(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년03월15일
(11) 등록번호 10-1716743
(24) 등록일자 2017년03월09일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04L 29/06* (2006.01)
H04W 8/20 (2009.01)
(52) CPC특허분류
H04W 12/06 (2013.01)
H04L 63/0853 (2013.01)
(21) 출원번호 10-2016-7011363(분할)
(22) 출원일자(국제) 2013년02월14일
심사청구일자 2016년05월10일
(85) 번역문제출일자 2016년04월28일
(65) 공개번호 10-2016-0052803
(43) 공개일자 2016년05월12일
(62) 원출원 특허 10-2014-7025521
원출원일자(국제) 2013년02월14일
심사청구일자 2014년09월12일
(86) 국제출원번호 PCT/US2013/026194
(87) 국제공개번호 WO 2013/123233
국제공개일자 2013년08월22일
(30) 우선권주장
61/598,819 2012년02월14일 미국(US)
13/767,593 2013년02월14일 미국(US)
(56) 선행기술조사문헌
KR1020090086276 A
KR1020080080160 A

(73) 특허권자
애플 인크.
미합중국 95014 캘리포니아 쿠퍼티노 인피니트 루프 1
(72) 발명자
해거티, 데이비드
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 87-2 씨지에스 인피니트 루프 1
호크, 제롤드
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 111-에이치오엠 인피니트 루프 1
(뒷면에 계속)
(74) 대리인
권성락, 양영준, 백만기

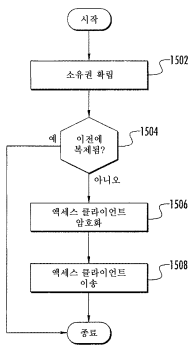
전체 청구항 수 : 총 20 항 심사관 : 문형섭

(54) 발명의 명칭 **복수의 액세스 제어 클라이언트를 지원하는 모바일 장치, 및 대응 방법들**

(57) 요 약

전자 액세스 제어 클라이언트들의 대규모 배포를 위한 방법들 및 장치, 하나의 태양에서, 계층형 보안 소프트웨어 프로토콜이 개시된다. 하나의 예시적인 실시예에서, 서버 eUICC(electronic Universal integrated Circuit Card)와 클라이언트 eUICC 소프트웨어는 소위 소프트웨어 계층들의 "스택"을 포함한다. 각 소프트웨어 계층은 그의 대응하는 피어 소프트웨어 계층들과 교섭되는 계층적 함수들의 세트에 대한 책임이 있다. 계층형 보안 소프트웨어 프로토콜은 eSIM(electronic Subscriber Identity Module)들의 대규모 배포를 위해 구성된다.

대 표 도 - 도15



(52) CPC특허분류
H04L 63/205 (2013.01)
H04W 8/20 (2013.01)
(72) 발명자
주앙, 벤
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 302-1 아이오에스 인피니트 루프 1
리, 리
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 302-1 아이오에스 인피니트 루프 1
마티아스, 아룬
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 302-2 아이오에스 인피니트 루프 1
맥로플린, 케빈
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 302-4 오에스4 인피니트 루프 1
나라시만, 아비나쉬
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 302-2 아이오에스 인피니트 루프 1
샤프, 크리스
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 87-2씨지에스 인피니트 루프 1
바이드, 유서프
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 302-2 아이오에스 인피니트 루프 1
양, 시앙잉
미국 95014 캘리포니아주 쿠퍼티노 엠/에스 302-2 아이오에스 인피니트 루프 1

명 세 서

청구범위

청구항 1

모바일 장치들에 포함되는 eUICC(electronic Universal Integrated Circuit Card)들과 연관되는 위태로운 디지털 인증서들(compromised digital certificates)을 대체하도록 구성되는 eUICC 관리 서버로서,

상기 eUICC 관리 서버로 하여금 단계들을 수행하도록 구성되는 프로세서를 포함하며, 상기 단계들은,

복수의 디지털 인증서와 연관되는 서명 기관이 위태롭다는(compromised) 표시를 수신하는 단계;

상기 복수의 디지털 인증서들 중 각각의 디지털 인증서에 대하여,

(i) 상기 디지털 인증서와 연관되는 eUICC와, (ii) 상기 eUICC가 포함되는 모바일 장치를 식별하는 단계; 및

업데이트된 디지털 인증서가 상기 디지털 인증서보다 신규인 경우, 상기 eUICC로 하여금 상기 디지털 인증서를 상기 업데이트된 디지털 인증서로 교체하도록 하는 단계

를 포함하는, eUICC 관리 서버.

청구항 2

제1항에 있어서,

상기 업데이트된 디지털 인증서에 포함되는 제2 에포크(epoch) 값이 상기 디지털 인증서에 포함되는 제1 에포크 값을 초과하는 경우, 상기 업데이트된 디지털 인증서가 상기 디지털 인증서보다 신규한 것인, eUICC 관리 서버.

청구항 3

제1항에 있어서,

상기 단계들은 또한,

공개키(PK_{eUICC})를 식별하는 단계 - 상기 공개키는, (i) 상기 eUICC에 대응하며 (ii) 상기 디지털 인증서와 연관됨 - ; 및

상기 업데이트된 디지털 인증서를 획득하는 단계 - 상기 업데이트된 디지털 인증서는 상기 PK_{eUICC}와, 상기 서명 기관에 대응하는 업데이트된 개인키($SK_{Updated\_SA}$)에 기초한 것임 - ;

를 포함하는, eUICC 관리 서버.

청구항 4

제3항에 있어서,

상기 복수의 디지털 인증서 중 각각의 디지털 인증서에 대하여, 상기 PK_{eUICC}를 식별하는 단계는, 최초에 상기 디지털 인증서가 생성되도록 한 인증서 서명 요청(Certificate Signing Request: CSR)을 획득하는 단계를 포함하는, eUICC 관리 서버.

청구항 5

제4항에 있어서,

상기 복수의 디지털 인증서 중 각각의 디지털 인증서에 대하여, 상기 디지털 인증서 및 상기 업데이트된 디지털 인증서는 (i) 상기 PK_{eUICC} 및 (ii) 상기 PK_{eUICC}에 대응하는 개인키(SK_{eUICC})와 연관되는, eUICC 관리 서버.

청구항 6

제3항에 있어서,

상기 복수의 디지털 인증서 중 각각의 디지털 인증서에 대하여, 상기 디지털 인증서는 상기 서명 기관에 대응하는 원본 개인키($SK_{Original\_SA}$)를 사용하여 디지털 방식으로 서명되며, 상기 $SK_{Original_SA}$는 위태로운(compromised), eUICC 관리 서버.

청구항 7

제6항에 있어서,

상기 $SK_{Updated_SA}$는 상기 $SK_{Original_SA}$의 변형(corruption)에 응답하여 상기 서명 기관에 의해 생성되는, eUICC 관리 서버.

청구항 8

모바일 장치들에 포함되는 eUICC들과 연관되는 위태로운 디지털 서명들을 대체하기 위한 방법으로서, eUICC 관리 서버에서,

복수의 디지털 인증서와 연관되는 서명 기관이 위태롭다는(compromised) 표시를 수신하는 단계;

상기 복수의 디지털 인증서들 중 각각의 디지털 인증서에 대하여,

(i) 상기 디지털 인증서와 연관되는 eUICC와, (ii) 상기 eUICC가 포함되는 모바일 장치를 식별하는 단계; 및

업데이트된 디지털 인증서가 상기 디지털 인증서보다 신규인 경우, 상기 eUICC로 하여금 상기 디지털 인증서를 상기 업데이트된 디지털 인증서로 교체하도록 하는 단계

를 포함하는 방법.

청구항 9

제8항에 있어서,

상기 업데이트된 디지털 인증서에 포함되는 제2 에포크(epoch) 값이 상기 디지털 인증서에 포함되는 제1 에포크 값을 초과하는 경우, 상기 업데이트된 디지털 인증서가 상기 디지털 인증서보다 신규한 것인, 방법.

청구항 10

제8항에 있어서,

공개키(PK_{eUICC})를 식별하는 단계 - 상기 공개키는, (i) 상기 eUICC에 대응하며 (ii) 상기 디지털 인증서와 연관됨 - ; 및

상기 업데이트된 디지털 인증서를 획득하는 단계 - 상기 업데이트된 디지털 인증서는 상기 PK_{eUICC}와, 상기 서명 기관에 대응하는 업데이트된 개인키($SK_{Updated\_SA}$)에 기초한 것임 - ;

를 더 포함하는 방법.

청구항 11

제10항에 있어서,

상기 복수의 디지털 인증서 중 각각의 디지털 인증서에 대하여, 상기 PK_{eUICC}를 식별하는 단계는, 최초에 상기 디지털 인증서가 생성되도록 한 인증서 서명 요청(Certificate Signing Request: CSR)을 획득하는 단계를 포함하는, 방법.

청구항 12

제11항에 있어서,

상기 복수의 디지털 인증서 중 각각의 디지털 인증서에 대하여, 상기 디지털 인증서 및 상기 업데이트된 디지털

인증서는 (i) 상기 PK_{eUICC} 및 (ii) 상기 PK_{eUICC}에 대응하는 개인키(SK_{eUICC})와 연관되는, 방법.

청구항 13

제10항에 있어서,

상기 복수의 디지털 인증서 중 각각의 디지털 인증서에 대하여, 상기 디지털 인증서는 상기 서명 기관에 대응하는 원본 개인키($SK_{Original\_SA}$)를 사용하여 디지털 방식으로 서명되며, 상기 $SK_{Original_SA}$는 위태로운(compromised), 방법.

청구항 14

제13항에 있어서,

상기 $SK_{Updated_SA}$는 상기 $SK_{Original_SA}$의 변형(corruption)에 응답하여 상기 서명 기관에 의해 생성되는, 방법.

청구항 15

명령어들을 저장하도록 구성되는 비일시적 컴퓨터 판독가능 저장매체로서, 상기 명령어들은, eUICC 관리 서버에 포함되는 프로세서에 의해 실행되는 경우, 단계들을 실행함으로써 상기 eUICC 관리 서버로 하여금 모바일 장치들에 포함되는 eUICC들과 연관되는 위태로운 디지털 인증서들을 교체하도록 하고, 상기 단계들은,

복수의 디지털 인증서와 연관되는 서명 기관이 위태롭다는(compromised) 표시를 수신하는 단계;

상기 복수의 디지털 인증서들 중 각각의 디지털 인증서에 대하여,

(i) 상기 디지털 인증서와 연관되는 eUICC와, (ii) 상기 eUICC가 포함되는 모바일 장치를 식별하는 단계; 및

업데이트된 디지털 인증서가 상기 디지털 인증서보다 신규인 경우, 상기 eUICC로 하여금 상기 디지털 인증서를 상기 업데이트된 디지털 인증서로 교체하도록 하는 단계

를 포함하는, 컴퓨터 판독가능 저장매체.

청구항 16

제15항에 있어서,

상기 업데이트된 디지털 인증서에 포함되는 제2 에포크(epoch) 값이 상기 디지털 인증서에 포함되는 제1 에포크 값을 초과하는 경우, 상기 업데이트된 디지털 인증서가 상기 디지털 인증서보다 신규한 것인, 컴퓨터 판독가능 저장매체.

청구항 17

제15항에 있어서,

상기 단계들은 또한,

공개키(PK_{eUICC})를 식별하는 단계 - 상기 공개키는, (i) 상기 eUICC에 대응하며 (ii) 상기 디지털 인증서와 연관됨 - ; 및

상기 업데이트된 디지털 인증서를 획득하는 단계 - 상기 업데이트된 디지털 인증서는 상기 PK_{eUICC}와, 상기 서명 기관에 대응하는 업데이트된 개인키($SK_{Updated\_SA}$)에 기초한 것임 - ;

를 포함하는, 컴퓨터 판독가능 저장매체.

청구항 18

제17항에 대하여,

상기 복수의 디지털 인증서 중 각각의 디지털 인증서에 대하여, 상기 PK_{eUICC}를 식별하는 단계는, 최초에 상기 디지털 인증서가 생성되도록 한 인증서 서명 요청(Certificate Signing Request: CSR)을 획득하는 단계를 포함하

는, 컴퓨터 판독가능 저장매체.

청구항 19

제18항에 있어서,

상기 복수의 디지털 인증서 중 각각의 디지털 인증서에 대하여, 상기 디지털 인증서 및 상기 업데이트된 디지털 인증서는 (i) 상기 PK_{eUICC} 및 (ii) 상기 PK_{eUICC}에 대응하는 개인키(SK_{eUICC})와 연관되는, 컴퓨터 판독가능 저장매체.

청구항 20

제17항에 있어서,

상기 복수의 디지털 인증서 중 각각의 디지털 인증서에 대하여, 상기 디지털 인증서는 상기 서명 기관에 대응하는 원본 개인키($SK_{Original\_SA}$)를 사용하여 디지털 방식으로 서명되며, 상기 $SK_{Original_SA}$는 위태로운(compromised), 컴퓨터 판독가능 저장매체.

발명의 설명

기 술 분 야

[0001] 우선권

[0002] 본 출원은 이와 함께 동시에 2013년 2월 14일자로 출원된 발명의 명칭이 "METHODS AND APPARATUS FOR LARGE SCALE DISTRIBUTION OF ELECTRONIC ACCESS CLIENTS"인 미국 특허 출원 제13/767,593호의 우선권을 주장하며, 이 선행 출원은 2012년 2월 14일자로 출원된 발명의 명칭이 "METHODS AND APPARATUS FOR LARGE SCALE DISTRIBUTION OF ELECTRONIC ACCESS CLIENTS"인 미국 가특허 출원 제61/598,819호의 우선권을 주장하며, 상기 출원들 각각은 그 전체 내용이 본 명세서에 참고로 포함된다.

