한을 갖는 액세스 제어 클라이언트에 대한 하나 이상의 업데이트를 수행하기 위해 상기 무선 장치에 네트워크로의 제한된 액세스만을 허용하도록 구성되는 제1 세트의 액세스 권한으로 제한된 인증된 데이터 세션을 설정하고,

상기 인증된 데이터 세션을 통해 액세스 제어 클라이언트에 대한 업데이트를 요청하고,

상기 업데이트된 액세스 제어 클라이언트와 연관된 네트워크와 가입자 세션을 설정

하도록 구성된 컴퓨터 실행가능 명령어들을 포함하며,

상기 제2 세트의 액세스 권한은 상기 무선 장치가 상기 가입자 세션을 통하여 상기 네트워크와 음성 및/또는 데이터 서비스를 수행하는 것을 허용하도록 구성되는, 무선 장치.

청구항 19

제18항에 있어서,

상기 무선 장치는 이동 디바이스를 포함하며, 상기 액세스 제어 클라이언트는 eSIM(electronic Subscriber Identity Module)을 포함하는 무선 장치.

청구항 20

네트워크 장치로서,

하나 이상의 무선 디바이스와 통신하도록 구성된 인터페이스;

프로세서; 및

상기 프로세서와 데이터 통신하는 저장 디바이스

를 포함하며,

상기 저장 디바이스는, 상기 프로세서에 의해 실행될 때,

상기 하나 이상의 무선 디바이스 중 하나의 무선 디바이스와 인증된 데이터 세션을 설정하고 - 상기 인증된 데이터 세션은 제1 세트의 액세스 권한을 가지고, 상기 제1 세트의 액세스 권한은 네트워크 내에서 상기 하나 이상의 무선 디바이스 중 하나의 무선 디바이스의 동작을 제한함 -,

상기 하나의 무선 디바이스로부터 업데이트 요청을 수신하여 적절한 업데이트 패키지를 생성하고,

상기 생성된 업데이트 패키지를 송신

하도록 구성된 컴퓨터 실행가능 명령어들을 포함하고,

상기 생성된 업데이트 패키지는 액세스 제어 클라이언트를 제2 세트의 액세스 권한으로 인에이블하도록 구성되

고, 상기 제2 세트의 액세스 권한은 상기 하나 이상의 무선 디바이스 중 하나의 무선 디바이스가 가입자 세션을 시작하기 위하여 상기 액세스 제어 클라이언트와 연관된 네트워크에 인증하는 것을 허용하도록 구성되는, 네트워크 장치.

명 세 서

기 술 분 야

[0001] <우선권 및 관련 출원>

[0002] 본 출원은, 2010년 10월 28일자로 출원되고 발명의 명칭이 "METHODS AND APPARATUS FOR DELIVERING ELECTRONIC IDENTIFICATION COMPONENTS OVER A WIRELESS NETWORK"인 미국 가특허출원 제61/407,862호의 우선권을 주장하는, 2011년 5월 19일자로 출원되고 발명의 명칭이 "METHODS AND APPARATUS FOR DELIVERING ELECTRONIC IDENTIFICATION COMPONENTS OVER A WIRELESS NETWORK"인 미국 특허 출원 제13/111,801호의 우선권을 주장하며, 이들 각각은 그 전체가 참조로서 여기에 포함된다.

[0003] 본 출원은 또한, 공동 소유되고 공동 계류중인 출원들로서, 2009년 1월 13일자로 출원되고 발명의 명칭이 "POSTPONED CARRIER CONFIGURATION"인 미국 특허출원 제12/353,227호, 2010년 11월 22일자로 출원되고 발명의 명칭이 "WIRELESS NETWORK AUTHENTICATION APPARATUS AND METHODS"인 미국 특허출원 제12/952,082, 2010년 11월 22일자로 출원되고 발명의 명칭이 "APPARATUS AND METHOD FOR PROVISIONING SUBSCRIBER IDENTITY DATA IN A WIRELESS NETWORK"인 미국 특허출원 제12/952,089호, 2010년 12월28일자로 출원되고 발명의 명칭이 "VIRTUAL SUNSCRIBER IDENTITY MODULE DISTRIBUTION SYSTEM"인 미국 특허출원 제12/980,232호, 2011년 4월 1일자로 출원되고 발명의 명칭이 "ACCESS DATA PROVISIONING SERVICE"인 미국 특허출원 제13/078,811호, 2011년 4월 4일자로 출원되고 발명의 명칭이 "MANAGEMENT SYSTEMS FOR MULTIPLE ACCESS CONTROL ENTITIES"인 미국 특허출원 13/079,619호, 2011년 4월 5일자로 출원되고 발명의 명칭이 "METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS"인 미국 특허출원 제13/080,521호, 2011년 4월 5일자로 출원되고 발명의 명칭이 "SIMULACRUM OF PHYSICAL SECURITY DEVICE AND METHODS"인 미국 특허출원 제13/080,533호, 2011년 4월 5일자로 출원되고 발명의 명칭이 "APPARATUS AND METHODS FOR CONTROLLING DISTRIBUTION OF ELECTRONIC SUBSCRIBER IDENTITY MODULES"인 미국 특허출원 제13/080,558호, 2011년 4월 25일자로 출원되고 발명의 명칭이 "APPARATUS AND METHODS FOR STORING ELECTRONIC SUBSCRIBER IDENTITY MODULES"인 미국 특허출원 제13/093,722호, 2011년 4월 27일자로 출원되고 발명의 명칭이 "SYSTEM FOR DISTRIBUTION OF UNIQUE SUBSCRIBER IDENTITY MODULES"인 미국 특허출원 제13/095,716호; 및 2010년 10월 28일자로 출원되고 발명의 명칭이 "METHODS AND APPARATUS FOR ACCESS CONTROL CLIENT ASSISTED ROAMING"인 미국 가특허출원 제61/407,858호, 2010년 11월 3일자로 출원되고 발명의 명칭이 "METHODS AND APPARATUS FOR ACCESS DATA RECOVERY FROM A MALFUNCTIONING DEVICE"인 미국 가특허출원 제61/409,891호, 2010년 11월 12일자로 출원되고 발명의 명칭이 "APPARATUS AND METHODS FOR RECORDATION OF DEVICE HISTORY ACROSS MULTIPLE SOFTWARE EMULATION"인 미국 가특허출원 제61/413,317호, 2011년 4월 26일자로 출원되고 발명의 명칭이 "ELECTRONIC ACCESS CLIENT DISTRIBUTION APPARATUS AND METHODS"인 미국 가특허출원 제61/479,319호, 2011년 4월 29일자로 출원되고 발명의 명칭이 "COMPACT FORM FACTOR INTEGRATED CIRCUIT CARD"인 미국 가특허출원 제61/481,114호, 2011년 5월 6일자로 출원된 발명의 명칭이 "METHODS AND APPARATUS FOR PROVIDING MANAGEMENT CAPABILITIES FOR ACCESS CONTROL CLIENTS"인 미국 가특허출원 제61/483,582호와 관련되며, 이들 출원은 그 전체가 참조로서 여기에 포함된다.

[0004] <발명의 분야>

[0005] 본 발명은 일반적으로, 예를 들어 디바이스들이 셀룰러 네트워크를 이용하여 통신하는 시스템과 같은 무선 시스템에 관한 것이다. 특히, 일 예시적인 양태에서, 본 발명은 셀룰러 네트워크를 통해 셀룰러 디바이스에 전자 식별 컴포넌트들을 전달하기 위한 방법 및 장치에 관한 것이다.

배 경 기 술

[0006] <관련 기술의 설명>

[0007] 대부분의 종래 기술의 무선 라디오 통신 시스템에서는 보안 통신을 위해 액세스 제어가 요구된다. 일례로, 한 가지 간단한 액세스 제어 방식은 (i) 통신하는 당사자의 아이덴티티를 검증하는 것, 및 (ii) 검증된 아이덴티티에 상응하는 액세스 레벨을 부여하는 것을 포함할 수 있다. 예시적인 셀룰러 시스템의 문맥 내에서, 액세스 제

어는 물리적인 카드 폼 팩터 UICC(Universal Integrated Circuit Card) 내에 물리적으로 내장되는 SIM(Subscriber Identity Module)이라고 지칭되는 액세스 제어 클라이언트에 의해 관리된다. 동작 동안, SIM 카드는 셀룰러 네트워크의 가입자를 인증한다. 성공적인 인증 후에, 가입자는 셀룰러 네트워크로의 액세스가 허용된다.

[0008] 각각의 SIM 카드는 단일의 사용자 계정과 관련되며, 사용자 계정 데이터는 SIM 카드 상에 영구적으로 저장된다. 사용자가 기존의 계정에서 새로운 계정으로 서비스를 변경하기를 원한다면, 사용자는 (예를 들어, SIM 카드 슬롯에서 기존의 SIM 카드를 물리적으로 제거하고 새로운 SIM 카드를 삽입함으로써) 기존의 SIM 카드를 새로운 SIM 카드로 교체해야 한다. 요컨대, 사용자 계정은 SIM 카드와 연계되는 것이며 이동 디바이스 자체와 연계되는 것이 아니다. 결과적으로, 추가의 계정을 추가하는 것은 새로운 SIM 카드를 이용하는 것을 필요로 한다. 예를 들어, 가입자가 새로운 서비스 지역으로 여행할 때, 가입자는 종종, 고가의 로밍 요금을 지불하는 것 또는 새로운 SIM 카드를 구매하는 것 사이에서 선택해야만 한다. 마찬가지로, (예를 들어, 업무와 개인 용도를 위한 전화를 공유하는 것과 같은) 청구 계좌들 사이에서 변경을 행하는 사용자에게 있어서, 사용자는 SIM 카드들 사이에서 지속적으로 교환하여야만 한다. 몇몇 디바이스들은 복수의 카드 리셉터클(receptacle)을 제공하여 복수의 SIM 카드들이 이용가능하게 함으로써 이러한 문제를 해결하려고 시도하였다. 그러나, 이들 "복수-카드" 해결책은 추가의 SIM 카드 리셉터클들이 상당한 공간을 차지하기 때문에 바람직하지 않으며, SIM 카드 계정들의 근원 불가변성을 해결하지 못한다.