[0003] 관련 출원

[0004] 본 출원은 공동 소유의 공히 계류 중인 2012년 4월 26일자로 출원된 발명의 명칭이 "ELECTRONIC ACCESS CLIENT DISTRIBUTION APPARATUS AND METHODS"인 미국 특허 출원 제13/457,333호, 2012년 5월 4일자로 출원된 발명의 명칭이 "METHODS AND APPARATUS FOR PROVIDING MANAGEMENT CAPABILITIES FOR ACCESS CONTROL CLIENTS"인 미국 특허 출원 제13/464,677호, 2011년 4월 27일자로 출원된 발명의 명칭이 "APPARATUS AND METHODS FOR DISTRIBUTING AND STORING ELECTRONIC ACCESS CLIENTS"인 미국 특허 출원 제13/095,716호, 2011년 4월 5일자로 출원된 발명의 명칭이 "APPARATUS AND METHODS FOR CONTROLLING DISTRIBUTION OF ELECTRONIC ACCESS CLIENTS"인 미국 특허 출원 제13/080,558호, 2010년 11월 22일자로 출원된 발명의 명칭이 "WIRELESS NETWORK AUTHENTICATION APPARATUS AND METHODS"인 미국 특허 출원 제12/952,082호, 2010년 11월 22일자로 출원된 발명의 명칭이 "APPARATUS AND METHODS FOR PROVISIONING SUBSCRIBER IDENTITY DATA IN A WIRELESS NETWORK"인 미국 특허 출원 제12/952,089호, 2011년 7월 14일자로 출원된 발명의 명칭이 "VIRTUAL SUBSCRIBER IDENTITY MODULE DISTRIBUTION SYSTEM"인 미국 특허 출원 제13/183,023호, 2009년 1월 13일자로 출원된 발명의 명칭이 "POSTPONED CARRIER CONFIGURATION"인 미국 특허 출원 제12/353,227호, 2011년 4월 25일자로 출원된 발명의 명칭이 "APPARATUS AND METHODS FOR STORING ELECTRONIC ACCESS CLIENTS"인 미국 특허 출원 제13/093,722호, 2011년 5월 17일자로 출원된 발명의 명칭이 "METHODS AND APPARATUS FOR ACCESS CONTROL CLIENT ASSISTED ROAMING"인 미국 특허 출원 제13/109,851호, 2011년 4월 4일자로 출원된 발명의 명칭이 "MANAGEMENT SYSTEMS FOR MULTIPLE ACCESS CONTROL ENTITIES"인 미국 특허 출원 제13/079,614호, 2011년 5월 19일자로 출원된 발명의 명칭이 "METHODS AND APPARATUS FOR DELIVERING ELECTRONIC IDENTIFICATION COMPONENTS OVER A WIRELESS NETWORK"인 미국 특허 출원 제13/111,801호, 2011년 4월 5일자로 출원된 발명의 명칭이 "METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS"인 미국 특허 출원 제13/080,521호, 2011년 4월 1일자로 출원된 발명의 명칭이 "ACCESS DATA PROVISIONING APPARATUS AND METHODS"인 미국 특허 출원 제13/078,811호, 2011년 11월 2일자로 출원된 발명의 명칭이 "METHODS AND APPARATUS FOR ACCESS DATA RECOVERY FROM A MALFUNCTIONING DEVICE"인 미국 특허 출원 제13/287,874호, 2011년 4월 5일자로 출원된 발명의 명칭이 "SIMULACRUM OF PHYSICAL SECURITY DEVICE AND METHODS"인 미국 특허 출원 제13/080,533호, 및 2011년 11월 11일자로 출원된 발명의 명칭이 "APPARATUS AND METHODS FOR RECORDATION OF DEVICE HISTORY ACROSS MULTIPLE

SOFTWARE EMULATION"인 미국 특허 출원 제13/294,631호와 관련이 있고, 상기 출원들 각각은 그 전체 내용이 본 명세서에 참고로 포함된다.

[0005] 본 개시 내용은 일반적으로 무선 통신 및 데이터 네트워크의 분야에 관한 것이다. 더 상세하게는, 본 발명은, 특히, 전자 액세스 제어 클라이언트들의 대규모 배포를 위한 방법들 및 장치에 관한 것이다.

배 경 기 술

[0006] 대부분의 종래 기술의 무선 라디오 통신 시스템들에서는 보안 통신을 위해 액세스 제어가 요구된다. 일례로, 하나의 간단한 액세스 제어 방식은 (i) 통신 파티(communicating party)의 ID(identity)를 검증하는 것과, (ii) 검증된 ID에 상응하는 액세스 레벨을 부여하는 것을 포함할 수 있다. 예시적인 셀룰러 시스템(예컨대, UMTS(Universal Mobile Telecommunications System))의 컨텍스트 안에서, 액세스 제어는 물리적 UICC(Universal Integrated Circuit Card)("SIM" 카드라고도 불림) 상에서 실행되는 USIM(Universal Subscriber Identity Module)이라고 불리는 액세스 제어 클라이언트에 의해 관리된다. USIM 액세스 제어 클라이언트는 UMTS 셀룰러 네트워크에 가입자를 인증한다. 성공적인 인증 후에, 가입자에게는 셀룰러 네트워크에의 액세스가 허용된다. 이하에서 사용되는, "액세스 제어 클라이언트"라는 용어는, 네트워크에의 제1 디바이스의 액세스를 제어하기에 적합한, 하드웨어 또는 소프트웨어 내에 구현된, 논리적 엔티티를 일반적으로 나타낸다. 액세스 제어 클라이언트들의 흔한 예들은 전술한 USIM, CSIM(CDMA Subscriber Identification Module), ISIM(IP Multimedia Services Identity Module), SIM(Subscriber Identity Module), RUIM(Removable User Identity Module) 등을 포함한다.

[0007] 종래의 SIM 카드 기반의 접근 방식들은 다수의 장애로 문제를 겪고 있다. 예를 들어, 전통적인 UICC들은 단 하나의 USIM(또는 더 일반적으로는 "SIM") 액세스 제어 클라이언트만을 지원한다. 사용자가 상이한 SIM을 이용하여 셀룰러 네트워크에 인증하기를 원한다면, 사용자는 디바이스 내의 SIM 카드를 상이한 SIM 카드로 물리적으로 교환해야만 한다. 일부 디바이스들은 동시에 2개의 SIM 카드를 수용하도록 설계되어 있지만(듀얼-SIM 폰들); 그러한 듀얼-SIM 폰들은 SIM 카드 디바이스들의 근본적인 물리적 한계를 해결하지 않는다. 예를 들어, 하나의 SIM 카드 내에 저장된 정보는 또 다른 SIM 카드 내에 저장된 정보와 쉽게 통합될 수 없다. 기존의 듀얼-SIM 디바이스들은 양쪽 SIM 카드들의 콘텐츠에 동시에 액세스할 수 없다.

[0008] 더욱이, SIM 카드에 액세스하려면 사용자에게 상당한 양의 시간이 필요하고; 정보를 이송하기 위해 SIM 카드들을 전환하는 것은 바람직하지 못하고, 전통적인 디바이스와 듀얼-SIM 디바이스 양쪽 모두에 존재한다.

[0009] 게다가, 기존의 SIM 카드 발행자들 및 활성화 엔티티들은 일반적으로 네트워크 특정적이고, 상이한 네트워크들의 상이한 사용자들에게 유비쿼터스하지 않다. 구체적으로, 주어진 네트워크 내의 주어진 사용자는 자신의 폰을 활성화하고 SIM 카드를 발행할 권한이 있는 매우 특정한 엔티티로부터 교체 SIM 카드들을 획득해야만 한다. 이것은 다른 네트워크들을 가로질러 로밍하는 경우, 자신의 폰을 교체하는 경우, 등등의 경우에, 유효한 액세스 권한을 신속히 얻는 사용자의 능력을 크게 제한할 수 있다.

[0010] 더 최근에는, 전자 SIM들(소위 eSIM들)이 예컨대 본 출원의 양수인에 의해 개발되었다. 이러한 전자 SIM들은 다른 eSIM과의 체인지아웃(changeout), 다른 디바이스로의 이송 등의 측면에서 강화된 융통성을 제공한다. 그러나, SIM들의 배포 및 활성화를 위한 기존의 네트워크 인프라는 이러한 발전에 따라가지 못하였다.

[0011] 이에 따라, 전자 액세스 클라이언트들(예컨대, eSIM들)에 의해 제공되는 강화된 융통성을 이용하고, 안전하고 유비쿼터스한 그의 배포를 지원하기 위한 새로운 솔루션들 및 인프라들이 필요하다.

발명의 내용

[0012] 본 개시 내용은, 특히, 전자 액세스 제어 클라이언트들의 대규모 배포를 제공한다.

[0013] 첫째로, 전자 액세스 제어 클라이언트들의 대규모 배포를 위한 방법이 개시된다. 하나의 예시적인 실시예에서, 이 방법은 하나 이상의 전자 액세스 제어 클라이언트들의 소유권(ownership)을 확립하는 단계; 하나 이상의 전자 액세스 제어 클라이언트들이 이전에 복제되지 않았는지를 판정하는 단계; 제2 디바이스로 이송하기 위해 하나 이상의 전자 액세스 제어 클라이언트들을 암호화하는 단계; 및 암호화된 하나 이상의 전자 액세스 제어 클라이언트들을 교환하는 단계를 포함한다.

[0014] 전자 액세스 제어 클라이언트들의 대규모 배포를 위한 장치가 또한 개시된다. 하나의 예시적인 실시예에서, 이 장치는 프로세서; 및 프로세서에 의해 실행될 때, 하나 이상의 전자 액세스 제어 클라이언트들의 소유권을 확립

하고; 하나 이상의 전자 액세스 제어 클라이언트들이 이전에 복제되지 않았는지를 판정하고; 제2 디바이스로 이송하기 위해 하나 이상의 전자 액세스 제어 클라이언트들을 암호화하고; 암호화된 하나 이상의 전자 액세스 제어 클라이언트들을 교환하는 명령어들을 포함하는 비일시적 컴퓨터 판독가능 매체를 포함한다.

[0015] 전자 액세스 제어 클라이언트를 취급하기 위한 모바일 디바이스가 또한 개시된다. 일 실시예에서, 이 디바이스는 무선 네트워크와 통신하도록 구성된 무선 인터페이스; 인터페이스와 데이터 통신하는 프로세서; 및 인터페이스와 데이터 통신하는 보안 요소를 포함한다. 하나의 변형례에서, 보안 요소는 보안 프로세서; 보안 프로세서와 데이터 통신하고, 적어도 네트워크와의 인증에 유용한 복수의 액세스 제어 클라이언트들이 저장된 보안 저장소; 및 보안 프로세서와 데이터 통신하는 로직을 포함하고, 이 로직은 장치로 또는 장치로부터 복수의 액세스 제어 클라이언트들을 저장하고, 그것들에 액세스하고, 그것들을 이송하도록 구성되며; 그리고 사용자 인터페이스 로직이 적어도 보안 요소와 통신하고, 장치의 사용자가 저장된 복수의 액세스 제어 클라이언트들 중 하나를 선택하고 네트워크와의 통신이 가능하도록 네트워크에 장치를 인증할 수 있게 하도록 구성된다.

[0016] 무선 시스템이 또한 개시된다.

[0017] 게다가, 컴퓨터 판독가능 장치가 개시된다. 일 실시예에서, 이 장치는 실행될 때 전자 액세스 제어 클라이언트들을 배포하도록 구성된 컴퓨터 프로그램이 배치된 저장 매체를 포함한다.

[0018] 게다가, 무선 모바일 디바이스들에 전자 액세스 클라이언트들을 제공하기 위한 네트워크 아키텍처가 개시된다. 일 실시예에서, 이 아키텍처는 복수의 브로커들 및 복수의 브로커들과 데이터 통신하는 복수의 제조사들을 포함한다. 하나의 변형례에서, 주어진 사용자 모바일 디바이스가 브로커들 중 다수의 브로커들에 의해 서비스를 받을 수 있고; 브로커들 중 임의의 브로커가 제조사들 중 하나 이상에 전자 액세스 클라이언트들을 주문할 수 있다.

[0019] 하나 이상의 모바일 디바이스들에 전자 액세스 클라이언트들을 제공하기 위한 장치가 또한 개시된다. 일 실시예에서, 이 장치는 적어도 하나의 프로세서; 및 적어도 하나의 프로세서와 데이터 통신하는 제1 로직 - 제1 로직은 장치가 액세스 클라이언트의 암호화 및 복호화를 수행하게 하도록 구성됨 -; 적어도 하나의 프로세서와 데이터 통신하는 제2 로직 - 제2 로직은 장치가 액세스 클라이언트가 복제되지 않는 것을 보장하게 하도록 구성됨 -; 및 적어도 하나의 프로세서와 데이터 통신하는 제3 로직 - 제3 로직은 장치가 액세스 클라이언트의 사용자의 신용, 소유권, 및/또는 검증 중 적어도 하나를 확립하게 하도록 구성됨 - 을 포함한다.

[0020] 전자 액세스 제어 클라이언트 폐기 절차가 또한 개시된다. 일 실시예에서, 이 절차는 인증서를 발행한 서명 인증 기관이 위태롭게 되었는지를 판정하는 단계 - 인증서는 인증서를 저장하는 하나 이상의 디바이스들과 연관됨 -; 인증서에 대한 최초 요청이 생성되었을 때 생성된 인증 서비스 요청을 하나 이상의 디바이스들에서 결정하는 단계; 결정된 인증 서비스 요청을 이용하여 새로운 인증서를 요청하는 단계; 및 요청에 기초하여 새로운 인증서를 발행하는 단계를 포함한다. 하나의 변형례에서, 하나 이상의 디바이스들은 요청의 일부로서 이전에 사용된 개인 키를 이용할 수 있고, 새로운 인증서는 이전의 개인 키에 대응하는 이전의 공개 키를 포함하여 발행된다.