[0009] 또한, 기존의 SIM 해결책은 물리적인 UICC 카드 매체에 "하드코딩된" 하나 이상의 SIM 소프트웨어 아이덴티티를 포함한다, 즉, 예를 들어, SIM 카드 어셈블리는 재프로그래밍될 수 없다. 모든 실용적인 의도 및 목적을 위해, 종래 기술의 SIM 카드는 분할 불가능하다, 즉, SIM 소프트웨어는 물리적인 UICC 카드 매체로부터 분리될 수 없다. 따라서, 특정 동작들은 기존의 SIM 카드 프레임워크 내에서 수행될 수 없다. 예를 들어, SIM은 SIM 카드들 사이에서 이동될 수 없고, 수정, 폐지될 수 없고, 및/또는 서로 다른 네트워크 제공업자들에 대해 이용가능해질 수 없다. 따라서, 이하에서 보다 상세히 설명되는 바와 같이, 기존의 SIM 카드 해결책들은 셀룰러 기술들(및 다른 무선 기술들)의 복잡성을 진화시키기에는 점점 불충분해지고 있다.

[0010] 따라서, 사용자 계정들을 획득(예를 들어, 구매)하고 관리하는 능력을 사용자에게 제공하기 위한 개선된 해결책이 필요하다. 이러한 개선된 해결책은 이상적으로, 새로운 SIM 카드를 필요로 하지 않고 이전에 배치되거나 구매된 디바이스들에 새로운 또는 상이한 사용자 계정을 전달하는 것을 지원해야 한다.

발명의 내용

[0011] 본 발명은 그 중에서도, 액세스 제어 클라이언트들의 안전한 구입 및 전달을 위한 개선된 장치 및 방법을 제공함으로써 전술한 요구들을 만족시킨다.

[0012] 본 발명의 제1 양태에서, 무선 네트워크를 통해 액세스 제어 클라이언트를 수신하는 방법이 개시된다. 일 실시예에서, 본 방법은, 인가된 데이터 세션을 설정하는 단계 - 인가된 데이터 세션은 제1 액세스 권한 집합을 가짐 -; 액세스 제어 클라이언트를 선택하는 단계 - 액세스 제어 클라이언트는 제2 액세스 권한 집합을 가짐 -; 하나 이상의 업데이트 패키지를 수신하는 단계; 하나 이상의 업데이트 패키지를 액세스 제어 클라이언트 내에 어셈블링하는 단계; 및 액세스 제어 클라이언트를 실행하는 단계를 포함한다.

[0013] 본 발명의 제2 양태에서, 무선 네트워크를 통해 다바이스 운영 체제를 수정하는 방법이 개시된다. 일 실시예에서, 본 방법은 인가된 데이터 세션을 설정하는 단계 - 인가된 데이터 세션은 제1 액세스 권한 집합을 가짐 -; 하나 이상의 업데이트 패키지를 수신하는 단계; 하나 이상의 업데이트 패키지를 운영 체제 컴포넌트 내에 어셈블링하는 단계를 포함하고, 운영 체제 컴포넌트는 제2 액세스 권한 집합을 갖는 액세스 제어 클라이언트와의 동작을 위해 구성된다.

[0014] 본 발명의 제3 양태에서, 네트워크를 통해 액세스 제어 클라이언트를 수신하는 방법이 개시된다. 일 실시예에서, 본 방법은 인가된 데이터 세션을 설정하는 단계 - 인가된 데이터 세션은 액세스 제어 클라이언트와 관련된 하나 이상의 패키지로의 액세스를 가능하게 하는 액세스 제1 액세스 권한 집합을 가짐 -; 액세스 제어 클라이언트와 관련된 하나 이상의 패키지를 다운로드하는 단계 - 상기 액세스 제어 클라이언트는 제2 액세스 권한 집합을 가짐 -; 다운로드된 하나 이상의 패키지에 적어도 부분적으로 기초하여 액세스 제어 클라이언트를 어셈블링하는 단계; 및 어셈블링된 액세스 제어 클라이언트를 가지고 가입자 세션을 설정하는 단계를 포함한다.

[0015] 일 변형예에서, 인가된 데이터 세션은 무선 네트워크와 수신자 디바이스 간의 상호 간의 검증을 포함한다. 예를 들어, 상호 간의 검증은 암호 키 프로토콜을 포함할 수 있다. 그러한 일례에서, 암호 키 프로토콜은 하나

이상의 비대칭 RSA(Rivest Shamir and Adelman) 공용 키 및 개인 키에 기초한다.

[0016] 다른 변형예에서, 제2 액세스 권한 집합은 예를 들어, 음성 호출을 걸거나 받는 것, 네트워크에 액세스하는 것, 미디어 파일에 액세스하는 것과 같은 하나 이상의 소비자 서비스를 가능하게 한다. 다르게, 제1 액세스 권한 집합은 소비자 서비스가 이용불가능하다.

[0017] 본 발명의 제4 양태에서, 네트워크를 통한 디바이스 운영 체제를 수정하는 방법이 개시된다. 일 실시예에서, 본 방법은 제1 액세스 권한 집합을 갖는 인가된 데이터 세션을 설정하는 단계; 인가된 데이터 세션을 통해 업데이트 요구를 수신하는 단계; 응답적으로 적절한 업데이트 패키지를 생성하는 단계; 및 인가된 데이터 세션을 통해 하나 이상의 업데이트 패키지를 전송하는 단계를 포함한다. 하나 이상의 업데이트 패키지는 액세스 제어 클라이언트와의 동작을 위해 구성되며, 액세스 제어 클라이언트는 제2 액세스 권한 집합을 갖는다.

[0018] 일 변형예에서, 네트워크는 무선 네트워크이고, 인가된 데이터 세션은 무선 네트워크와 디바이스 간의 상호 간의 검증을 포함한다.

[0019] 제2 변형예에서, 제1 액세스 권한 집합은 실질적으로 업데이트 패키지들을 교환하는 것으로 제한된다. 다르게, 다른 변형예에서, 제2 액세스 권한 집합은 하나 이상의 가입자 세션을 가능하게 한다. 다른 대안으로서, 제1 액세스 권한 집합은 제2 액세스 권한 집합의 부분집합이다. 또 다른 대안에서, 제2 액세스 권한 집합은 하나 이상의 사용자 선택에 기초하여 선택된다. 또한, 업데이트 요청은 하나 이상의 사용자 선택을 포함할 수 있다. 하나 이상의 업데이트 옵션도 디바이스에 제시될 수 있다.

[0020] 본 발명의 다른 양태에서, 무선 장치가 개시된다. 일 실시예에서, 무선 장치는 하나 이상의 무선 네트워크에 접속하도록 구성된 하나 이상의 무선 인터페이스; 복수의 사용자 액세스 데이터 구성요소를 저장하도록 구성된 보안 구성요소 - 각각의 사용자 액세스 데이터 구성요소는 대응하는 네트워크와 관련됨 -; 프로세서; 및 프로세서와 데이터 통신하는 저장 디바이스 - 저장 디바이스는 컴퓨터-실행가능 명령어들을 포함함 -를 포함한다.

[0021] 일 변형예에서, 컴퓨터-실행가능 명령어들은 프로세서에 의해 실행될 때, 제1 액세스 권한 집합으로 제한된 인가된 데이터 세션을 설정하고; 인가된 데이터 세션을 통해 액세스 제어 클라이언트에 대한 업데이트를 요청하고; 업데이트된 액세스 제어 클라이언트를 가지고 가입자 세션을 설정하도록 구성되며, 가입자 세션은 제2 액세스 권한 집합을 갖는다.

[0022] 제2 변형예에서, 무선 디바이스는 이동 디바이스이고, 액세스 제어 클라이언트는 eSIM(electronic Subscriber Identity Module)이다.

[0023] 본 발명의 또 다른 양태에서, 네트워크 장치가 개시된다. 일 실시예에서, 네트워크 장치는 하나 이상의 무선 디바이스와 통신하도록 구성된 하나 이상의 인터페이스; 프로세서; 및 프로세서와 데이터 통신하는 저장 디바이스를 포함하고, 저장 디바이스는 컴퓨터-실행가능 명령어들을 포함한다. 일 변형예에서, 컴퓨터-실행가능 명령어들은 프로세서에 의해 실행될 때, 하나 이상의 무선 디바이스 중 하나의 무선 디바이스와의 인가된 데이터 세션을 설정하고 - 인가된 데이터 세션은 제1 액세스 권한 집합을 가짐 -; 그 하나의 무선 디바이스로부터 업데이트 요청을 수신하고 응답적으로 적절한 업데이트 패키지를 생성하고; 생성된 업데이트 패키지를 전송하도록 구성된다. 생성된 업데이트 패키지는 액세스 제어 클라이언트와의 동작을 위해 구성되며, 액세스 제어 클라이언트는 제2 액세스 권한 집합을 갖는다.

[0024] 본 발명의 또 다른 양태에서, 컴퓨터 판독가능 장치가 개시된다. 일 실시예에서, 장치는 적어도 하나의 컴퓨터 프로그램을 저장하도록 구성된 저장 매체를 포함한다. 일 변형예에서, 프로그램은 실행될 때, 제1 액세스 권한 집합을 갖는 인가된 데이터 세션을 설정하고; 하나 이상의 업데이트 패키지를 수신하고; 하나 이상의 업데이트 패키지를 운영 체제 컴포넌트 내에 어셈블링하는 명령어들을 포함한다.

[0025] 본 발명의 다른 특징들 및 장점들은, 본 기술분야에 통상의 지식을 가진 자가 이하에 제공되는 예시적인 실시예들의 상세한 설명 및 첨부 도면을 참조하면 쉽게 인지될 것이다.

도면의 간단한 설명

[0026] 도 1은 SIM을 이용하는 종래 기술의 AKA(Authentication and Key Agreement) 프로시저를 도시하는 논리 래더도.

도 2는 본 발명의 다양한 양태에 따라 이동 디바이스 eSIM을 프로그래밍하기 위한 일 예시적인 실시예를 세부화한 논리 흐름도.

도 3은 본 발명의 다양한 양태에 따라 이동 디바이스 운영 체제를 프로그래밍하기 위한 일 예시적인 실시예를 세부화한 논리 흐름도.

도 4는 본 발명에 따라 이동 디바이스의 컴포넌트들을 프로그래밍하기 위한 일반화된 방법의 일 실시예를 도시하는 논리 흐름도.

도 5는 본 발명의 방법을 구현하는 데에 유용한 예시적인 장치의 블럭도.

발명을 실시하기 위한 구체적인 내용

[0027] 도면에 대한 참조가 이루어지며, 도면 전반에 걸쳐 유사 참조번호는 유사 부분들을 지칭한다.

[0028] 개요

[0029] 일 양태에서, 본 발명은 네트워크를 통해 액세스 제어 클라이언트를 디바이스에 전달하기 위한 방법 및 장치를 제공한다. 일 예시적인 실시예에서, 셀룰러 네트워크는 셀룰러 디바이스가 배치된 후에 eSIM을 셀룰러 디바이스에 안전하게 전달할 수 있다. 특히, 셀룰러 디바이스는 네트워크로의 접속을 위한 제한된 능력으로 프리-프로그래밍된다. 셀룰러 디바이스는 업데이트 포털에 접속하기 위한 몇몇 제한된 액세스 능력을 갖지만, 음성 호출을 하고 사용자 데이터를 수신 및 전송하는 등을 행하기 위한 기능을 충분히 갖춘 eSIM을 수신해야 한다. 예를 들어, 사용자는 간단한 액세스 모듈을 가진 이동 디바이스(예를 들어, 셀룰러 폰)를 구매한다. 액세스 모듈은 셀룰러 네트워크에 접속하고 디바이스를 인증하고 사용자로 하여금 충분한 기능을 가진 eSIM을 구매 또는 검색할 수 있게 하도록 구성된다. 셀룰러 네트워크는 부트스트랩 OS에 의해 어셈블링되고 활성화되는 eSIM을 안전하게 전달한다.

[0030] 여기에서 더 상세히 설명되는 바와 같이, 본 발명의 일 예시적인 실시예는 (예를 들어, 운영 체제 및 액세스 제어 클라이언트 컴포넌트들을 포함하는) 액세스 제어 클라이언트와 관련된 컴포넌트들의 전달을 용이하게 할 수 있는 액세스 모듈 시스템을 개시한다. 올바르게 부호화되고/되거나 암호화된 적절히 전달된 패키지를 수신한 후에, 운영 체제는 컴포넌트들을 어셈블링 및 로드할 수 있다. 본 발명의 다양한 실시예에서, 운영 체제, 액세스 제어 클라이언트, 사용자 계정 데이터 등을 전달하는 데에 패키지들이 이용될 수 있다.

[0031] 일 양태에서, 본 발명은 또한, 무선 디바이스의 전체 라이프 사이클을 관리하기 위한 소프트웨어 기반 업데이트들을 고려한다. 따라서, 제시된 방법론에 할당된 유연성은, 심지어 액세스 모듈 및/또는 운영 체제 컴포넌트들을 포함하는 무선 디바이스의 임의의 소프트웨어 구성요소의 대체 능력을 포함한다. 예를 들어, 셀룰러 디바이스는 완전히 새로운 운영 체제를 수신하여 그것의 인증 알고리즘을 업데이트할 수 있다.

[0032] 개시된 발명에 대한 다른 다양하고 유용한 응용들은 보안 능력, 업데이팅 변경 제어, 새로운 기능 및 서비스의 사후-배치 프로비저닝을 진화시키는 것을 포함한다.

[0033] 예시적인 실시예의 상세한 설명

[0034] 본 발명의 예시적인 실시예들 및 양태들이 이제 상세히 설명된다. 이들 실시예 및 양태는 주로 GSM, GPRS/EDGE 또는 UMTS 셀룰러 네트워크의 SIM(Subscriber Identity Module)의 문맥에서 논의되지만, 통상의 기술을 가진 자라면 본 발명이 그렇게 제한되는 것은 아니라는 점을 인지할 것이다. 사실, 본 발명의 다양한 양태들은 액세스 제어 엔티티들 또는 클라이언트들의 안전한 수정, 저장 및 실행으로부터 이익을 얻을 수 있는 (셀룰러든지 아니면 다른 것이든지) 임의의 무선 네트워크에서 유용하다.

[0035] 또한, 여기에서 "SIM(Subscriber Identity Module)이라는 용어가 사용되지만(예를 들어, eSIM), 이 용어가 반드시 (i) 그 자체로 가입자에 의한 사용(즉, 본 발명은 가입자 또는 비가입자에 의해 실시될 수 있음); (ii) 단일의 개인의 아이덴티티(즉, 본 발명은 가족과 같은 개인들의 그룹, 또는 기업과 같은 무형 또는 허구의 엔티티를 대신하여 실시될 수 있음); 또는 (iii) 임의의 유형의(tangible) "모듈" 장비 또는 하드웨어를 함축하거나 요구하는 것은 아니다.

[0036] **종래 기술의 SIM 동작**

[0037] 종래 기술의 UMTS 셀룰러 네트워크 문맥에서, 사용자 장비(UE)는 이동 디바이스 및 USIM을 포함한다. USIM은 물리적인 UICC(Universal Integrated Circuit Card)로부터 저장 및 실행되는 논리적 소프트웨어 엔티티이다. 가입자 정보와 같은 다양한 정보가 USIM에 저장될 뿐만 아니라, 무선 네트워크 서비스를 획득하기 위해 네트워

크 운영자와의 인증을 위한 키 및 알고리즘이 사용된다.

[0038] 일반적으로, UICC들은 가입자 배포 전에 USIM을 이용하여 프로그래밍되고, 프리 프로그래밍 또는 "개인 설정(personalization)"은 각각의 네트워크 오퍼레이터에 특정된다. 예를 들어, 배포 전에, USIM은 IMSI(International Mobile Subscriber Identify), 고유한 ICC-ID(Integrated Circuit Card Identifier) 및 특정한 인증키(K)와 연관된다. 네트워크 오퍼레이터는 네트워크의 AuC(Authentication Center) 내에 포함된 레지스트리에 그 연관을 저장한다. 개인 설정 후에, UICC는 가입자들에게 배포될 수 있다.

[0039] 이제부터 도 1을 참조하여, 전술한 종래 기술의 USIM을 이용한 하나의 예시적인 AKA(Authentication and Key Agreement) 프로시저(100)를 상세히 설명하도록 한다. 표준 인증 프로시저들 동안에, UE(102)는 USIM(104)으로부터 IMSI(International Mobile Subscriber Identifier)를 획득한다. UE는 이를 네트워크 오퍼레이터의 SN(Serving Network; 106) 또는 방문한 코어 네트워크에 전달한다. SN은 HN(Home Network)의 AuC(108)에게 인증 요청을 포워딩한다. HN은 수신된 IMSI를 AuC의 레지스트리와 비교하고 적절한 K를 획득한다. HN은 RAND(random number)를 생성하고, 이를 알고리즘을 이용하여 K로 서명하여 XRES(expected response)를 생성한다. HN은 다양한 알고리즘들을 이용하여 암호화 및 무결성 보호(integrity protection)에서 사용하기 위한 CK(Cipher Key) 및 IK(Integrity Key)뿐만 아니라 AUTN(Authentication Token)를 더 생성한다. HN은 RAND, XRES, CK 및 AUTN으로 이루어진 인증 벡터를 SN으로 전송한다. SN은 인증 벡터를 일 회의 인증 프로세스에서만 사용하도록 저장한다. SN은 RAND 및 AUTN을 UE로 전달한다.