[0021] 당업자들은 첨부된 도면들 및 아래에 주어진 예시적인 실시예들에 대한 상세한 설명을 참조하여 다른 특징들 및 이점들을 즉시 인지할 것이다.

도면의 간단한 설명

[0022] <도 1>

도 1은 본 개시 내용의 다양한 태양들과 함께 유용한 하나의 예시적인 eUICC(electronic Universal Integrated Circuit Card)의 논리적 블록도.

<도 2>

도 2는 본 개시 내용의 다양한 태양들과 함께 유용한 하나의 예시적인 eSIM(electronic Subscriber Identity Module) 디렉터리 구조의 논리적 블록도.

<도 3>

도 3은 본 개시 내용의 다양한 태양들과 함께 유용한 SIM(Subscriber Identity Module) 전용 파일들(SIM Dedicated Files, SDF)에 대한 하나의 예시적인 상태 기계를 나타내는 논리적 블록도.

<도 4>

도 4는 본 개시 내용의 다양한 태양들과 함께 유용한 eSIM 동작에 대한 하나의 예시적인 상태 기계를 나타내는 논리적 블록도.

<도 5>

도 5는 본 개시 내용의 다양한 태양들과 함께 유용한 하나의 예시적인 eSIM 브로커 네트워크의 그래픽 표현.

<도 6>

도 6은 본 개시 내용의 다양한 태양들과 함께 유용한 하나의 예시적인 계층형 보안 프로토콜(tiered security protocol)의 논리적 블록도.

<도 7>

도 7은 본 개시 내용의 다양한 태양들과 함께 유용한 3개의 부분(pieces)을 포함하는 하나의 예시적인 데이터 구조의 그래픽 표현.

<도 8>

도 8은 본 개시 내용의 다양한 태양들과 함께 유용한 하나의 예시적인 OEM 인증 계층 구조의 그래픽 표현.

<도 9>

도 9는 개인화 없이 eSIM을 디바이스에 전달하기 위한 하나의 예시적인 논리적 시퀀스를 보여주는 논리 흐름도.

<도 10>

도 10은 사전 개인화와 함께 eSIM을 디바이스에 전달하기 위한 하나의 예시적인 논리적 시퀀스를 보여주는 논리 흐름도.

<도 11>

도 11은 eSIM들의 배치(batch)를 디바이스에 전달하기 위한 하나의 예시적인 논리적 시퀀스를 보여주는 논리 흐름도.

<도 12>

도 12는 eUICC(electronic Universal Integrated Circuit Card) 장치의 논리적 표현.

<도 13>

도 13은 eSIM(electronic Subscriber Identification Module) 데포(depot) 장치의 논리적 표현.

<도 14>

도 14는 하나의 예시적인 사용자 장치를 보여주는 논리 흐름도.

<도 15>

도 15는 전자 액세스 제어 클라이언트들의 대규모 배포를 위한 방법의 일 실시예를 보여주는 논리 흐름도.

모든 도면들의 저작권© 2012-2013은 애플 인크.(Apple Inc.)에 있으며, 모든 도면들에 대한 복제를 불허한다.

발명을 실시하기 위한 구체적인 내용

[0023] 지금부터 전체에 걸쳐 유사한 도면 부호들이 유사한 부분들을 나타내는 도면들이 참조된다.

[0024] 예시적인 실시예들에 대한 설명

[0025] 지금부터 본 개시 내용의 예시적인 실시예들 및 태양들이 상세히 설명된다. 이러한 실시예들 및 태양들은 주로 GSM, GPRS/EDGE, 또는 UMTS 셀룰러 네트워크의 SIM(Subscriber Identity Module)의 컨텍스트에서 논의되지만, 당업자들은 본 개시 내용이 그렇게 제한되지 않는다는 것을 인지할 것이다. 사실상, 본 개시 내용의 다양한 특징들은 액세스 제어 클라이언트들을 디바이스들에 저장하고 배포하는 것으로부터 이익을 얻을 수 있는 임의의 네트워크(무선 셀룰러이든 아니든)에서 유용하다.

[0026] 본 명세서에서 사용되는, "클라이언트" 및 "UE"라는 용어들은 무선 지원(wireless-enabled) 셀룰러 전화, 스마

트폰(예를 들어 아이폰(iPhone)™과 같은), 무선 지원 퍼스널 컴퓨터(PC), 모바일 디바이스, 예를 들어, 핸드헬드 컴퓨터, PDA, PMD(personal media device), 무선 태블릿(예를 들어 아이패드(iPAD)™와 같은), 소위 "패블릿(phablet)", 또는 전술한 것들의 임의의 조합들을 포함하지만, 이들에 제한되지는 않는다.

[0027] 이하에서 사용되는, "SIM(Subscriber Identity Module)", "eSIM(electronic SIM)", "프로파일", 및 "액세스 제어 클라이언트"라는 용어는 네트워크에의 제1 디바이스의 액세스를 제어하기에 적합한, 하드웨어 또는 소프트웨어 내에 구현된, 논리적 엔티티를 일반적으로 나타낸다. 액세스 제어 클라이언트들의 흔한 예들은 전술한 USIM, CSIM(CDMA Subscriber Identification Module), ISIM(IP Multimedia Services Identity Module), SIM(Subscriber Identity Module), RUIM(Removable User Identity Module) 등, 또는 전술한 것들의 임의의 조합들을 포함한다.

[0028] 또한 "가입자 식별 모듈(subscriber identity module)"이라는 용어가 본 명세서에서 사용되지만(예컨대, eSIM), 이 용어는 결코 반드시 (i) 가입자 자신에 의한 사용을 암시하거나 요구하는 것은 아니고(즉, 본 개시 내용의 다양한 특징들은 가입자 또는 비가입자에 의해 실시될 수 있다); (ii) 단 하나의 개인의 식별을 암시하거나 요구하는 것은 아니고(즉, 본 개시 내용의 다양한 특징들은 가족과 같은 개인들의 그룹, 또는 기업과 같은 무형의 또는 허구의 엔티티를 대표하여 실시될 수 있다); 또는 (iii) 임의의 유형(tangible)의 "모듈" 장비 또는 하드웨어를 암시하거나 요구하는 것은 아니라는 것도 알 것이다.

[0029] 예시적인 eUICC 및 eSIM 동작

[0030] 지금부터 본 개시 내용의 다양한 특징들 및 기능들이 하나의 예시적인 구현예에 관하여 논의된다. 본 개시 내용의 예시적인 실시예의 컨텍스트에서는, 종래 기술에서와 같이 물리적 UICC를 이용하는 대신에, UICC는 UE 내의 보안 요소(예컨대, 보안 마이크로프로세서 또는 저장 디바이스) 내에 포함되어 있는, 이하에서 eUICC(Electronic Universal Integrated Circuit Card)라고 불리는, 예컨대, 소프트웨어 애플리케이션과 같은 가상 또는 전자 엔티티로서 에뮬레이트된다. eUICC는 이하에서 eSIM(Electronic Subscriber Identity Module)이라고 불리는, 다수의 SIM 요소들을 저장 및 관리할 수 있다. 각 eSIM은 전형적인 USIM의 소프트웨어 에뮬레이션이고, 유사한 프로그래밍 및 그와 연관된 사용자 데이터를 포함하고 있다. eUICC는 eSIM의 ICC-ID에 기초하여 eSIM을 선택한다. eUICC가 원하는 eSIM(들)을 선택하면, UE는 그 eSIM의 대응 네트워크 오퍼레이터로부터 무선 네트워크 서비스들을 획득하기 위한 인증 절차를 개시할 수 있다.

[0031] eUICC 소프트웨어 아키텍처

[0032] 이제 도 1을 참조하면 본 개시 내용과 함께 유용한 하나의 예시적인 eUICC(electronic Universal Integrated Circuit Card)가 도시되어 있다. 예시적인 eUICC의 예들은 앞서 그 전체 내용이 참고로 포함된, 공동 소유의 공히 계류 중인 2011년 4월 25일자로 출원된 발명의 명칭이 "APPARATUS AND METHODS FOR STORING ELECTRONIC ACCESS CLIENTS"인 미국 특허 출원 제13/093,722호에 기술되어 있지만, 본 개시 내용에 따라 다른 것이 이용될 수도 있다는 것을 알 것이다.

[0033] 도 1은 하나의 예시적인 자바 카드(Java Card)™ eUICC 아키텍처를 보여준다. 스마트 카드 애플리케이션들에서 사용되는 운영 체제(OS)들의 다른 예들로는 MULTOS 및 특허(proprietary) OS들이 있지만, 이들에 제한되지는 않고, 자바 카드는 예시에 불과하다. OS는 애플리케이션 소프트웨어와 하드웨어 간의 인터페이스를 제공한다. 일반적으로, OS는 입출력(I/O), 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 비휘발성 메모리(NV)(EEPROM, 플래시) 등을 위해 구성된 서비스들 및 기능을 포함한다. OS는 또한 상위 계층들에 의해 이용되는 암호 서비스들, 메모리 및 파일 관리, 및 통신 프로토콜들을 제공할 수 있다.

[0034] 예시적인 자바 구현예는 다음 3개의 부분: 자바 카드 가상 머신(Java Card Virtual Machine, JCVM)(바이트 코드 인터프리터); 자바 카드 실행 시간 환경(Java Card run time environment, JCRE)(카드 리소스들, 애플릿 실행 및 기타 실행 시간 특징들을 관리함); 및 자바 애플리케이션 프로그래밍 인터페이스들(Application Programming Interfaces, APIs)(스마트 카드 애플리케이션들의 프로그래밍을 위한 맞춤화(customize)된 클래스들의 세트)로 구성되어 있다.

[0035] JCVM은 온-카드 컴포넌트(바이트 코드 인터프리터), 및 오프-카드 카운터파트(컨버터)를 가지고 있다. 일부 컴파일 작업들은 카드 리소스 제약으로 인해 컨버터에 의해 수행될 수 있다. 처음에, 자바 컴파일러는 소스 코드로부터 클래스 파일들을 생성한다. 컨버터는 클래스 파일들을 전처리하고 CAP 파일을 생성한다. 컨버터는 자바 클래스들의 로드 이미지들이 제대로 구성되어 있는 것을 확인하고, 자바 카드 언어 서브세트 위반이 있는지를 체크하고, 또한 어떤 다른 작업들을 수행한다. CAP 파일은 자바 패키지 내의 클래스들의 실행가능 이진 표

현을 포함하고 있다. 컨버터는 또한 공개 API 정보를 포함하는 익스포트(export) 파일들을 생성한다. 단지 CAP 파일이 카드 내에 로딩된다. 또 다른 흔히 사용되는 포맷은 CAP 파일들로부터 변환될 수 있는 IJC이다. IJC 파일들은 CAP 파일들과 비교하여 크기가 약간 작을 수 있다.

[0036] 전형적으로, 애플릿을 카드에 다운로드하려면 CAP 파일의 콘텐츠를 카드의 지속성 메모리 안에 로드하기 위한 애플리케이션 프로토콜 데이터 유닛(Application Protocol Data Unit, APDU) 교환이 필요하다. 온 카드 인스톨러는 또한 CAP 파일 내의 클래스들을 카드 상의 다른 클래스들과 링크시킬 것이다. 그 후 설치 프로세스는 애플릿의 인스턴스를 생성하고 그 인스턴스를 JCRE에 등록한다. 애플릿들은 선택될 때까지 중지 상태(suspended state)로 유지된다.

[0037] 전술한 절차는 추가로 하나 이상의 보안 계층을 구현할 수 있다. 하나의 예시적인 실시예에서, 글로벌 플랫폼(Global Platform, GP)이 애플리케이션들을 관리하기 위한 보안 프로토콜을 제공한다. GP는 카드 발행자의 온-카드 표현인 보안 발행자 보안 도메인(secure issuer security domain) 내에서 동작한다. 카드는 또한, 예컨대, 애플리케이션 제공자들을 위한 다른 보안 도메인들을 실행할 수 있다.

[0038] 하나의 예시적인 실시예에서, eUICC는 디바이스의 비이동식 컴포넌트이다. 동작 중에, eUICC는 보안 부트스트랩 OS를 실행한다. 부트스트랩 OS는 eUICC가 안전하도록 보장하고, 그 안의 보안 프로토콜들의 실행을 관리한다. 보안 부트스트랩 SO의 예들은 앞서 그 전체 내용이 참고로 포함된, 공동 소유의 공히 계류 중인 2011년 4월 5일자로 출원된 발명의 명칭이 "METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS"인 미국 특허 출원 제13/080,521호에 기술되어 있다. 또한 상이한 모바일 네트워크 오퍼레이터들(Mobile Network Operators, MNO들)이 다양한 정도의 서비스 차별화를 지원하기 위해 eSIM들을 맞춤화할 수 있다는 것이 인지된다. 맞춤화의 흔한 예들로는 특허 파일 구조들 및/또는 소프트웨어 애플리케이션들이 있지만, 이들에 제한되지는 않는다. eSIM들의 구성 가능성으로 인해, eSIM들은 크기가 매우 다양할 수 있다.

[0039] 종래 기술의 SIM 카드들과 달리, eSIM들은 보안 트랜잭션에 따라 디바이스들 사이에 자유로이 교환될 수 있다. 가입자들은 디바이스들 사이에 SIM들을 이송하기 위해 "물리적 카드"를 필요로 하지 않지만; eSIM들의 실제 트랜잭션은, 예컨대, 특정 보안 프로토콜들을 통해 안전하게 보호되어야 한다. 하나의 예시적인 실시예에서, eSIM은 전달되기 전에 특정 수신기에 대해 암호화된다. 일부 변형례들에서는, 암호화된 콘텐츠에 더하여, 각 eSIM은 평문인 메타-데이터 섹션을 포함할 수 있다. 평문 콘텐츠의 무결성(integrity)을 보장하기 위해 암호 서명이 추가로 이용될 수 있다. 이 메타-데이터 섹션은 비보안 저장 등을 돕기 위해 자유로이 제공될 수 있다(불안전한 엔티티들에게조차).