[0040] UE(102)가 RAND 및 AUTN을 수신하고 나면, USIM(104)은 수신된 AUTN이 유효한지 검증한다. 만약 유효하다면, UE는 수신된 RAND를 사용하여, 저장된 K 및 XRES를 생성한 동일한 알고리즘을 이용하여 그 자신의 응답(RES)을 계산한다. UE는 RES를 SN에게 다시 전달한다. SN(106)은 XRES를 수신된 RES와 비교하고, 만약 이들이 매치되면, SN은 UE가 오퍼레이터의 무선 네트워크 서비스들을 사용하는 것을 인증한다.

[0041] **예시적인 동작 -**

[0042] 본 발명의 예시적인 실시예의 컨텍스트에서는, 종래의 기술에서와 같이 물리적인 UICC를 사용하는 대신에, UICC는 UE의 보안 요소(예를 들어, 보안 마이크로프로세서 또는 저장 디바이스) 내에 포함되는, 예를 들어, 소프트웨어 애플리케이션과 같은 가상 또는 전자 엔터티(이하에서는, eUICC(Electronic Universal Integrated Circuit Card)로서 참조됨)로서 에뮬레이트된다. eUICC는 이하에서 eSIM(Electronic Subscriber Identity Modules)으로서 참조되는 복수의 USIM을 저장하고 관리할 수 있다. 각각의 eSIM은 통상적인 USIM과 동일한 데이터를 포함한다. eUICC는 eSIM의 ICC-ID에 기초하여 eSIM을 선택한다. eUICC가 원하는 eSIM(들)을 선택하고 나면, UE는 인증 프로시저를 시작하여 eSIM의 대응하는 네트워크 오퍼레이터로부터 무선 네트워크 서비스들을 획득할 수 있다.

[0043] 도 2는 본 발명에 따른 eSIM 데이터를 보안 전송하는 하나의 예시적인 실시예(200)의 프로세스도이다. 사용자는 로컬 캐리어에 대해 인증된 소매 엔터티(authorized retail entity)로부터 무선 디바이스를 구매하고, 무선 디아비스의 eUICC는 액세스 모듈에 의해 프리 로딩(pre-load)된다. 예를 들어, 신뢰된 통신들을 구축하기 위한 예시적인 장치들 및 방법들을 개시하고 본 명세서에서 이전에 참조로 포함된, 공유되고 동시 계류 중인 미국 특허 출원 번호 제13/080,521호(2011년 4월 5일에 출원되고, 발명의 명칭이 "METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS"임)를 참조한다.

[0044] 액세스 모듈의 제한된 기능은 로컬 캐리어 네트워크의 미리 정의된 데이터 포털과의 데이터 접속들을 구축하고, 업데이트 포털로부터 소프트웨어 패키지들을 다운로드하고, 수신된 패키지들을 어셈블한다. 이들 패키지들은 운영 체제 컴포넌트들, 액세스 제어 클라이언트들, 사용자 계정 데이터 등을 전체적으로 또는 부분적으로 포함할 수 있다. 이하의 예에서, 사용자는 새로운 eSIM을 자신의 디바이스에 전자적으로 다운로드하여, 임의의 물리적인 컴포넌트 소유 요청들을 제거한다. eSIM이 사용자를 인증하고 난 후, 네트워크는 사용자에의 액세스를 허용하며, 네트워크 액세스는 휴대전화 호출들을 발신하고/수신하는 것, 인터넷을 브라우징하는 것, 네트워크를 통해 오디오 가상 컨텐츠에 액세스하는 것과 같은 최종 사용자 동작들을 허용한다.

[0045] 방법(200)의 단계(202)에서, 무선 디바이스는 이동 디바이스의 eUICC 보안 요소와 로컬 캐리어 업데이트 포털 간의 인증된 데이터 세션을 구축한다. 세션 인증은 eUICC 모듈 식별 데이터에 기초한다. eUICC 모듈 식별 데이터는 eUICC에 특정한 기존의 키를 참조하지만, 본 명세서가 주어졌을 때 당업자들에 의해 인식되는 다수의 다른 접근 방식들 또한 사용될 수 있다. 여기서 상세히 설명되는 바와 같이, eUICC는 하나의 변형에서 공용키/개인키 및 인증 기관(authenticating authority)(예를 들어, 그 담당자(Assignee))에 의한 인증서에 의해 "버

닝"되거나 하드코딩된 액세스 모듈을 포함한다. 공용키 및 보증 인증서(endorsement certificate)가 로컬 캐리어 업데이트 포털에 제공된다. 로컬 캐리어 업데이트 포털은 보증 인증서를 검증한다(예를 들어, 인증서를 발행한 인증 기관에 의한 검증). 보증 인증서가 유효하면, 로컬 캐리어 업데이트 포털은 벤더 인증서 및 세션키를 이동 디바이스로 전송하며, 여기서 벤더 인증서 및 세션키는 이동 디바이스의 공용키에 의해 더 암호화된다. 이에 응답하여, eUICC는 벤더의 공용키에 의해 벤더 인증서를 암호해독하고, 그 신뢰성을 검증한다. 단, 벤더의 공용 서명키에 의하여 벤더의 인증서를 성공적으로 암호해독하는 것은 서명이 위조되지 않았다는 증거를 eUICC에게 제공하는 것임을 유의하도록 한다. 이동 디바이스는 벤더 인증서 및 세션키를 그 개인키에 의해 암호해독한다. 만약 벤더 인증서가 유효하면, 이동 디바이스는 세션키를 허용한다.

[0046] 상술한 교환이 성공적으로 완료되는 것은 이동 디바이스 및 로컬 캐리어 업데이트 포털이 모두 합법적이고 이제는 공유된 세션키를 가지고 있다는 것을 보장한다. 공유된 세션키는 이동 디바이스와 로컬 캐리어 업데이트 포털 간의 보안 세션을 행하는 데에 사용된다.

[0047] 다시 도 2를 참조하면, 단계(204)에서, 사용자(또는 디바이스 관리 엔터티)에게 하나 이상의 업데이트 옵션이 제시된다. 다양한 옵션들은 예를 들어, 이용가능한 데이터 계획들, 이용가능한 네트워크 캐리어 옵션들 등의 목록을 포함할 수 있다. 단계(206)에서 사용자 선택을 수신하면, 하나 이상의 패키지가 로컬 캐리어 업데이트 포털에 의해 준비된다. 단계(208)에서, 패키지들은 이동 디바이스로 전송되고, 각각의 패키지는 세션키에 의해 암호화된다.

[0048] 하나 이상의 패키지는 예를 들어, eSIM을 포함할 수 있다. 다른 공통 패키지들은 SIM OS 또는 "공통 OS"에 필요한 추가의 피처(feature)들 또는 컴포넌트들을 포함할 수 있다. 특히, 액세스 모듈이 로컬 캐리어 업데이트 포털과 보안 세션을 구축하기에 충분한 동안에는, SIM 동작에 필요한 다른 요소들을 제공하지 않는다. 예를 들어, 공통 OS는 파일 입력 및 출력, 파일 관리, 메모리 할당 등과 같은 서비스들을 제공한다. 공통 OS는 eUICC 소프트웨어와 결합하여 SIM 동작을 지원하기 위하여 종래 기술의 UICC에 의해 통상적으로 구현되는 서비스들을 에뮬레이트한다.

[0049] 단계(210)에서, 보안 전송된 패키지들을 수신한 후, 부트스트랩 OS는 패키지들을 로딩하고 어셈블할 수 있다. 일단 어셈블되고 나면, 부트스트랩 OS는 공통 OS를 실행시키고, 공통 OS는 적절한 eSIM을 로딩하고 실행시킨다. 단, 공통 OS는 패키지를 통해 전달되거나 또는 eUICC 내에 존재할 수 있음을 유의하도록 한다. 게다가, 상이한 eSIM들이 상이한 공통 OS 서비스들을 요청할 수도 있음을 또한 유의하도록 한다. 부트스트랩 OS는 eSIM과 공통 OS가 호환가능함을 보장해야 한다. 호환가능성은 버전 식별자들, 신뢰된 엔터티 인증들 등에 의해 검증될 수 있다. 예를 들어, 부트스트랩 OS는 eSIM이 현존하는 공통 OS와 사용하는 데에 허용될 수 있고 신뢰된 엔터티에 의해 서명되었다는 것을 검증할 수 있다.

[0050] 예들 들어, 디바이스가 사용자에게 필요에 따라 새로운 계정 정보(예를 들어, 사용자 명, 계좌 번호, 비밀 번호 및/또는 PIN)를 프롬프트하는 것에 의해 추가적인 서비스들이 활성화된다(단계 212). 그 후, 업데이트된 이동 디바이스가 풀-피처드(full featured) eSIM을 활성화시켜서 음성 호출들을 하게 하고 사용자 데이터를 수신 및 전송하게 하는 등을 할 수 있다. 다르게는, 휴대전화가 아닌 구현들에서, (예를 들어, WLAN 내에서의) 액세스 포인트 또는 게이트웨이 액세스, 브로드밴드 액세스 등과 같은 기능들이 상기한 방법론을 사용하여 인에이블될 수 있다.

[0051] **수명 주기 관리 -**

[0052] 무선 장치의 전체적인 수명 주기를 관리하기 위한 본 발명의 예시적인 실시예가 설명된다. 제시된 프로그래밍 방법론들은 보안 업데이트들 설치, OS 패치들 설치 및/또는 OS의 하나 이상의 양태의 완전한 대체를 지원한다.