[0040] eSIM 소프트웨어 아키텍처

[0041] 이제 도 2를 참조하면, 예시적인 eUICC 내에 구현된, 하나의 예시적인 eSIM(electronic Subscriber Identity Module) 디렉터리 구조가 개시되어 있다. 도시된 바와 같이, eSIM 디렉터리 구조는 eSIM들에 의해 제공되는 융통성을 지원하도록 수정되었다. 예를 들어, eSIM 디렉터리 구조는 특히 (i) 설치된 eSIM들의 목록을 포함하고 있는 EFeSimDir; (ii) eUECC를 전세계적으로 고유하게 식별하는 카드 일련 번호를 포함하고 있는 EFcsn; (iii) 하나 이상의 eUICC 인증서에 대응하는 개인 키 및 보안 관련 데이터를 저장하는 DFsecurity를 포함한다. 하나의 그러한 변형례에서, DFsecurity 정보는 (i) eUICC 플랫폼 레벨 PCF를 포함하고 있는 DFepcf; (ii) OEM의 루트 인증서 및 일반 이름을 포함하고 있는 EFoemcert(OEM 인증서는 공장 재정비(factory refurbishment)와 같은 특수 동작들에 이용될 수 있다); (iii) eUICC의 인증서인 EfeUICCcert; (iv) 서버 L1 어플라이언스들의 루트 인증서인 EFsL1cert; (v) 서버 L2 어플라이언스들의 루트 인증서인 EFsL2cert; 및 (vi) 서버 L3 어플라이언스들의 루트 인증서인 EFsL3cert를 포함한다.

[0042] 하나의 예시적인 실시예에서, 디렉터리 구조는 eSIM에 특유한 파일 구조들을 포함하고 있는 SIM 전용 파일들(SIM Dedicated Files, SDF)을 추가로 포함한다. 각 SDF는 MF 바로 아래에 위치해 있다. 각 SDF는 이름 속성 및 ICCID(Integrated Circuit Card Identifier)와 같은 SID(eSIM ID)를 가지고 있다. 도시된 바와 같이, 각 SDF는 DFprofile들 및 DFcode들을 추가로 포함하고 있다. 더욱이, 하나의 변형례에서, 모든 프로파일 PCF 관련 EF들은 DFprofile 아래에 저장되어 있는 DFppcf 아래에 저장된다.

[0043] 하나의 예시적인 실시예에서, DFprofile 정보는 (i) eSIM의 설명(예컨대, eSIM의 이름 및 버전)인 EFname; (ii) eSIM의 타입(예컨대, 정규, 부트스트랩, 및 테스트)을 기술하는 EFtype - 소프트웨어 애플리케이션들은, 예컨대, 부트스트랩 eSIM이 사용되고 있을 때 아이콘을 표시하기 위해 이 정보를 이용할 수 있다 -; (iii) eSIM을 지원하는 데 필요한 eUICC 소프트웨어의 최저 버전 번호인 EFsys_ver; (iv) eSIM에 의해 요구되는 비휘발성

메모리의 최저량을 나타내는 EFnv_min; (v) 요구되는 휘발성 메모리의 최저량을 나타내는 EFram_min; (vi) OTA(over the air transactions)를 위해 예약된 비휘발성 메모리의 양을 나타내는 EFnv_rsvd; 및 (vii) OTA를 위해 예약된 휘발성 메모리의 양을 나타내는 EFram_rsvd를 포함한다.

[0044] 하나의 예시적인 실시예에서, DFcode 정보는 각 eSIM에 대한 키들의 세트를 포함하고 있다. 이러한 값들은 대부분의 상황에서 eUICC로부터 판독될 수 없다. 하나의 예외적인 사용 경우는 전체 eSIM을 암호화로 래핑하고(wrap) 익스포트하는 익스포트 동작이다. 전체 eSIM이 암호화되어 있으므로, 키들의 값들은 안전하게 유지된다. 하나의 예시적인 실시예에서, DFcode 정보는 (i) 글로벌 PIN(Personal Identification Number) 및 PUK(PIN Unlock Key)를 포함하고 있는 ExEFgPinx/gPukx; (ii) 유니버설 PIN 및 PUK를 포함하고 있는 EFuPin/uPuk; (iii) ADMIN 코드들을 포함하고 있는 EFadminx; 및 (iv) OTA 코드들을 포함하고 있는 EFotax를 포함한다. 일부 변형예들에서는, (i) 128 비트 공유 인증 키인 K를 저장하고 있는 EFk; (ii) 가입자 키 및 오퍼레이터 변형 알고리즘 구성 필드 OP로부터 도출되는 OPc를 저장하고 있는 EFopc(일부 변형례들은 OPc 대신에 OP를 저장할 수 있다); (iii) RES의 길이를 명시하는 EFauthpar; (iv) 네트워크 인증 알고리즘(예를 들어, Milenage)을 명시하는 EFalgid; (v) SQN을 저장하고 있는 EFsan; 및 (vi) 로컬 PIN에 대한 PIN 및 PUK 코드를 저장하고 있는 EFlpinx/lpukx와 같은 추가 요소들을 포함하고 있는 ADFusim이 있을 수도 있다.

[0045] 이 개시 내용을 읽은 당업자들은 전술한 파일들, 구조들, 또는 요소들이 예시에 불과하고, 원하는 기능 또는 구조를 가지고 있는 다른 것들로 대체될 수도 있다는 것을 알 것이다.

[0046] 이제 도 3을 참조하면, SDF 동작에 대한 하나의 예시적인 상태 기계가 예시되어 있다. 도시된 바와 같이, SDF 상태 기계는 다음과 같은 상태들을 포함한다: CREATION(생성), INITIALISATION(초기화), OPERATIONAL(동작)(ACTIVATED(활성화됨)), 동작(DEACTIVATED(비활성화됨)), 및 TERMINATION(종료).

[0047] eSIM이 처음 설치될 때, SDF가 생성되고(CREATION) 그 후 초기화되고(INITIALISATION) 파일 구조 데이터가 eSIM에 포함된다. eSIM이 설치되면, SDF는 DEACTIVATED 상태로 전이한다. 이 비활성화 상태에서는, 파일들 중 아무 것도 이용 불가하다. eSIM이 선택되면, SDF는 DEACTIVATED 상태에서 ACTIVATED 상태로 전이하고; 이 ACTIVATED 상태는 SDF의 파일들에의 액세스를 가능하게 한다. eSIM이 선택 해제될 때(암시적으로 또는 명시적으로), SDF는 ACTIVATED 상태에서 다시 DEACTIVATED 상태로 전이한다.

[0048] 이제 도 4를 참조하면, eSIM 동작에 대한 하나의 예시적인 상태 기계가 예시되어 있다. 도시된 바와 같이, eSIM 상태 기계는 다음과 같은 상태들을 포함한다: INSTALLED(설치됨), SELECTED(선택됨), LOCKED(잠김), DEACTIVATED(비활성화됨), EXPORTED(익스포트됨), 및 DELETED(삭제됨).

[0049] eSIM 설치(INSTALLED) 중에, eSIM에 대한 항목이 eUICC 레지스트리에 생성된다; 이 항목은 하나 이상의 연관된 SDF 및 애플리케이션들을 나타낸다. INSTALLED 상태 동안, SDF는 DEACTIVATED 상태로 설정되고 애플리케이션들은 INSTALLED 상태로 설정된다.

[0050] eSIM이 선택되면, eSIM은 SELECTED 상태로 전이한다. 이 선택된 상태 동안, SDF들은 ACTIVATED 상태로 전이하고 애플리케이션들은 SELECTABLE(선택가능) 상태로 전이된다. eSIM이 선택 해제되면, eSIM은 다시 INSTALLED 상태로 전이한다.

[0051] 소정의 상황들에서, eSIM은 LOCKED 상태에 들어갈 수 있다. 예를 들어, eUICC PCF가 설치된 eSIM이 더 이상 사용될 수 없도록 변경되면, eSIM은 LOCKED 상태로 전이할 것이다. LOCKED 상태에서, SDF는 DEACTIVATED 상태로 설정되고 애플리케이션들은 LOCKED 상태로 설정된다. 다른 잡다한 상태들은 EXPORTED 상태(즉, eSIM이 익스포트되어 더 이상 선택될 수 없는 경우), 및 DELETED 상태(즉, eSIM이 삭제된 경우)를 포함한다.

[0052] 네트워크 인증 알고리즘들

[0053] 네트워크 인증 알고리즘들(Network Authentication Algorithms, NAA)은 일반적으로 모바일 네트워크 오퍼레이터들(MNO들)과의 동작을 위해 필수적이다. NAA의 상이한 구현예들이 존재하지만, 그 기능은 많이 다르지 않다. 소정의 실시예들에서, eUICC는 NAA들을 위한 공통 패키지들을 포함할 수 있다. eSIM 설치 중에, eSIM의 전체적인 로딩 시간과, eUICC에서의 불필요한 메모리 소비를 줄이기 위해 사전 로딩된 패키지들로부터 각 eSIM에 대해 각 NAA 앱의 인스턴스가 생성될 수 있다.

[0054] NAA의 흔한 예들로는 Milenage, COMP128 V1, COMP128 V2, COMP128 V3, 및 COMP128 V4, 및 소정의 특허 알고리즘들이 있지만, 이들에 제한되지는 않는다. 여전히 사용되고 있는 더 많은 수의 특허 알고리즘들이 있다(COMPI28 VI에 대한 알려진 공격들로 인해). 일 실시예에서, 네트워크 인증은 잘 알려진 인증 및 키 합의

(Authentication and Key Agreement, AKA) 프로토콜에 기초한다.

[0055] 있을 것 같지는 않지만 NAA가 위태롭게 되는 경우에는, 교체 NAA 방식들이 소프트웨어 업데이트를 필요로 할 수 있다. 그러한 경우 동안에, 예컨대, 보안 소프트웨어 업데이트를 통해 교체 알고리즘과 함께 eSIM들이 패치될 수 있다. 그 후, MNO는 기존의 OTA 메커니즘을 통해 교체 알고리즘을 사용 가능하게 할 수 있다.

[0056] 예시적인 eSIM 브로커 네트워크

[0057] 도 5는 본 개시 내용의 다양한 실시예들과 함께 유용한 하나의 예시적인 eSIM 브로커 네트워크의 하이 레벨 뷰를 보여준다. 하나의 예시적인 실시예에서, 브로커 네트워크는 브로커들과 제조사들의 분산형 네트워크를 포함하고, 따라서 디바이스는 다수의 브로커들에 의해 서비스를 받을 수 있고, 브로커는 다수의 eSIM 제조사들에 eSIM들을 주문할 수 있다. 일부 실시예들에서는, 소정의 eSIM 동작들을 위해 디바이스가 통신할 수 있는 브로커들의 그룹을 제한하는 eUICC 및/또는 eSIM 프로파일 정책들이 존재할 수 있다. 예를 들어, MNO는 그 MNO에 의해 보조금을 받는 디바이스들만이 그 MNO에 의해 소유되는 브로커들과 통신할 것을 요구할 수 있다.

[0058] 하나의 그러한 변형례에서, 주요 브로커(primary broker)는 디바이스들에 발견 서비스들을 제공하고, 따라서 디바이스는 적절한 브로커를 식별할 수 있다. 그 후, 디바이스는 eSIM 동작들(예컨대, 구입, 설치, 익스포트, 및 임포트와 같은)을 위해 식별된 브로커와 직접 통신할 수 있다.

[0059] 관련 네트워크 기술의 당업자들은 도 5에 의해 나타낸 것과 같은 대규모 배포 네트워크들의 동작 중에 다수의 실제적인 문제들이 발생한다는 것을 인지할 것이다. 구체적으로, 대규모 배포 네트워크들은 (주어진 모바일 사용자 디바이스의 소위 "출시일"에 발생할 수 있는 것과 같은) 폭주하는 프로비저닝 트래픽을 다루기 위해 스케일러블(scalable)해야 한다. 전체적인 네트워크 트래픽을 줄이기 위한 하나의 제안된 방식은 (가능할 경우) 출시일 이전에 eSIM들을 사전 개인화하는 것을 수반한다. 예를 들어 소위 "SIM-in" 유닛들이 발송시 eSIM에 이미 할당되어 있다; 이 사전 할당된 eSIM은, 예를 들어, 그 유닛의 eUICC에 특유한 키로 대응 eSIM 프로파일을 암호화함으로써 그 유닛에 대해 사전 개인화될 수 있다.

[0060] 다른 고려 사항들은 시스템 신뢰도를 포함하는데, 예를 들어, 브로커 네트워크는 다양한 장비 고장들로부터 복구할 수 있어야 한다. 하나의 솔루션은 상이한 장소들에 걸쳐 다수의 데이터 센터들이 복제된 콘텐츠를 가지는 지리적 중복(geographic redundancy)이지만; 데이터 센터들의 네트워크는 eSIM 복제를 피하기 위해 서로 활발히 동기화할 수 있다. 그러한 네트워크 동기화는 엄청난 양의 네트워크 대역폭을 필요로 할 것이다. 대안의 솔루션들에서, 각 데이터 센터는 별개의 eSIM들의 세트를 가질 수 있지만; 이는 상당한 eSIM 오버헤드를 요구한다.

[0061] 이상적으로, 브로커 네트워크는 다양한 비즈니스 모델들에 유연하게 적응할 수 있다. 구체적으로, 다양한 법적인 그리고 독점 금지의 이유로, 전술한 브로커 네트워크의 다양한 컴포넌트들은 상이한 파티들에 의해 다루어질 수 있다. 그에 따라, eSIM 트래픽의 보안 측면들이 신중하게 모니터되고 평가될 필요가 있다. 각 eSIM은 소중한 사용자 및 MNO 정보를 포함하고 있다. 예를 들어, eSIM은 공유 인증 키(USIM의 경우 K 및 SIM의 경우 Ki)를 포함할 수 있는데, 이것은 위태롭게 될 경우 SIM 복제에 이용될 수도 있다. 유사하게, eSIM들은 은행 계좌 정보와 같은 민감한 사용자 데이터를 가질 수 있는 애플리케이션들을 포함할 수도 있다.

[0062] 더욱이, eUICC 소프트웨어는 디바이스 복구를 위한 추가의 대책들을 필요로 한다는 것도 인지된다. 물리적 SIM들과 달리, eUICC 소프트웨어가 복구 불능 상태가 되면, 디바이스 전체가 교체될 필요가 있을 것이다(이는 SIM 카드를 교체하는 것보다 훨씬 더 많은 비용이 든다). 그에 따라, 예시적인 솔루션들은 그러한 가혹한 조치를 배제하도록 디바이스 복구를 다룰 수 있어야 한다.

[0063] 마지막으로, 네트워크 동작은 "양호한" 사용자 체험을 제공해야 한다. 과도한 응답 시간, 신뢰할 수 없는 동작, 과도한 소프트웨어 충돌 등은 전반적인 사용자 체험을 상당히 손상시킬 수 있다.

[0064] 예시적인 보안 프로토콜

[0065] 그에 따라, 전술한 다양한 문제들을 해결하기 위해 본 명세서에서는 계층형 보안 소프트웨어 프로토콜(tiered security software protocol)이 개시된다. 하나의 예시적인 실시예에서, 서버 eUICC와 클라이언트 eUICC 소프트웨어는 소위 소프트웨어 계층들의 "스택"을 포함한다. 각 소프트웨어 계층은 그의 대응하는 피어 소프트웨어 계층들과 교섭되는 계층적 함수들의 세트에 대한 책임이 있다. 더욱이, 각 소프트웨어 계층은 추가로 그 자신의 계층들과 통신한다. 일부 경우에, 디바이스 애플리케이션 프로세서(AP)가 위태롭게 될(예컨대, "jailbroken" 등) 수 있다는 것도 인지되고; 따라서, 클라이언트 eUICC와 대응하는 서버 eUICC(또는 다른 보안 엔티티) 간에 신뢰 관계들이 존재한다는 것, 즉, AP가 신뢰할 수 없는 것임이 인지된다.

[0066] 하나의 예시적인 실시예에서, 3 계층형 시스템이 개시된다. 도 6에 예시된 바와 같이, 보안 소프트웨어 프로토콜은 레벨 1(L1), 레벨 2(L2), 및 레벨 3(L3)를 포함한다. L1 보안은 eSIM 데이터의 암호화 및 복호화를 수행한다. L1 동작들은 보안 실행 환경들(예컨대, eUICC 또는 하드웨어 보안 모듈(Hardware Security Module, HSM))로 제한된다. L1 내에서, eSIM 데이터는 논리적 L1 경계 내에 평문으로(예컨대, 암호화되지 않고) 저장될 수 있고; L1 경계의 밖에서 eSIM 데이터는 항상 안전하게 암호화된다. L2 보안은 eSIM이 복제될 수 없도록 보장한다. L2 경계는 eSMI의 하나의 유일한 사본만이 존재하도록 보장한다. L2 경계 내에 다수의 사본들이 존재할 수 있다. 더욱이, L2 보안은 암호화된 eSIM 페이로드 내에 챌린지를 더 포함시킬 수 있다; eSIM의 수취인은 그의 eSIM이 구식이 아니도록(즉, 현재의 하나의 유일한 eSIM이도록) 보장하기 위해 수신된 챌린지를 eSIM의 설치 전에 먼저 저장된 챌린지와 비교할 것이다. L3 보안은 사용자의 신용, 소유권 및 검증을 확립하는 데 책임이 있다. 각 eSIM마다, eUICC는 eSIM과 연관된 소유권을 나타내는 정보를 저장할 수 있다.

[0067] 하나의 예시적인 구현예에서, 소위 "챌린지들"은 특정 eSIM 인스턴스를 eUICC와 연관시키는 데 이용되는 중요한 리소스이다. 구체적으로, 각 eUICC는 L2 보안을 유지하는 논리적 엔티티인 각 프로파일 에이전트에 대해 소정 수의 챌린지를 유지한다. 챌린지가 유효함을 검증함으로써, eUICC는 eSIM이 구식 eSIM(즉, 무효한 복제본)이 아님을 확신할 수 있다. 개인화될 각 eSIM마다 다수의 챌린지들이 생성된다. eUICC는 매칭하는 eSIM이 수신될 때 챌린지를 삭제한다.

[0068] 하기의 사전 개인화 시나리오를 고려하면, eUICC가 네트워크에 제공되는 다수의 챌린지들을 생성하고(또는 제공받고); 이 챌린지들은 또한 eUICC의 비휘발성 메모리에 저장된다. 그 후에, 네트워크는 사전 생성된 챌린지에 결합되는 eSIM을 eUICC를 위해 생성할 수 있다. eUICC가 나중에 디바이스 활성화 중에 eSIM을 수신하면, eUICC는 수신된 eSIM이 적절한 챌린지를 포함하고 있는지를 검증할 수 있다.

[0069] 그러나, 전술한 방식의 하나의 결점은 일정한 수의 챌린지들이 서비스 거부(denial of service, DOS) 공격으로 쉽게 위태롭게 될 수 있다는 것이다. DOS 공격 시에, eUICC는 그의 모든 챌린지 리소스들이 고갈될 때까지 챌린지들을 생성하도록 계속해서 트리거된다. 그에 따라, 하나의 그러한 변형례에서, eUICC는 eUICC로 하여금 챌린지를 생성하도록 트리거할 요청들을 처리하기 전에 프로파일 서버/에이전트를 인증하기 위해 세션 핸드셰이크를 추가로 수행한다. 게다가, 있을 것 같지는 않지만 리소스들이 고갈되고 eUICC가 새로운 챌린지들을 생성하지 못하는 경우에는, eUICC는 또 다른 챌린지들의 세트를 풀어주도록 특별히 설계된 별개의 예약된 챌린지들의 세트를 저장할 수 있다. 일부 경우들에, eUICC는 OEM(Original Equipment Manufacturer)이 챌린지 동작을 추가로 제어하기 위해 이용할 수 있는 OEM 인증서를 추가로 포함할 수 있다.

[0070] 이제 도 7을 참조하면, eSIM에 대한 하나의 예시적인 데이터 구조가 예시되어 있다. 도시된 바와 같이, 이 예시적인 데이터 구조는 L1, L2, 및 L3 보안 레벨들 각각에 대해 하나씩 3개의 부분들을 포함한다. 보안 컴포넌트들을 별개의 레벨들로 분리시킴으로써, 전반적인 네트워크 동작이 매우 다양한 옵션들에 따라 다수의 엔티티들에 걸쳐 분산될 수 있다. 예를 들어, 다양한 네트워크 엔티티들이 보안 레벨들 중 하나 또는 2개만 수행할 수 있고(예컨대, eSIM 벤더는 L2만을 다룰 수 있다, 기타 등등); 이 융통성은 사실상 임의의 비즈니스 배열을 용이하고 유리하게 수용한다.

[0071] 도 7에 도시된 바와 같이, 비대칭 암호화(즉, 각 엔티티가 별개의 고유한 키를 가지고 있는 경우)가 대칭 동작(엔티티들이 키를 공유하는 경우)보다 훨씬 느리기 때문에, 각 eSIM 프로파일 컴포넌트(702)는 대칭 키로 암호화되고, 대칭 키는 목적지 eSIM 수신기의 L1 공개 키로 암호화된다. eSIM은 (ICCID의 텍스트 스트링과 같은) 메타데이터에 대한 평문 섹션을 추가로 포함할 수 있다. 암호화된 대칭 키, 메타 데이터, 및 암호화된 eSIM 콘텐츠는 "제공하는" L1 엔티티의 공개 키로 해싱되고 서명된다. 연관된 L1 인증서가, 검증을 위해, 예컨대, 끝에 부가된다.

[0072] 도 7의 배치 디스크립터(batch descriptor) 컴포넌트(704)는 eSIM에 대한 L2 정보를 포함하고 있다. 그것은 전역 고유 식별자(Globally Unique Identifier, GUID), 목적지 eSIM 수신기에 대한 챌린지, eSIM 수신기의 고유 ID, 프로파일을 검색할 URL, 및 설치 결과를 게시할 URL을 포함하는 평문 섹션을 가지고 있다. 배치 디스크립터는 또한 각 프로파일에 대한 ICCID, 및 프로파일의 해싱된 부분(메타데이터 섹션 및 암호화된 eSIM 콘텐츠)으로 이루어지는 요소들의 어레이의 평문 섹션을 포함한다. 일 실시예에서, 해시는 대칭 키를 포함하지 않고, 따라서 실제 프로파일이 생성되는 것을 기다리지 않고 배치 디스크립터가 생성될 수 있다. 디바이스 측 동작을 위해, 배치 디스크립터는 하나의 ICCID 및 프로파일 해시만을 포함하고 있다. 서버 대 서버 일괄 이송(server to server batching transfer)을 위해서는, 훨씬 더 큰 어레이가 예상된다. 배치 디스크립터의 데이터 콘텐츠는 L2 공개 키로 해싱되고 서명되며, 연관된 L2 인증서가 끝에 부가된다.

[0073] L3 오너(owner) 컴포넌트(706)는 eSIM에 대한 L3 정보를 포함하고 있다. 주요 필드는 eSIM과 연관된 사용자 계정(예컨대, abc@me.com)을 식별하고, 서비스 이름은 사용자 계정을 인증할 서비스 제공자를 식별한다. 배치 디스크립터의 해시는 L2 및 L3 데이터 구조들을 연관시키기 위해 포함된다. 데이터는 평문으로 저장되고, L3 공개 키로 해싱되고 서명될 수 있다. L3 인증서가 끝에 부가된다.

[0074] 본 명세서에 사용된 바와 같이, 3가지 타입의 인증서들이 있다: eUICC 인증서들, 서버 어플라이언스 인증서들, 및 OEM 인증서들. 일 실시예에서, 신뢰할 수 있는 제3자가 보증된 eUICC들에 대한 인증서들을 발행한다. 각 eUICC는 개인 키 및 이 엔티티 또는 이 엔티티의 하위 키 기관(subordinate key authority)에 의해 발행된 연관된 인증서를 포함하고 있다. 일부 실시예들에서, 하나의 신뢰할 수 있는 제3자가 보증된 L1, L2, 및 L3 어플라이언스들에 대한 인증서들을 발행할 수 있고; 또는 대안으로, 별개의 제3자 엔티티들이 L1, L2, 또는 L3 어플라이언스들에 대한 인증서들을 발행할 수 있다. 다수의 제3자들이 존재하는 경우, eUICC는 이 제3자들의 루트 인증 기관(Certificate Authority, CA)을 사전 로딩하였으며(또는 신뢰할 수 있는 엔티티로부터 OTA로 제공될 수 있으며), 적절한 CA에 기초하여 서버 어플라이언스들로부터 수신된 메시지들을 검증할 수 있다.

[0075] 이제 도 8을 참조하면, 하나의 예시적인 OEM 인증 계층 구조가 예시되어 있다. 루트 인증 기관(CA)은 작업들(예컨대, iOS 또는 비슷한 디바이스 인증서들의 발행)의 서브세트를 수행하는 중간 CA들의 세트를 가지고 있다. 도시된 바와 같이 eUICC CA가 eSIM 특유 동작들로 채워져 있다. 이 eUICC CA는 서버들의 세트에 대한 인증서들을 발행할 수 있다; 도시된 바와 같이 인증서들은, 예컨대, eUICC 유지 보수를 위한 공장 재정비 서버들, 및 eUICC PCF에 서명하기 위한 활성화 서버들을 포함한다. 루트 CA는 eUICC CA의 일반 이름과 함께 클라이언트 eUICC에 의해 OEM 서명된 메시지들을 검증하는 데 이용된다.

[0076] 전술한 내용에 따라, 하나의 예시적인 실시예에서, 각 클라이언트 eUICC는 다음과 같은 보안 관련 데이터를 저장한다: (i) eUICC L1, L2, 및 L3 동작들을 위해 이용되는 eUICC 인증서(각 eUICC는 L1, L2, 및 L3 보안 관련 동작들 모두를 위해 이용되는 인증서를 저장한다); (ii) eUICC 인증서들과 연관되는 eUICC 개인 키; (iii) OEM들의 루트 인증서 및 OEM eUICC CA의 일반 이름을 포함하는 OEM 인증서들; (iv) 및 서버 어플라이언스들을 보증할 수 있는 제3자들의 루트 인증서들. 일부 변형례들에서, eUICC 내의 인증서들은 서명 CA가 위태롭게 되면 대체될 필요가 있을 수 있다; 예를 들어, eUICC CA 또는 서버 CA가 위태롭게 되면(예컨대, 개인 키가 위태롭게 되었거나/분실되었다면), 2가지 폐기 절차들이 아래에 설명된다.

[0077] 제1 예시적인 폐기 절차에 따르면, eUICC 인증서들을 발행하는 서명 CA가 위태롭게 되면, 감염된 eUICC에 저장된 eUICC 인증서는 대체되어야 한다. 구체적으로, 해당 eUICC에 대해 초기 인증서 요청이 생성되었을 때, 인증서 서명 요청(Certificate Signing Request, CSR)이 저장되었다. 서명 CA가 위태롭게 되면, 초기 CSR을 이용하여 해당 eUICC에 대해 새로운 인증서가 요청될 수 있다. 동일한 CSR을 유지함으로써, eUICC는 동일한 개인 키를 이용할 수 있고, 동일한 eUICC 공개 키를 포함하여 새로운 인증서가 발행될 것이다. OEM은 OEM의 개인 키로 새로운 인증서에 서명할 수 있다. eUICC가 서버 브로커에 요청들을 전송할 때, 브로커는 불량 eUICC CA들의 폐기 목록을 체크하고 인증서가 대체될 필요가 있음을 나타내는 특정 오류와 함께 요청을 거절할 수 있다. AP는 기존 OEM 서비스들을 통해 새로운 eUICC 인증서를 검색하고 새로운 인증서를 eUICC에 전송할 수 있다(AP는 이 시나리오에서 신뢰할 수 있는 것일 필요는 없다).