[0053] 한 예시적인 실시예에서, eUICC는 부트스트랩 OS 및 공통 OS를 추가로 포함한다. 간단한 부트스트랩 OS가 공통 OS, 및 그와 연관된 eSIM 및 패치들을 로딩하고 실행시킨다. 운영 체제는 SIM 동작을 지원하는 데에 요구되지만, 사용자 액세스 제어 자체에 직접 관련되지는 않는다. 특히, 공통 OS는 파일 입력 및 출력, 파일 관리, 메모리 할당 등과 같은 범용화된 서비스들을 제공한다. 극단적인 경우들에는, 휴대전화 또는 다른 장치가 완전히 새로운 부트스트랩 OS를 수신하고 어셈블하여 그 인증 알고리즘을 업데이트할 수 있다.

[0054] 도 3은 본 발명의 실시예에 따른 운영 체제를 대체(또는 업데이트)하기 위한 예시적인 프로세스(300)를 도시한다. 부트스트랩 OS 업데이트를 요청하는 공통된 이유들로는 새로이 발견된 보안 구멍들, 인증 알고리즘들에 대한 개선들, 새로운 기능들 등이 있다. 일부 경우들에서는, 시기 적절한 보안 업데이트들을 권장하기 위하여, 캐리어들이 적정한 시간 내에 업데이트되지 않은 이동 장치들을 디스에이블시키도록 택할 수 있다. 또한, 캐리

어는 사용자가 업데이트하는 것을 권장하기 위하여 자동 관리 동작(proactive action)(예를 들어, 빈도가 증가하는 반복되는 리마인더들)을 취하거나, 또는 심지어 통지 시에, 계속된 서비스 액세스에 대해 업데이트가 완료되어야 하도록 장치를 구성할 수도 있다. 또한, 어떤 실시예들에서는, 강제적인 업데이트들(즉, 사용자 동의 없이 수행되는 업데이트들)이 본 발명에 의해 고려된다. 운영 체제를 대체하거나 업데이트하는 다른 이유들로는 예를 들어, 소비자 기반 고려사항들, 예를 들어, 새로운 휴대전화 네트워크 서비스로의 이동, 제품 기능들의 업데이트, 새로운 휴대전화 계약의 구매 등이 있을 수 있다.

[0055] 단계(302)에서, 이동 장치는 eUICC에 특정한 기존의 키를 통해 보안 요소와 캐리어 업데이트 포털 간의 인증된 데이터 세션을 구축한다.

[0056] 또한, 일부 환경들에서, 부트스트랩 OS에 대한 변경들은 예를 들어, 새로운 보안 기능 등을 인에이블시키기 위하여 공통 OS의 대응하는 부분들을 업데이트할 것을 요청할 것이다. 따라서, 예시된 실시예의 단계(304)에서, 이동 장치는 (i) 부트스트랩 OS 부분만을 업데이트하거나, (ii) 공통 OS 부분을 업데이트하거나, 또는 (iii) 부트스트랩 OS 및 공통 OS를 업데이트할 수 있다. 예를 들어, 이동 장치는 그 부트스트랩 OS를 업데이트함으로써 그 지원된 캐리어들의 리스트를 업데이트할 수 있다. 마찬가지로, 이동 장치는 공통 OS 업데이트에 의해 보다 큰 eSIM 파일 구조들을 지원하기 위하여 그 내부 파일 구조를 업데이트할 수 있다. 또한, 이동 장치는 파일 구조에 대한 변경들을 더 포함하는 새로운 캐리어를 지원하기 위하여 재프로그래밍될 수 있다(부트스트랩 OS 및 공통 OS 모두가 업데이트됨).

[0057] 부트스트랩 OS가 업데이트되면, 로컬 캐리어 업데이트 포털이 이동 장치의 부트스트랩 OS 프로파일 구성을 저장한다(단계 306). 부트스트랩 OS 프로파일은 네트워크 인증 구성, eSIM 관리 등을 포함하지만, 이에 제한되지 않는다. 이 저장된 OS 프로파일은 나중에 공통 OS 업데이트 패키지를 구성하는 데에 사용될 수 있다(공통 OS 업데이트는 이동 장치의 구성에 특정될 수 있다). 단계(308)에서, 부트스트랩 OS를 포함하는 업데이트 패키지는 후속하여 이동 장치로 다운로드되고 새로운 부트스트랩 OS로 어셈블된다. 단계(310)에서, eUICC의 현존하는 부트스트랩 OS가 새로운 부트스트랩 OS에 의해 대체된다.

[0058] 부트스트랩 OS가 현존하는 공통 OS에 대응하는 어떠한 변경들도 요청하지 않으면, 장치는 새로운 부트스트랩 OS에 의해 동작할 준비를 한다. 한편, 부트스트랩 OS 업데이트가 또한 풀-피처드 공통 OS의 적어도 일부분들을 업데이트할 것을 요청하면, 공통 OS 업데이트는 단계(306)에서 저장된 업데이트된 OS 프로파일에 적어도 부분적으로 기초하여 진행될 것이다.

[0059] 따라서, 공통 OS는 단계(312)들마다 다운로드될 수 있다. 이동 장치, eUICC 또는 로컬 캐리어 네트워크의 특정 구현 요청사항들로 인해, 공통 OS 패키지는 단계(306)에서 이전에 저장된 OS 프로파일에 대응하여 커스터마이즈될 수 있다(단계(314)마다). 풀-피처드 공통 OS가 이동 장치로 다운로드되고 새로운 공통 OS로 어셈블된다.

[0060] 일부 경우들에서, 복수의 공통 OS는 예를 들어, 복수의 eSIM 등을 지원하도록 이동 장치 내에 저장될 수 있다. 부트스트랩 OS는 eSIM들의 실행을 제어할 것이고, 이는 적절한 공통 OS의 선택을 포함할 수 있다. 일부 실시예들에서, 공통 OS 및/또는 그의 여러 컴포넌트들의 실행은 호환가능성에 의존하여 행해질 수 있다(예를 들어, 부트스트랩 OS는 공통 OS에, 공통 OS 컴포넌트는 공통 OS 컴포넌트에, 기타 등등).

[0061] **방법들-**

[0062] 이제부터 도 4를 참조하여, 휴대전화 네트워크를 통해 전자 식별 컴포넌트들을 전달하기 위한 일반화된 방법(400)의 일 실시예가 개시된다. 프리 로딩된 제한된 기능 액세스 모듈을 갖는 이동 장치는 가입 계획 등의 일부로서 예를 들어, 세일, 프로모션에 의해 최종 사용자에게 배포된다. 액세스 모듈의 제한된 기능은 로컬 캐리어 네트워크와의 데이터 접속들을 구축하고, 캐리어 네트워크로부터 소프트웨어 패키지들을 다운로드하고, 수신된 패키지들을 어셈블하도록 구성된다.

[0063] 단계(402)에서, 이동 장치는 하나 이상의 허용가능한 캐리어 네트워크 상에서 업데이트 포털에 대한 접속을 구축한다. 업데이트 포털은 예를 들어, 캐리어 데이터 포털, 제3자 소프트웨어 벤더, 이동 장치 제조업자 등일 수 있다. 전자 식별 컴포넌트들을 제공할 수 있는 여러 유형들의 네트워크 엔터티들은 미국 특허 출원 번호 제13/093,722호(2011년 4월 25에 출원되고, 발명의 명칭이 "APPARATUS AND METHODS FOR STORING ELECTRONIC SUBSCRIBER IDENTITY MODULES"임) 및 제13/095,716호(2011년 4월 27일에 출원되고, 발명의 명칭이 "SYSTEM FOR DISTRIBUTION OF UNIQUE SUBSCRIBER IDENTITY MODULES"임), 및 미국 가특허 출원 번호 제61/479,319호(2011년 4월 26일에 출원되고, 발명의 명칭이 "ELECTRONIC ACCESS CLIENT DISTRIBUTION APPARATUS AND METHODS"임) 및 제61/483,582호(2011년 5월 6일에 출원되고, 발명의 명칭이 "METHODS AND APPARATUS FOR PROVIDING MANAGEMENT

CAPABILITIES FOR ACCESS CONTROL CLIENTS"임) 내에 개시되어 있으며, 상기한 출원들 각각은 본 명세서에서 전체적으로 참조로 포함된다. 예를 들어, eUICC 기기 또는 eSIM 디포(depot)는 이동 장치들에 대하여 보안 접속들을 구축하여 현존하는 eSIM들을 교환하거나 수정할 수 있는 네트워크 구조들이다.

[0064] 일부 실시예들에서, 프리 로딩된 제한된 기능 액세스 모듈은 복수의 우선적인(preferred) 캐리어에 대하여 스캔하도록 구성될 수 있다. 복수의 캐리어가 이용가능하면, 장치는 하나 이상의 캐리어 네트워크의 이용가능성을 판정하고, 이용가능한 캐리어들의 리스트로부터 선택을 행한다. 일 실시예에서, 캐리어들의 리스트는 "우선적인" 캐리어들로 추가적으로 우선순위화되고, 우선적인 캐리어들은 예를 들어, 비지니스 고려사항들, 사용자 선호도들 등으로 인해 다른 캐리어들보다 우선순위화된다. 일부 실시예들에서는, 캐리어들의 리스트가 그래픽 사용자 인터페이스(GUI)를 통해 사용자에게 제시된다.