[0078] 그 후, eUICC는 OEM 서명을 검증하고 수신된 공개 키가 eUICC에 이전에 저장된 그의 공개 키와 일치할 것을 보장한다. 일부 변형례들에서, 서비스 거부(DOS) 공격들 또는 재전송 공격들(replay attacks)을 방지하기 위하여, eUICC는 eUICC 인증서들을 추가로 포함한다. 에포크(epoch)는 한 변형례에서 새로운 인증서가 발행될 때 증가된다. eUICC는, 새로운 인증서를 저장하기 전에, 수신된 인증서 내의 eUICC 에포크가 현재의 인증서의 에포크보다 높은 것을 확인할 수 있다.

[0079] 안타깝게도, eUICC에서 서버 인증서들을 폐기하는 것은 다양한 eUICC 리소스 제약으로 인해 힘들 수 있다; 즉, 큰 폐기 목록을 처리하는 것은 eUICC에 대해 성립하지 않는 것일 수 있다. 폐기 목록들을 유지하는 것을 방지하기 위해, 제2 폐기 방식에서는, 각 서버 인증서가 추가로 에포크와 연관된다. CA가 위태롭게 되면, 루트 CA는 모든 정당한 엔티티들을 위해 인증서들을 재발행하고, 각각의 새로운 인증서의 에포크를 증가시킨다. 서버 인증서들의 수는 많지 않을 것이므로, 인증서들을 재발행하는 것은 기존 시스템들에서 다루어질 수 있다. 클라이언트 eUICC에서, eUICC는 서버 L1, L2, 및 L3 인증서들의 예상되는 에포크를 비휘발성 메모리에 저장한다. 수신된 인증서가 더 높은 에포크를 포함하고 있을 때, eUICC는 대응하는 NV 에포크를 업데이트하고 더 낮은 에포크를 가진 임의의 향후의 인증서들을 거절해야 한다; 즉, eUICC는 CA가 위태롭게 된 이후 서명되지 않은 악성 서버들을 거절할 것이다. 일부 변형례들에서, 서버는 또한 위태롭게 된 eUICC들에 대한 eUICC 블랙리스트를 유

지할 수 있다. 블랙리스트에 오른 eUICC에 대한 요청들은 일 실시예에서 서버에 의해 거절된다.

[0080] 정책 제어 기능들

[0081] 전술한 보안 솔루션의 컨텍스트 안에서, 2개 레벨의 정책 제어 기능(Policy Control Functions, PCF)이 있다: (i) eUICC 플랫폼 레벨, 및 (ii) 프로파일 레벨. 하나의 예시적인 실시예에서, eUICC PCF는 OEM에 의해서만 업데이트될 수 있는 반면, 프로파일 PCF는 MNO들에 의해 제어되고 eSIM의 일부이다. 하나의 그러한 변형례에서, eSIM이 익스포트되고/되거나 임포트될 때, 프로파일 PCF는 익스포트/임포트 패키지의 일부로서 포함된다.

[0082] 이제 eUICC PCF를 언급하면, eUICC PCF는 다음과 같은 것들을 포함할 수 있다: (i) eUICC가 활성화할 수 있는 eSIM들의 타입들을 명시하는 SIM 잠금 정책; (ii) eUICC 내의 모든 eSIM들의 삭제를 인가하는 데 사용될 수 있는 비밀 코드; (iii) eUICC가 (예컨대, 비즈니스 고려 사항들 또는 방법들에 기초하여) 통신할 수 있는 서버 어플라이언스들의 클러스터를 명시하는 서버(L1, L2, 및 L3)의 일반 이름들의 목록(즉, 포괄적 목록); (iv) eUICC가 통신할 수 없는 서버 어플라이언스들의 클러스터를 명시하는 서버(L1, L2, 및 L3)의 일반 이름들의 목록(즉, 배타적 목록).

[0083] 유사하게, 프로파일 PCF는 다음과 같은 것들을 포함할 수 있다: (i) eUICC가 eSIM을 익스포트할 수 있는 데포들의 클러스터를 명시하는 서버들(L1, L2, 및 L3)의 일반 이름들의 목록(포괄적); (ii) eUICC가 eSIM을 익스포트할 수 없는 데포들의 클러스터를 명시하는 서버들(L1, L2, 및 L3)의 일반 이름들의 목록(배타적); (iii) 명시된 eSIM 동작의 완료 시에 통지들을 보낸 URL들을 명시하는 통지 URL들 및 동작 타입들; (iv) 프로파일이 만료되면 AP가 eSIM을 삭제할 수 있는 자동 만료 파라미터들; (v) 구현된 보안 레벨들을 나타내는 상이한 클래스들이 할당될 수 있는 서버 어플라이언스들(L1, L2, 및 L3)의 클래스들(프로파일은 소정의 레벨들보다 높은 서버 컴포넌트들과만 통신하기로 선택할 수 있다); (vi) 설치 중에 체크되는 서버 인증서들(L1, L2, 및 L3)의 에포크(예컨대, eUICC는 eUICC 서버 인증서들의 에포크가 명시된 에포크와 같거나 그보다 높은 경우에만 프로파일들을 설치한다); (vii) L3 인증이 사용할 수 있는 L3 서비스 이름들, 및/또는 L3 인증이 사용할 수 없는 서비스 이름들의 목록; (viii) eUICC 시스템의 최저 버전(명시된 최저 버전보다 높은 eUICC 시스템들에서만 eSIM이 설치될 수 있는 경우); (ix) eSIM을 위해 필요한 최소 RAM 사이즈(OTA 동작들은 포함하지 않음); (x) OTA를 위해 예약된 최소 RAM 사이즈; (xi) eSIM을 위해 필요한 최소 비휘발성(NM) 메모리 사이즈(OTA를 위해 서빙되는 공간은 제외함); (xii) OTA를 위해 예약된 최소 NM 사이즈.

[0084] 예시의 동작

[0085] 전술한 컴포넌트들(예컨대, eUICC, eSIM, 브로커 네트워크, 보안 프로토콜, 등)의 컨텍스트 안에서, 하기의 예시적인 메시징 시퀀스들이 개시된다. 이하의 시퀀스 다이어그램들에서는, 3개의 엔티티들이 제시된다: L3, L2, L1 보안들에 대해 각각 책임이 있는 엔티티들을 나타내는, 브로커, 프로파일 에이전트, 및 프로파일 로커. 그러나, 이들은 논리적 엔티티들이고 상이한 네트워크 토폴로지들은 전술한 그것의 기능들을 포함하거나 추가로 구별할 수 있다는 것이 인지된다.

[0086] 클라이언트 eUICC는 예시된 실시예에서 3개의 모든 보안 레벨들에 대한 책임이 있지만; 명확성을 위해, 클라이언트 eUICC는 eUICC 내의 기능적 요건들을 캡처하는 3개의 논리적 엔티티들로 분리된다. 더욱이, 클라이언트 eUICC 내에 L1, L2, 및 L3에 대한 별개의 인증서 세트들이 있을 수 있지만, 클라이언트 디바이스가 단일 디바이스이므로 동일한 것(즉, 하나의 인증서)이 사용될 수 있다는 것이 인지된다.

[0087] eSIM 전달, 개인화 없음

[0088] 도 9는 개인화 없이 eSIM을 디바이스에 전달하기 위한 하나의 예시적인 논리적 시퀀스를 보여준다. 먼저, 디바이스는 발견 프로세스(미도시)를 통해 서버 브로커를 식별한다. 디바이스가 서버 브로커와 통신하려고 시도하면, 다음과 같은 3개의 주요 동작이 있다: (i) 디바이스는 이용 가능한 eSIM 옵션들에 관하여 서버 백엔드에 문의한다; (ii) 디바이스는 요청된 eSIM이 사전 개인화되어 있지 않다면 서버가 eSIM을 개인화할 것을 요청한다; 그리고 (iii) 디바이스는 실제 eSIM을 다운로드하고 그것을 설치한다.

[0089] 제1 단계에서는, 이용 가능한 eSIM 옵션들에 관하여 서버 백엔드에 문의하기 위해 디바이스에 의해 getProfileOptions가 이용된다. 디바이스와 연관된 eUICC는, 예를 들어 카드 일련 번호일 수 있는, 그것의 UniqueId로 식별된다. 브로커는 판매 정보를 이용하여 디바이스가 이용할 수 있는 하나 이상의 eSIM 옵션을 결정한다. 잠겨 있지 않은 디바이스들의 경우, 이용 가능한 eSMI들의 세트가 매우 클 수 있다; 따라서, 일부 실시예들에서, 사용자에 의해 선택될 가능성이 있는 공통 옵션들이 표시된다(예컨대, 장소, 비용 등에 기초하여). 서버는 디바이스에 대해 유효한 프로파일 제공자들(MNO) 및 프로파일 타입들(예컨대, 선불/후불)의 어레이를 반

환한다.

[0090] 일부 시나리오들에서, 사용자가 이용할 수 있는 eSIM들의 타입은 개인 정보로 간주될 수 있으므로, 일부 변형례들에서 getProfileOptions API는 디바이스 eUICC L3에게 eUICC의 고유 식별자에 서명할 것을 추가로 요구하고, 서명된 식별자를 API에 포함시킨다. 서버 브로커(또는 브로커 서버)는 요청을 처리하기 전에 이 서명을 검증할 수 있다. 이는 악성 관계자가 가장된 요청들을 송신함으로써 사용자의 프로파일 옵션들을 검색하는 것을 막는다. 일부 변형례들에서, 디바이스 브로커와 서버 브로커 간의 통신은 캡처 및 재전송 공격들을 막기 위해 보안 프로토콜(예컨대, 전송 계층 보안(transport layer security, TLS))을 이용한다.

[0091] 일 실시예에서, getProfileOptions는 eSIM의 현재 그리고 새로운 소유권을 검증하기 위해 2개의 L3 토큰을 포함하고 있다. 현재 L3 토큰은 고유 식별자 또는 소위 "모조 카드(faux card)" 스크래치 코드일 수 있다. 새로운 L3 토큰은 예를 들어, iCloud 계정에 대한 사인-온 토큰과 같이 사용자 계정을 eSIM과 연관시키는 데 이용되는 정보일 수 있다(예컨대, 디바이스가 토큰을 검색하기 위해 사용자 계정에 로그인한 경우). 양쪽 L3 토큰들은 eUICC L3에 의해 서명된다. 서버 브로커는 연관된 인증 서비스를 이용하여 L3 토큰들의 유효성을 검사한다. 예를 들어, 그것은 사인-온 토큰의 유효성을 검사하기 위해 네트워크 서버(예컨대, 본 양수인의 iCloud 서버) 또는 제3자 서비스와 통신할 수 있다.

[0092] 성능을 최적화하고 복제 인증을 피하기 위해, 디바이스에 의해 전달된 토큰을 인증한 후에, 서버 브로커는 일회용 코드(one time code, OTC)를 생성하고 이 OTC를 다시 디바이스에 전달한다. 디바이스는 이 OTC를 서버가 이미 L3 인증을 수행했다는 증거로 이용할 수 있다. 완전한 데이터 BLOB(binary large object)는 생성된 OTC, 고유 디바이스 식별자(예컨대, 카드 일련 번호(CSN)), 프린서플(principal), 서비스 제공자, OTC의 유효성을 나타내는 타임스탬프를 포함할 수 있다. 이 BLOB는 브로커에 의해 해싱되고 서명된다. 하나의 변형례에서, 해싱은 전체적인 성능을 향상시키기 위해 대칭 키로 수행된다. getProfileOptions가 eSIM들의 어레이를 반환하면, 사용자는 선택을 하도록 요구받는다.

[0093] 제2 단계에서는, 디바이스는 eSIM을 개인화하도록 서버 백엔드에 요청하기 위해 personalizeProfile을 호출할 것이다. 디바이스가 서버에 개인화 요청을 보내기 전에, 인증을 위해 eUICC 프로파일 에이전트와 서버 프로파일 에이전트 간에 세션 핸드셰이크가 있다. 디바이스 브로커와 eUICC는, 사용자가 선택한 프로파일 옵션과, 서버 브로커에 의해 송신된 현재 L3 코드 및 새로운 L3 코드에 기초하여 세션을 생성한다. eUICC는 차후에 송신되는 프로파일 요청에 채우기 위해 이 정보를 저장할 수 있다. eUICC 프로파일 에이전트는 세션 id를 생성하고, 이것은 그 후의 인증을 위해 서버 에이전트에 의해 에코 백될 것이다.

[0094] 디바이스 브로커는 이제 eUICC에 의해 생성된 세션 요청을 서버 브로커에 전달할 수 있다. 서버 브로커는 요청을 체크할 수 있다. 예를 들어, 서버 브로커는 고유 ID가 나타내는 요청 eUICC가 서비스 가능한지를 판정한다. 고유 식별자는 평문으로 포함되므로, 서버 브로커는 비록 서버 프로파일 에이전트에 의해 요청의 더 철저한 검증이 수행된다 할지라도 그 정보를 검색할 수 있다.

[0095] 요청이 적절하다면, 서버 브로커는 그 요청을 프로파일 에이전트에 전달한다. 프로파일 에이전트는 eUICC L2 인증서를 검증하고 eUICC L2 공개 키를 이용하여 L2 서명을 검증함으로써 요청을 암호로 검증한다. 검증이 통과하면, 서버 프로파일 에이전트는 수신된 세션 식별자와 고유 식별자를 포함하고 있는 평문 섹션, (상기 평문 섹션을 해싱하고 그 해시에 서버 프로파일 에이전트의 개인 키를 이용하여 서명함으로써 생성된) L2 서명, 및 서버 프로파일 에이전트의 인증서를 포함하는 SessionResponse를 생성한다.