[0065] 일부 변형들에서, 캐리어는 이동 장치를 TSM(Trusted Service Manager) 포털에 연결한다. TSM은 이동 장치에 업데이트 패키지들을 전달하기 위하여 로컬 캐리어에 의해 인증되는 엔터티이다.

[0066] 하나의 예시적인 실시예에서, 단계(402)는 장치가 작동하는 액세스 제어 클라이언트를 갖기 전에 인증된 데이터 세션을 요청한다. 구체적으로, 단계(402)는 장치가 유효한 eSIM을 활성화시키기 전에 수행된다. 이제부터, 본 명세서에서 이전에 포함된 공유되고 동시 계류 중인 미국 특허 출원 번호 제13/080,521호(2011년 4월 5일 출원되고, 발명의 명칭이 "METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS"임)에 개시된 보안 전송 방식의 일 실예를 참조하도록 한다. 당업자들은 이하의 방식이 다른 유사한 방식들에 의해 대체될 수 있음을 이해할 것이다.

[0067] 따라서, 예시적인 실시예에서, 이동 장치는 소프트웨어 엔터티, 예를 들어, eUICC의 물리적으로 보호된 보안 요소에 저장되는 암호화 공용키/개인키 쌍(예를 들어, RSA(Rivest, Shamir and Adleman) 알고리즘)에 의해 하드코딩된다. 또한, eUICC의 신뢰성 및 개인키의 보안은 eUICC 키 쌍에 대한 "보증(endorsement)" 인증서를 발행한 신뢰된 엔터티에 의해 더욱 증명된다. 신뢰된 엔터티의 한 예로는 예를 들어, 장치 제조업자, 네트워크 오퍼레이터 등일 수 있다.

[0068] 간단한 부연으로서, 공용키/개인키 쌍은 보안 개인키 및 공개된 공용키를 포함한다. 공용키에 의해 암호화된 메시지는 적절한 개인키를 사용하여서만 암호해독될 수 있다. 암호화 및 암호해독에 사용된 키가 상이하면, 공용키/개인키 방식들은 "비대칭형"인 것으로 고려되며, 따라서 암호기 및 암호해독기는 동일한 키를 공유하지 않는다. 반대로, "대칭형" 키 방식들은 암호화 및 암호해독 모두에 동일한 키(또는 사소하게 변형된 키들)를 사용한다. RSA(Rivest, Shamir and Adleman) 알고리즘은 관련된 기술들 내에서 통상적으로 사용되는 공용키/개인키 쌍 암호 기법 중 한 유형이지만, 본 발명은 RSA 알고리즘 또는 사실상의 비대칭형 기술들에 제한되지 않는 방식으로 됨을 인식할 것이다.

[0069] 보증키(endorsement key) 쌍들은 비대칭형이기 때문에, 공용키들은 개인키들의 무결성을 훼손시키지 않고 배포될 수 있다. 따라서, 보증키 및 인증서는 이전에 알려지지 않은 당사자들(예를 들어, 이동 장치 및 로컬 캐리어 업데이트 포털) 간의 통신을 보호하고 검증하는 데에 사용될 수 있다.

[0070] 상술한 교환이 성공적으로 완료되는 것(예를 들어, 이동 장치 및 로컬 캐리어 업데이트 포털의 상호 검증)은 이동 장치 및 로컬 캐리어 업데이트 포털이 합법적이고 이제는 공유된 세션키를 가지고 있다는 것을 보장한다. 공유된 세션키는 이동 장치와 로컬 캐리어 업데이트 포털 간의 보안 세션을 수행하는 데에 사용된다.

[0071] 다시 도 4를 참조하면, 단계 404에서, 이동 장치는 하나 이상의 컴포넌트를 요청하거나, 또는 하나 이상의 컴포넌트를 다운로드하라고 지시받는다. 일 실시예에서, 여러 컴포넌트들은 필요한 다운로드 사이즈를 최소화하기 위하여 이동 장치로 프리 로딩될 수 있다. 예를 들어, 예시적인 일 실시예에서, (상이한 모든 OS 및 eSIM에 걸쳐 공통인 그것들의 컴포넌트들을 포함하는) 일반적으로 사용되는, 큰 사이즈의 부분들은 제조 중에 이동 디바이스에 프리 로드된다; 프리로드된 부분은 다운로드될 필요가 없고 패키지 크기를 줄일 수 있다. 따라서, 이동 디바이스는 프리로드되었던 컴포넌트들을 다운로드 할 필요가 없다.

[0072] 일 구체화 예에서, 업데이트 포탈은 업데이트 요청(예를 들면, eSIM 다운로드, 운영 체제 다운로드, 사용자 계정 데이터 다운로드 등), 사용자 계정 정보, 관련된 계획과 서비스, 및 식별 정보를 분석하고, 대응하여 적절한 업데이트 패키지를 생성한다. 일부 변형에 있어서, 업데이트 요청은 업데이트 패키지를 생성하기 전에 인가되고 그리고/또는 검증된다.

[0073] 단계 406에서, 업데이트 패키지가 준비된다. 일 실시예에서, 업데이트는 더 쉬운 전송을 위해 여러 패키지로 분할된다. 단계 408에서, 업데이트 패키지(들)은 목표에 무선으로 안전하게 전송된다. 이러한 패키지들은, 전

체적으로 또는 부분적으로, 운영 체제 컴포넌트들, 액세스 제어 클라이언트들, 사용자 계정 데이터 등을 포함할 수 있다. 예시적인 일 실시예에서, 이동 디바이스는 액세스 제어 클라이언트를 다운로드 및/또는 업데이트한다. 일 변형에서, 액세스 제어 클라이언트는 eSIM이다. eSIM의 여러가지 타입은 SIM(Subscriber Identity Module), USIM(Universal Subscriber Identity Module), RUIM(Removable User Identity Module) 등을 에뮬레이트하도록 구성되어 있다. 일부 실시예에서, 액세스 제어 클라이언트는, 예를 들어 그 전체가 참조로서 포함되며, 제목이 "POSTPONED CARRIER CONFIGURATION" 이고 공동 소유, 공동 계류된 2009년 1월 13일에 출원된 미국 특허 출원번호 제12/353,227호 내에서 기술된 지연 방식(postponed scheme)을 통해 전송시에 결정될 수 있다.

[0074] 다른 실시예에서, 이동 디바이스는 운영 체제(OS) 또는 OS 컴포넌트들을 다운로드 및/또는 업데이트 한다. 예를 들어, 이러한 운영 체제 컴포넌트들은 공용 또는 개인 키(key), 새로운 암호화 알고리즘, 보안 액세스를 위한 업데이트 절차, 새로운 디바이스 인증서, 하나 혹은 그 이상의 다른 신뢰된 공급 업체 인증서 등을 포함할 수 있다. 예를 들면, 통신하는 당사자의 아이덴티티를 검증하고, 그 검증된 아이덴티티에 상응하는 액세스 레벨을 승인하는 액세스 모듈은 검증의 방법에 대한 임의의 수의 변경들 및/또는 허가될 수 있는 액세스 레벨들을 가질 수 있다는 것을 알게 된다.

[0075] 또 다른 변형에서, 운영 체제 컴포넌트들은 액세스 제어 동작을 지원하도록 구성되지만, 액세스 제어와는 직접적으로 연관되지 않는다. 예를 들면, 보통의 OS 서비스는 파일 입력 및 출력, 파일 관리, 메모리 할당 등을 포함한다.

[0076] 단계 408에서, 패키지(들)을 수신하고 인증할 때, 이동 디바이스는 컴포넌트들을 어셈블링하고 업데이트한다. 이 후, 이동 디바이스는 새로이 어셈블링되고 업데이트된 액세스 제어 클라이언트로 가입자 세션(subscriber session)을 구축할 수 있고, 이 가입자 세션은 조작자의 무선 네트워크 서비스의 사용을 가능하게 한다. 예를 들면, 업데이트된 이동 디바이스는 음성 호출을 행하고, 사용자 데이터 등을 수신하고 전송하기 위해 업데이트된 eSIM을 활성화할 수 있다.

[0077] **예시적 이동 장치**

[0078] 이제 도 5를 참조하면, 본 발명의 방법을 구현하는데 유용한 예시적인 장치(500)가 도시되었다.

[0079] 도 5의 예시적인 UE 장치는 디지털 신호 프로세서, 마이크로프로세서, 필드 프로그램가능한 게이트 어레이, 또는 하나 이상의 기판상에 탑재된 복수의 프로세싱 컴포넌트들과 같은 프로세서 서브시스템(processor subsystem)(502)을 가진 무선 디바이스이다. 프로세싱 서브시스템은 또한 내부 캐쉬 메모리를 포함할 수 있다. 프로세싱 서브시스템은, 예를 들어 SRAM, 플래쉬 및 SDRAM 컴포넌트들을 포함할 수 있는 메모리를 포함하는 메모리 서브시스템(504)에 연결되어 있다. 메모리 서브시스템은 당 기술 분야에서 잘 알려진 것처럼 데이터 액세스를 용이하게 하도록, 하나 이상의 DMA 타입의 하드웨어를 구현할 수 있다. 메모리 서브시스템은 프로세서 서브시스템에 의해서 실행 가능한 컴퓨터 실행가능 명령어들을 포함한다.