[0096] 이 세션 응답은 서버 프로파일 에이전트로부터 서버 브로커로 송신되고, 서버 브로커는 그 후 이 세션 응답을 디바이스 브로커에 전송한다. 디바이스 브로커는 이 응답을 prepareProfileRequest 메시지에서 eUICC에 전달한다. eUICC L2는 서버 프로파일 에이전트의 인증서와 L2 서명을 검증함으로써 이 sessionResponse를 검증한다. eUICC L2는 또한 세션 식별자와 고유 식별자가 eUICC 내의 정보와 일치하는 것을 검증한다. 검증이 통과하면, eUICC는 개인화된 프로파일 요청에 대한 챌린지를 생성한다. 이 챌린지는 비휘발성 메모리에 커밋(commit)된다. 그 후 eUICC는 L1, L2 및 L3 관련 정보를 포함하여 프로파일 요청 BLOB를 생성한다. 상세 구조들은 본 명세서에 참고로 포함된 부록(APPENDIX) A에 열거되어 있다.

[0097] 그 후, 프로파일 요청 BLOB는 서버 백엔드에 송신된다. 서버 브로커는 L3 검증을 수행하고 eSIM을 연관시킬 L3 오너 정보(예컨대, 프린서플 및 서비스 제공자)를 포함시키고; 서버 프로파일 에이전트는 배치 디스크립터를 생성하고, 서버 프로파일 로커는 eUICC에 대한 eSIM을 개인화한다. 개인화된 eSIM은 성능 최적화를 위해 콘텐츠 전달 네트워크(content delivery network, CDN)에 배포될 수 있다.

[0098] 디바이스 브로커가 프로파일 디스크립터 및 연관된 L3 오너 정보를 수신한 후, 그것은 수신된 GUID(Globally Unique Identifier)를 제공함으로써 getProfile을 통해 연관된 프로파일을 검색한다.

[0099] 디바이스 브로커가 프로파일 디스크립터 및 프로파일을 검색하면, 그것은 클라이언트 eUICC에게 eSIM을 설치하도록 지시한다. 호 흐름들은 3개의 별개의 호, processL3Owner, processProfileDescriptor 및 installProfile을 보여주지만, 실제 구현예에서는, 이들 3개의 논리적 호들이 단일 트랜잭션 내에서 결합될 수 있다는 것이 인지된다. eUICC는 L3, L2, 및 L1 검증을 수행하고; 일단 검증되면, eSIM은 설치된다. 연관된 챌린지는 삭제된다. L3 오너 정보는 정당한 소유권을 나타내기 위해 eSIM과 함께 저장된다. L3 오너 정보는 사용자가 eSIM을 익스포트하면 나중 시점에 제공될 수 있다.

[0100] 프로파일이 설치되면, eUICC는 설치 결과들을 서버에 반환한다. 서버 인프라는 그 통지를 이용하여 콘텐츠 전달 네트워크(CDN) 내의 캐싱된 콘텐츠의 퍼지를 트리거할 수 있다. 일부 경우에, 이 정보는, 예컨대, 성공적인 설치, 부분 설치, 성공하지 못한 설치 등을 나타내는 통지 서비스들에 이용될 수도 있다.

[0101] eSIM 전달, 사전 개인화

[0102] 도 10은 사전 개인화와 함께 eSIM을 디바이스에 전달하기 위한 하나의 예시적인 논리적 시퀀스를 보여준다. 도 9의 방식과 유사하게, 사전 개인화된 eSIM을 전달하는 데는 3개의 단계가 필요하다.

[0103] 처음에, 클라이언트 디바이스의 제조 중에, 공장 브로커가 eUICC에게 eSIM 사전 개인화에 대한 챌린지를 나중에 생성하도록 지시한다. 그러나, 도 9의 방식과 다르게, 디바이스는 아직 MNO, 또는 eSIM 타입과 연관되어 있지 않고; 오히려 이 필드들은 선택이 나중에 이루어질 것임을 나타내는 특수 값으로 채워져 있다. 프로파일 요청 BLOB의 완전한 콘텐츠는 나중에 개인화 사용을 위해 저장된다.

[0104] 제2 단계는, 예컨대, 발송 통지, 디바이스 판매 등에 의해 자동으로 트리거된다. 배포 센터 내의 L2(클라이언트 프로파일 에이전트)는 클라이언트 eUICC L2에 대한 프록시로서의 역할을 한다. eUICC 프로파일 요청 BLOB는 MNO 및 eSIM 타입을 포함하고 있지 않지만, 클라이언트 프로파일 에이전트는 이 필드들을 업데이트된 정보로 대체함으로써 BLOB를 재생성할 수 있다. 클라이언트 프로파일 에이전트는 그 자신의 챌린지들을 생성하고 eUICC 챌린지를 대체할 수 있다. 클라이언트 프로파일 에이전트는 그 자신의 개인 키로 콘텐츠에 서명할 것이다(그렇지 않으면 모든 L2들이 고유 챌린지들을 요구할 것이다). BLOB는 eUICC의 L1 서명을 포함할 것이고, eUICC는 여전히 개인화된 eSIM을 복호화할 필요가 있다. 새로운 프로파일 요청 BLOB는 기존 personalizeProfile 요청을 이용하여 서버 브로커에 송신된다. 이하, 절차는 도 9의 절차와 다르지 않다.

[0105] 더욱이, MNO가 그 자신의 브로커링 시스템을 지원하고 싶다 할지라도, 개시된 사전 개인화 프로세스는 동일한 인터페이스를 이용할 수 있다는 것도 인지된다. 서버 브로커는 배치 디스크립터를 클라이언트에 반환하고 eSIM을 개인화할 것이다. 클라이언트 프로파일 에이전트는 eUICC가 나중에 프로파일을 요청할 때 이용되도록 eUICC의 챌린지와 함께 새로운 배치 디스크립터를 생성할 것이다.

[0106] 마지막으로, 최종 단계에서는, 사용자가 디바이스의 전원을 켤 때, 디바이스는 이용 가능한 eSIM 옵션들을 체크하기 위해 getProfileOptions를 수행한다. eSIM이 이미 사전 개인화되어 있으므로, 응답은 유효한 배치 디스크립터를 포함할 것이고 디바이스는 더 이상 personalizeProfile을 호출할 필요가 없다. 그것은 디스크립터 내의 정보를 이용하여 getProfile 요청을 통해 eSIM을 바로 검색할 것이다.

[0107] eSIM 전달, 배치 전달

[0108] 도 11은 예컨대, 2개의 엔티티들 간에 다수(배치)의 eSIM들을 전달하기 위한 하나의 예시적인 논리적 시퀀스를 보여준다. 일 실시예에서, 클라이언트 브로커와 서버 브로커는, 예컨대, 가상 사설 네트워크(Virtual Private Network, VPN)를 통해 보안 통신을 갖는 안전한 엔티티들이다. 클라이언트가 다량의 eSIM들을 주문할 수 있도록 "배칭(batching)"이 지원된다.

[0109] 이 시나리오에서는, 프로파일 에이전트가 프로파일들을 개인화하라는 요청을 수신할 때, 배치 디스크립터가 반환되면 프로파일들은 개인화될 필요가 없다; 오히려, 클라이언트는 원하는 대로 나중 단계에서 실제 프로파일들을 요청할 수 있다. 배치 디스크립터 동작에서, 프로파일 콘텐츠의 해시는 (대칭 키로 래핑된) 암호화된 프로파일과 프로파일 메타데이터 - 이들 중 어느 것도 프로파일이 개인화되는 것을 요구하지 않음 - 에 대해 계산된다. 이것은 또한 L1에게 eUICC마다 대칭 키를 저장할 것을 요구하지 않는데, 그렇지 않다면 충족시키기 어려운 추가의 저장 요건으로 L1에 부담이 될 것이다. 일 실시예에서, (대칭 키로 래핑된) 암호화된 eSIM은 오프-저장소(off-storage)에 저장될 수 있다. 대칭 키는 L1 RFS(remote file system) 키로 래핑될 것이고 래핑된 키는

암호화된 eSIM과 함께 오프-저장소에 저장될 수 있다.

[0110] eSIM 익스포트

[0111] 마지막으로, eSIM이 클라이언트 디바이스에 저장되면, 사용자는 디바이스 밖으로 eSIM을 익스포트하고 나중에 동일한 또는 상이한 디바이스로 eSIM을 임포트하기로 선택할 수 있다. 하나의 목적은 eSIM 스왑을 지원하는 것이다. 다른 목적은 추가 eSIM들을 저장하기 위해 eUICC 메모리를 풀어주는 것이다. 익스포트할 때, 다음과 같은 3가지 가능한 시나리오가 있다: (i) 클라우드에 익스포트하는 것, (ii) (오프-보드 저장을 위해) AP에 익스포트하는 것, 및 (iii) 디바이스 간 eSIM 이송. 유사하게, 사용자는 클라우드, AP, 또는 다른 디바이스로부터 임포트할 수 있다.

[0112] eSIM 설치 중에, 사용자 계정 정보가 eSIM과 연관된다(사용자가 동의하지 않기로 하지 않는 한). 계정 정보는 L3 인증을 위한 충분한 정보를 포함한다. 예를 들어, 그것은 프린서플(예컨대, x2z@yahoo.com) 및 인증을 위한 연관된 서비스 제공자를 포함할 수 있다. eSIM과 연관된 계정 정보가 없다면, 사용자는 다른 인증 방법들을 이용해 eSIM을 익스포트할 수 있다. 하나의 그러한 실시예는 디바이스의 물리적 소유를 입증하기 위해 eUICC에 안전하게 연결되어 있는 물리적 버튼을 포함한다. 또 다른 실시예에서, 각 eSIM은 고유 패스워드를 포함하고, 사용자는 자신의 소유권을 입증하기 위해 패스워드를 가져야 한다. OEM 인증서를 이용하는 것은 여전히 또 다른 옵션이다.

[0113] 사용자가 eSIM을 익스포트할 때, AP는 eUICC로부터 설치된 프로파일들의 목록을 검색한다; 각 프로파일마다, eUICC는 또한 연관된 프린서플 및 재전송 방지(anti-replay)를 위해 생성된 난스(nonce)를 반환한다. 사용자가 프로파일을 익스포트하기로 선택할 때, AP는 프린서플에 포함된 정보를 이용하여 서비스 제공자로부터 통합 인증(single sign-on, SSO) 토큰을 획득하고, 여기서 사용자는 그 목적으로 사용자 명과 패스워드를 입력하도록 요구받을 것이다. SSO 토큰은 익스포트 요청에서 프린서플 및 난스와 함께 서버 브로커에 전달된다. 서버 브로커는 디바이스에 의해 공급된 SSO 토큰을 이용하여, 서비스 제공자와의 인증을 처리할 수 있다. 인증이 통과하면, 흐름은 클라이언트와 서버 역할이 뒤바뀐 것을 제외하고 디바이스로의 eSIM 전달을 미러링한다. 하이 레벨에서, 서버 브로커는 eUICC와의 세션을 개시하고, 익스포트에 대한 요청 BLOB를 생성한다. 요청에서, 그것은 동작이 L3 인증을 통과한 것을 나타내기 위해, eUICC가 생성한 난스를 포함시킨다. eUICC는 요청 BLOB를 검증하고, 서버 에이전트의 공개 키로 eSIM을 암호화하고, 배치 디스크립터와 eSIM에 대한 L3 오너 정보를 생성한다. eSIM은 L3 및 L2 정보와 함께 서버에 송신될 수 있다.

[0114] eUICC가 익스포트를 위해 eSIM을 암호화하면, eUICC는 eSIM의 소유권을 포기하고 더 이상 eSIM을 사용하거나 eSIM을 임의의 다른 엔티티들에 익스포트하지 않는다. 일부 경우에, eUICC는 접속 손실로부터의 회복을 돕기 위해 암호화된 사본을 저장할 수 있다(즉, 암호화된 eSIM이 서버에 결코 도달하지 않았다면). 대안으로, AP는 접속 실패의 경우에 재송신을 위해 암호화된 eSIM의 사본을 저장할 수 있다. 서버들은 확인 응답(acknowledgements)을 반환할 수 있고 이는 AP가 저장된 사본을 정리(clean up)하도록 트리거한다.

[0115] 일부 실시예들에서, 익스포트는 웹 포털로부터 개시될 수도 있다. 사용자가 그의 디바이스를 분실하면, 그는 그의 디바이스로부터 eSIM들을 익스포트하기 위해 웹 포털을 이용할 수 있다. 이 경우, 웹 포털은 익스포트 동작을 개시하기 위해 디바이스와 통신할 것이다. 흐름은 사용자가 소유권 검증을 위한 SSO 토큰을 얻기 위해 AP 대신에 웹 포털을 이용할 것이라는 점을 제외하고는 유사하다.

[0116] 장치

[0117] 위에 기술한 방법들과 함께 유용한 다양한 장치들이 이제 더 상세히 설명된다.

[0118] eUICC 어플라이언스

[0119] 도 12는 본 개시 내용에 따른 eUICC 어플라이언스(1200)의 하나의 예시적인 실시예를 보여준다. eUICC 어플라이언스는 독립형 엔티티를 포함하거나, 예컨대, 서버들과 같은 다른 네트워크 엔티티들과 통합될 수 있다. 도시된 바와 같이, eUICC 어플라이언스(1200)는 일반적으로 통신 네트워크와 인터페이스하기 위한 네트워크 인터페이스(1202), 프로세서(1204), 및 하나 이상의 저장 장치(1206)를 포함한다. 네트워크 인터페이스는 다른 eUICC 어플라이언스들로의 접근, 및 하나 이상의 모바일 디바이스들로의 직접 또는 간접 접근을 제공하기 위해, MNO 인프라에 연결되는 것으로 도시되어 있지만, 다른 구성들 및 기능들이 대체될 수 있다.