[0080] 본 발명의 예시적인 일 실시예에서, 디바이스는 하나 이상의 무선 네트워크에 접속하도록 구성된 하나 이상의 무선 인터페이스(506)를 포함할 수 있다. 다수의 무선 인터페이스는 적절한 안테나 및 모뎀 서브시스템을 장착함으로써 GSM, CDMA, UMTS, LTE/LTE-A, WiMAX, WLAN, Bluetooth 등과 같은 상이한 무선 기술들을 지원할 수 있다.

[0081] 사용자 인터페이스 서브시스템(508)은 키패드, 터치 스크린(예를 들면, 멀티 터치 인터페이스), LCD 디스플레이, 백라이트, 스피커 및/또는 마이크로폰을 제한 없이 포함하는 잘 알려진 임의의 수의 I/O를 포함한다. 그러나, 어떤 애플리케이션에서는 이들 컴포넌트들 중의 하나 이상이 제거될 수 있다는 점이 인식된다. 예를 들면, PCMCIA 카드 타입 클라이언트 실시예들은 (그 실시예들은 그것들이 물리적으로 및/또는 전기적으로 연결되는 호스트 디바이스의 사용자 인터페이스에 피기백 방식으로 장착될 수 있기 때문에) 사용자 인터페이스가 없을 수 있다.

[0082] 도시된 실시예에서, 디바이스는 eUICC 애플리케이션을 포함하고 동작시키는 보안 요소(510)를 포함한다. eUICC는 복수의 액세스 제어 클라이언트를 저장하고 액세스할 수 있고, 액세스 제어 클라이언트는 각각의 네트워크에 사용자를 인증하도록 구성된다. 보안 요소는 프로세서 서브시스템의 요청시에 메모리 서브시스템에 의해 액세스가능하다. 또한 보안 요소는 소위 "보안 마이크로프로세서(secure microprocessor)" 혹은 보안 분야에서 잘 알려진 형태의 SM을 포함할 수 있다.

[0083] 더욱이, eUICC의 다양한 구현들은 이동 디바이스와 포탈 사이에 보안 접속을 구축하도록 구성된 액세스 모듈을

포함한다. 몇몇의 실시예들에서, eUICC는, 기존의 eSIM의 이득 없이, 더욱이 사용자의 장비가 배치된 이후에도, 포탈에 대한 보안 접속을 구축할 수 있다. 일 변형에서, 디바이스는 임의의 단일 eSIM(및 eSIM을 발행하는 MNO)과 관련된 대칭 키(symmetric key)와 분리된 별개의 비대칭 승인 키 쌍(asymmetric endorsement key pair)을 가진다.

[0084] 다시 도 5를 참조하면, 예시적인 일 실시예에서, 액세스 모듈은 하나 또는 그 이상의 액세스 제어 클라이언트들의 사용을 위해 컴포넌트들을 수신하고 저장하는 것이 가능하다. 하나의 예시적 실시예에서, 보안 요소는 연관된 승인 키를 가지고 있다. 이 승인 키는 이동 디바이스와 외부 업데이트 포탈 사이의 통신을 보호하고 검증하는데 사용된다. 그러한 일 변형에서, 승인 키는 비대칭 공용/개인 키 쌍의 개인 키이다. 반대쪽 공용 키는 개인 키의 무결성을 손상시킴이 없이 자유롭게 분배될 수 있다. 이러한 일 변형에서, 디바이스에는 공용/개인 키가 할당된다. 그러한 또 다른 변형에서, 디바이스는 내부적으로 공용/개인 키 쌍을 생성한다. 대안의 변형들에서, 승인 키는 대칭 키 알고리즘에 기초한다. 승인 키는 승인 키의 무결성을 보장하기 위해 주의하여 분배되어야 한다.

[0085] 또한, 예시적인 실시예의 다양한 구현은 동작을 위한 적어도 하나의 액세스 제어 클라이언트를 선택하기 위해 추가 구성된 부트스트랩 운영체제를 포함한다. 일 변형에서, 부트스트랩 운영체제는 실행 전에 액세스 제어 클라이언트의 무결성을 검증할 수 있다. 더욱이, 일 실시예에서, 부트스트랩 OS는 다수의 액세스 제어 클라이언트 중 적어도 하나를, 선택적으로 저장, 선택 및 실행하도록 구성된다. 특히, 본 발명의 다양한 구현예들은 다수의 eSIM을 저장하고, 현재의 네트워크 캐리어와의 동작을 위해 eSIM을 선택적으로 활성화하도록 구성된다.

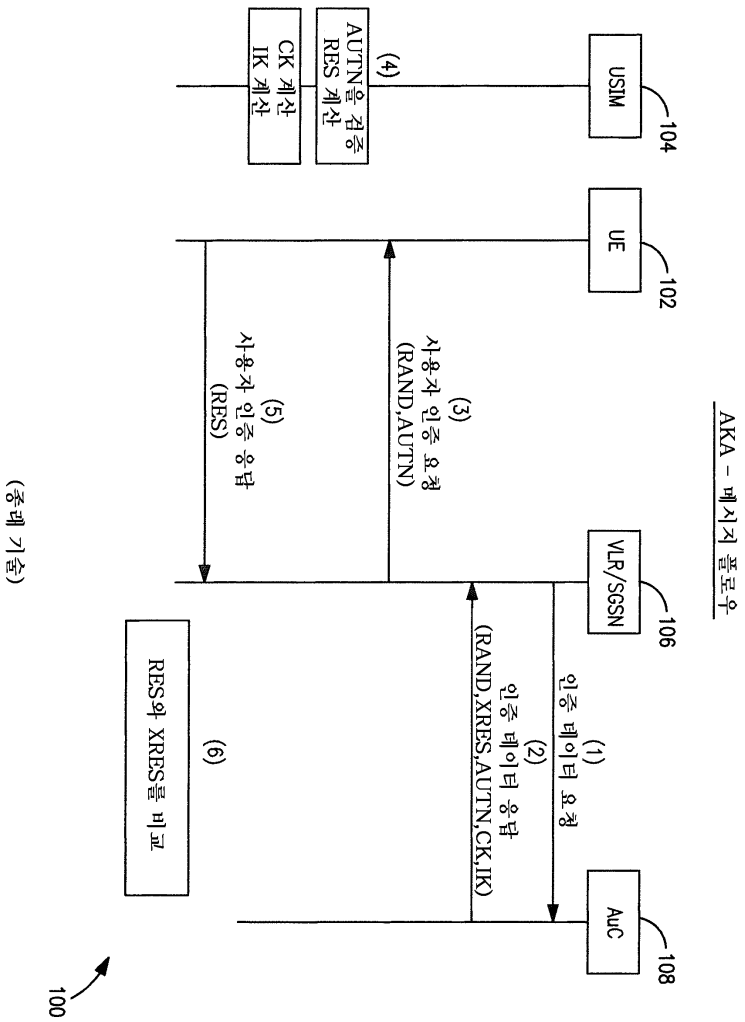
[0086] 셀룰러 디바이스에 전자 식별 컴포넌트들을 전달하기 위한 앞서 말한 방법들과 장치가 셀룰러 네트워크를 통해 도시되었지만, 다른 분배 방식들이 마찬가지로 대체될 수 있다는 것은, 당업자들에 의해, 쉽게 이해된다. 예를 들면, 다른 변형에서, 전자 식별 컴포넌트들은 근거리 통신네트워크 혹은 개인 영역 통신네트워크를 통해 분배될 수 있다.

[0087] 본 발명의 특정 양태가 방법의 단계들의 특정 시퀀스에 의하여 설명되었지만, 이런 설명들은 단지 본 발명의 광범위한 방법들을 예시하는 것이며, 특정한 애플리케이션에 의해 요구되는대로 수정될 수 있다는 것을 인지할 수 있다. 특정 단계들은 특정 환경에서 불필요하게 또는 선택적으로 재현될 수 있다. 추가적으로, 특정 단계들 또는 기능성은 개시된 실시예들 또는 두개 이상의 치환된 단계의 성능 순서에 추가될 수 있다. 그러한 모든 변형들은 본 명세서에 개시되고 청구되는 발명내에 포함되는 것으로 고려된다.

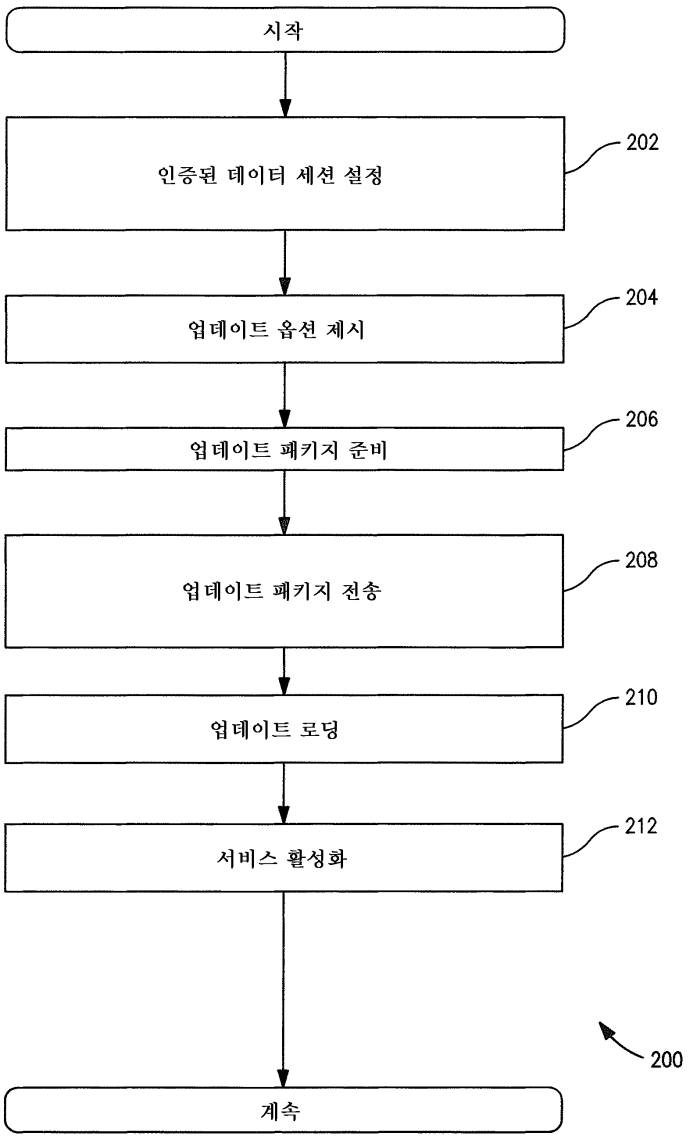
[0088] 전술한 상세한 설명이 다양한 실시예들에 적용된 것과 같이 본 발명의 신규한 특징들을 보여주고, 설명하고, 알려주는 한편, 본 발명으로부터 벗어나지 않고, 이 분야의 숙련자들에 의해, 도시된 디바이스 또는 프로세스의 양식 및 세부사항들에 다양한 생략, 대체 및 변경을 행할 수 있음을 이해할 수 있을 것이다. 전술한 설명은 본 발명의 수행에 대해 현시점에 고려되는 최선의 모드이다. 이 설명은 절대 제한적인 것을 의미하는 것이 아니며, 오히려 본 발명의 일반적인 원칙의 예시로서 채택되어야 한다. 본 발명의 범위는 청구항을 참조하여 결정되어야 한다.

도면

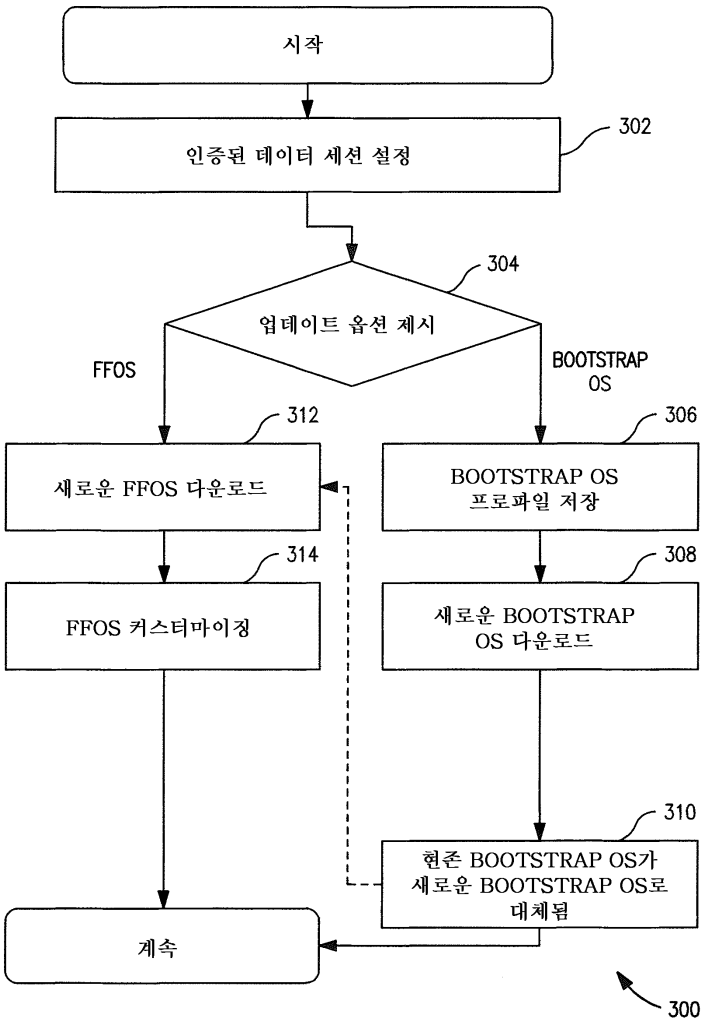
도면1


AKA - 메시지 플로우
USIM
104
UE
102
VLR/SGSN
106
AuC
108
(1) 인증 데이터 요청
(2) 인증 데이터 응답 (RAND,XRES,AUTN,CK,IK)
(3) 사용자 인증 요청 (RAND,AUTN)
(4) AUTN을 검증 RES 계산 CK 계산 IK 계산
(5) 사용자 인증 응답 (RES)
(6) RES와 XRES를 비교
(종래 기술)
100

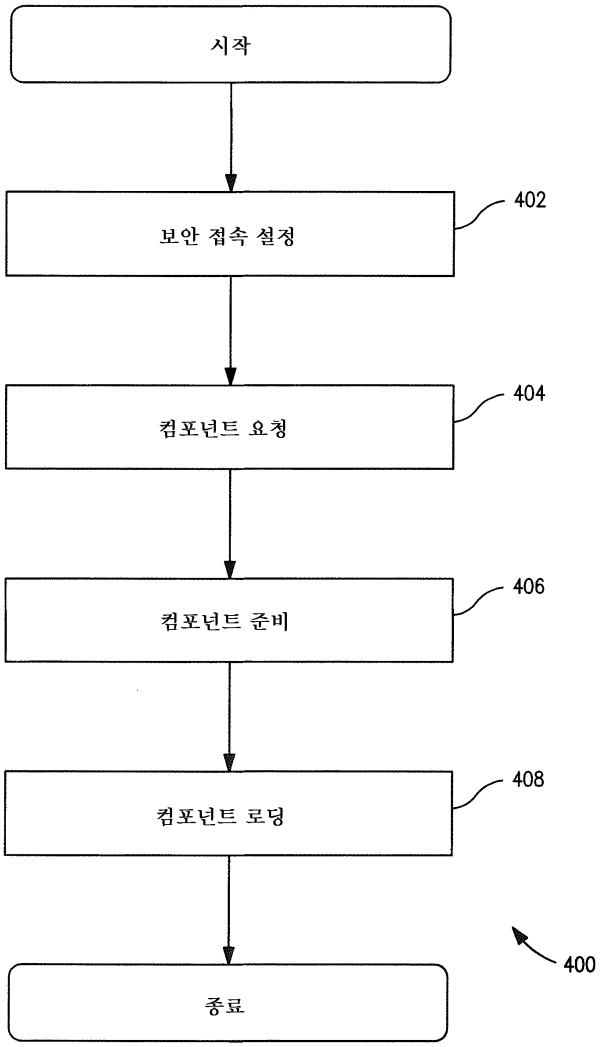
도면2


시작
인증된 데이터 세션 설정
202
업데이트 옵션 제시
204
업데이트 패키지 준비
206
업데이트 패키지 전송
208
업데이트 로딩
210
서비스 활성화
212
200
계속

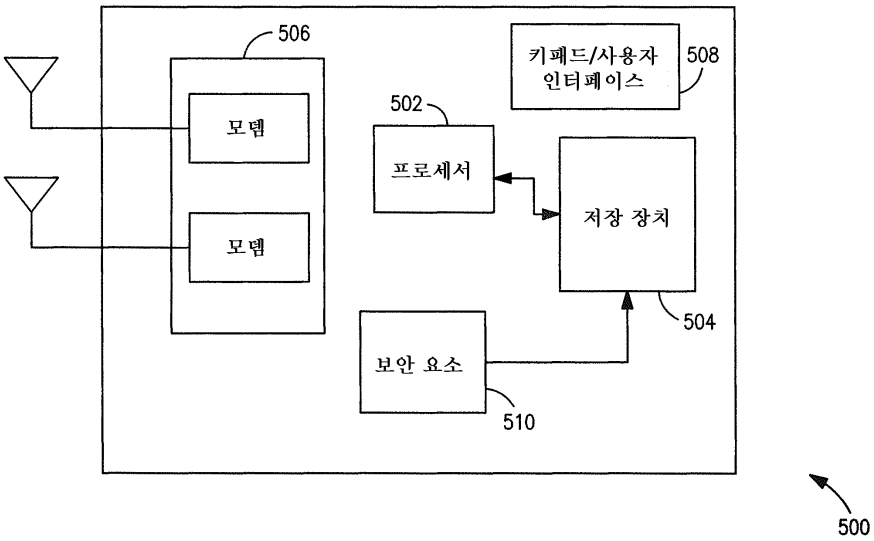
도면3


시작
인증된 데이터 세션 설정
302
304
업데이트 옵션 제시
FFOS
BOOTSTRAP OS
312
306
새로운 FFOS 다운로드
BOOTSTRAP OS 프로파일 저장
314
308
FFOS 커스터마이징
새로운 BOOTSTRAP OS 다운로드
310
현존 BOOTSTRAP OS가 새로운 BOOTSTRAP OS로 대체됨
계속
300

도면4


시작
보안 접속 설정
402
컴포넌트 요청
404
컴포넌트 준비
406
컴포넌트 로딩
408
종료
400

도면5


506
모뎀
모뎀
키패드/사용자 인터페이스
508
502
프로세서
저장 장치
504
보안 요소
510
500