[0120] 하나의 구성에서, eUICC 어플라이언스는 (i) 또 다른 eUICC(eUICC 어플라이언스 또는 클라이언트 디바이스)와의 통신을 설정하는 것, (ii) eSIM을 안전하게 저장하는 것, (iii) 안전하게 저장된 eSIM을 검색하는 것, (iv) 또

다른 특정 eUICC로의 전달을 위해 eSIM을 암호화하는 것, 및 (v) eSIM 데포로/로부터 다수의 eSIM들을 송신하는 것을 할 수 있다.

[0121] eSIM 데포

[0122] 도 13은 본 개시 내용에 따른 eSIM 데포(1300)의 하나의 예시적인 실시예를 보여준다. eSIM 데포(1300)는 독립형 엔티티로서 구현되거나, 다른 네트워크 엔티티들(예컨대, eUICC 어플라이언스(1200) 등)과 통합될 수 있다. 도시된 바와 같이, eSIM 데포(1300)는 일반적으로 통신 네트워크와 인터페이스하기 위한 네트워크 인터페이스(1302), 프로세서(1304), 및 저장 장치(1306)를 포함한다.

[0123] 도 1300의 도시된 실시예에서, eSIM 데포(304)는 (i) (예컨대, 연관된 메타데이터를 통해) eSIM들의 재고 관리, (ii) (예컨대, 다른 eSIM 데포들, 및/또는 eUICC 어플라이언스들(1200)로부터) 암호화된 eSIM들에 대한 요청들에 응답하는 것, (iii) eSIM들에 대한 가입자 요청들을 관리하는 것을 할 수 있다.

[0124] 예를 들어, eSIM이 사용자에 의해 eSIM 데포(1300)에 저장될 때, eSIM은 의도된 목적지와 함께 저장되거나(예컨대, 다른 디바이스로의 이송을 용이하게 하기 위해), 불명확하게 파킹될 수 있다. 어떤 경우든, eSIM 데포는 안전한 저장을 위해 그리고 목적지 디바이스에 대한 후속의 암호화를 위해 eSIM을 eUICC 어플라이언스에 제공할 수 있다.

[0125] 사용자 장치

[0126] 이제 도 14를 참조하면, 본 개시 내용의 다양한 태양들에 따른 예시적인 사용자 장치(1400)가 도시되어 있다.

[0127] 도 14의 예시적인 UE 장치는 디지털 신호 처리기, 마이크로프로세서, 필드-프로그래머블 게이트 어레이, 또는 하나 이상의 기판에 탑재된 복수의 처리 컴포넌트들과 같은 프로세서 서브시스템(1402)을 갖춘 무선 디바이스이다. 프로세싱 서브시스템은 또한 내장 캐시 메모리를 포함할 수 있다. 프로세싱 서브시스템은, 예를 들어, SRAM, 플래시, 및/또는 SDRAM 컴포넌트들을 포함할 수 있는 메모리를 포함하는 메모리 서브시스템(1404)과 통신한다. 메모리 서브시스템은 당업계에 잘 알려져 있는 바와 같이 데이터 액세스들을 용이하게 하기 위해, 하나 이상의 DMA 타입 하드웨어를 구현할 수 있다. 메모리 서브시스템은 프로세서 서브시스템에 의해 실행가능한 컴퓨터 실행가능 명령어들을 포함한다.

[0128] 하나의 예시적인 실시예에서, 이 디바이스는 하나 이상의 무선 네트워크에 연결되도록 구성된 하나 이상의 무선 인터페이스(1406)를 포함한다. 다수의 무선 인터페이스들은 무선 기술 분야에 잘 알려진 타입의 적절한 안테나 및 모뎀 서브시스템들을 구현함으로써 GSM, CDMA, UMTS, LTE/LTE-A, WiMAX, WLAN, Bluetooth 등과 같은 다양한 무선 기술들을 지원할 수 있다.

[0129] 사용자 인터페이스 서브시스템(1408)은 키패드, 터치 스크린(예컨대, 멀티-터치 인터페이스), LCD 디스플레이, 백라이트, 스피커, 및/또는 마이크를 포함하는(이들에 제한되지는 않음) 임의의 수의 잘 알려진 I/O를 포함한다. 그러나, 소정의 응용들에서는, 이러한 컴포넌트들 중 하나 이상이 제거될 수도 있다는 것이 인지된다. 예를 들어, PCMCIA 카드-타입 클라이언트 실시예들은 사용자 인터페이스가 없을 수 있다(그것들은 그것들이 물리적으로 및/또는 전기적으로 연결되어 있는 호스트 장치의 사용자 인터페이스에 편승할 수 있으므로).

[0130] 도시된 실시예에서, 디바이스는 eUICC 애플리케이션을 포함하고 운용하는 보안 요소(1410)를 포함한다. eUICC는 네트워크 오퍼레이터와의 인증을 위해 사용될 복수의 액세스 제어 클라이언트들을 저장하고 이들에 액세스하는 것을 할 수 있다. 보안 요소는 보안 매체에 저장된 소프트웨어를 실행하는 보안 프로세서를 포함한다. 보안 매체는 (보안 프로세서 이외에) 모든 다른 컴포넌트들이 액세스할 수 없는 것이다. 더욱이, 예시적인 보안 요소는 전술한 바와 같이 부당 변경(tampering)을 막기 위해 추가로 강화될 수 있다(예컨대, 수지로 둘러싸일 수 있다). 예시적인 보안 요소(1410)는 하나 이상의 액세스 제어 클라이언트를 수신하고 저장하는 것을 할 수 있다. 일 실시예에서, 보안 요소는 사용자와 연관되어(예컨대, 하나는 업무 용도, 하나는 개인 용도, 몇몇은 로밍 액세스 용도 등), 및/또는 또 다른 논리적 방식 또는 관계에 따라(예컨대, 하나는 가족 또는 기업체의 다수의 구성원들 각각을 위한 것, 하나는 가족의 구성원들에 대한 개인 및 업무 용도 각각을 위한 것, 기타 등등) 어레이 또는 복수의 eSIM들을 저장한다. 각 eSIM은 컴퓨터 판독가능 명령어들(eSIM 프로그램), 및 연관된 데이터(예컨대, 암호 키, 무결성 키, 등)를 포함하는 소규모 파일 시스템을 포함한다.

[0131] 보안 요소는 모바일 디바이스로 및/또는 모바일 디바이스로부터의 eSIM들의 이송을 가능하게 하도록 추가로 구성되어 있다. 하나의 구현예에서, 모바일 디바이스는 eSIM의 이송을 개시하기 위한 GUI 기반 확인 응답을 제공한다.

[0132] 모바일 디바이스의 사용자가 eSIM을 활성화하기로 선택하면, 모바일 디바이스는 활성화 장치에 활성화를 위한 요청을 송신한다. 모바일 디바이스는 표준 인증 및 키 합의(Authentication and Key Agreement, AKA) 교환들을 위해 eSIM을 이용할 수 있다.

[0133] 방법들

[0134] 전술한 방법들과 함께 유용한 다양한 방법들이 이제 더 상세히 설명된다.

[0135] 도 15는 전자 액세스 제어 클라이언트들의 대규모 배포를 위한 방법의 일 실시예를 보여준다.

[0136] 단계 1502에서, 제1 디바이스가 하나 이상의 전자 액세스 제어 클라이언트들의 소유권을 확립한다.

[0137] 단계 1504에서, 제1 디바이스가 하나 이상의 전자 액세스 제어 클라이언트들이 이전에 복제되지 않았는지를 판정한다.

[0138] 단계 1506에서, 제1 디바이스가 제2 디바이스로의 이송을 위해 하나 이상의 전자 액세스 제어 클라이언트들을 암호화한다.

[0139] 단계 1508에서, 제1 디바이스와 제2 디바이스가 암호화된 하나 이상의 전자 액세스 제어 클라이언트들을 교환하거나 이송한다.

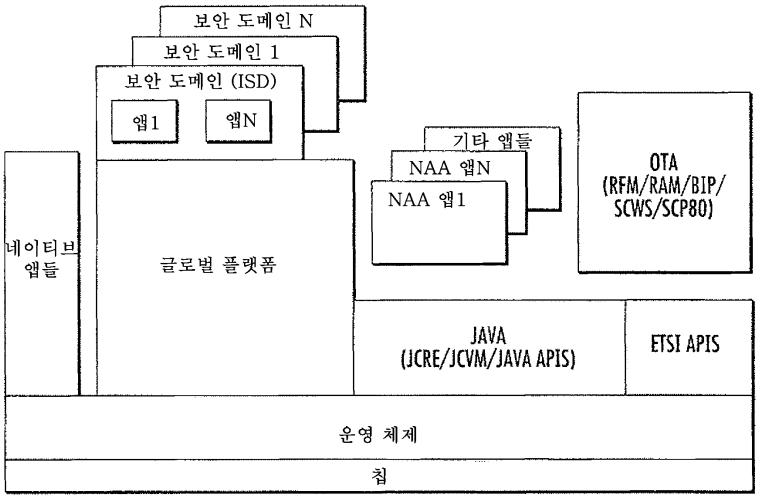
[0140] 본 개시 내용을 고려하여 당업자들에 의해 전자 액세스 제어 클라이언트들의 대규모 배포를 위한 무수히 많은 방식들이 인지될 것이다.

[0141] 본 개시 내용의 소정의 태양들이 방법의 특정 시퀀스의 단계들의 면에서 설명되어 있지만, 이러한 설명들은 본 개시 내용의 더 광범위한 방법들을 예시하는 것일 뿐이고, 특정 응용에 의해 필요에 따라 수정될 수 있다는 것을 인지할 것이다. 소정의 단계들이 소정의 상황에서는 불필요하거나 선택 사항이 될 수 있다. 게다가, 소정의 단계들 또는 기능이 개시된 실시예들에 추가되거나, 둘 이상의 단계들의 수행 순서가 바뀔 수 있다. 모든 그러한 변형례들은 본 명세서에 개시되고 청구된 개시 내용 안에 포함되는 것으로 간주된다.

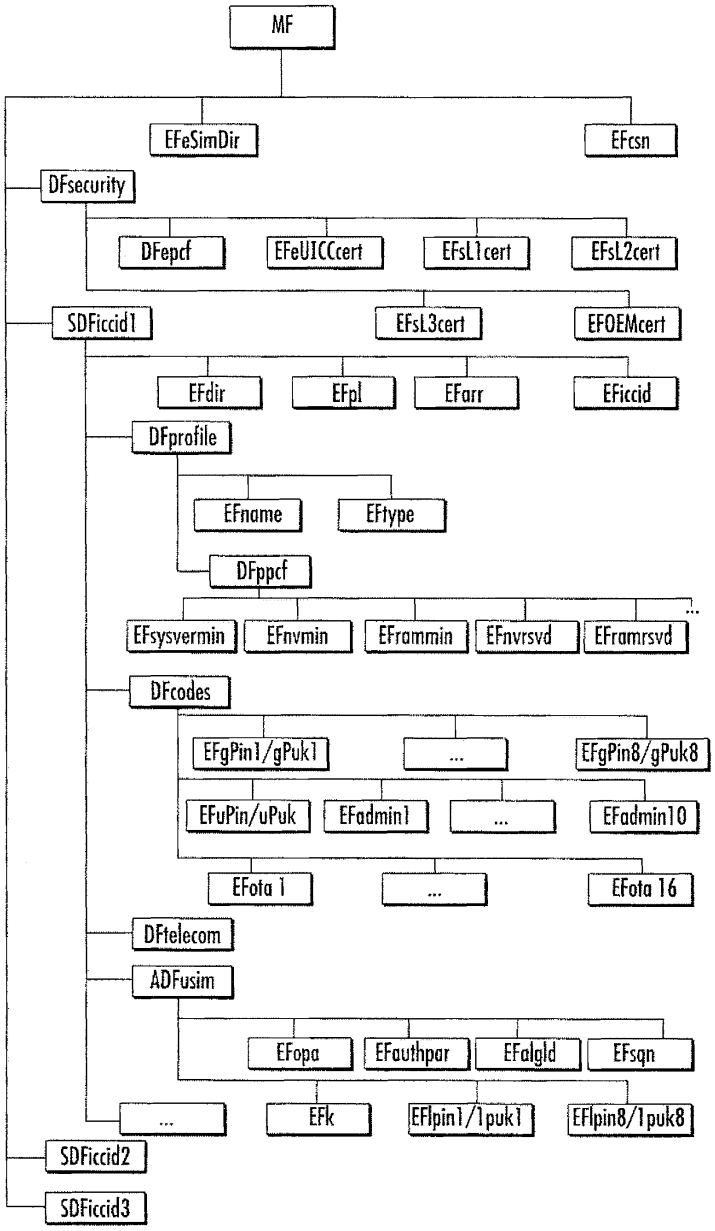
[0142] 상기 상세한 설명은 다양한 실시예들에 적용되는 바와 같은 본 개시 내용의 신규한 특징들을 보여주고, 설명하고, 지적하였지만, 예시된 디바이스 또는 프로세스의 형태 및 세부 사항의 다양한 생략, 대체, 또는 변경이 본 개시 내용에서 벗어나지 않고 당업자들에 의해 이루어질 수 있다는 것이 이해될 것이다. 전술한 설명은 본 개시 내용을 수행하는 현재 고려되는 최적의 방식이다. 이 설명은 결코 제한적인 것이 아니며, 오히려 본 개시 내용의 일반 원리들을 예시하는 것으로 간주되어야 한다. 본 개시 내용의 범주는 특허청구범위를 참고하여 결정되어야 한다.

도면

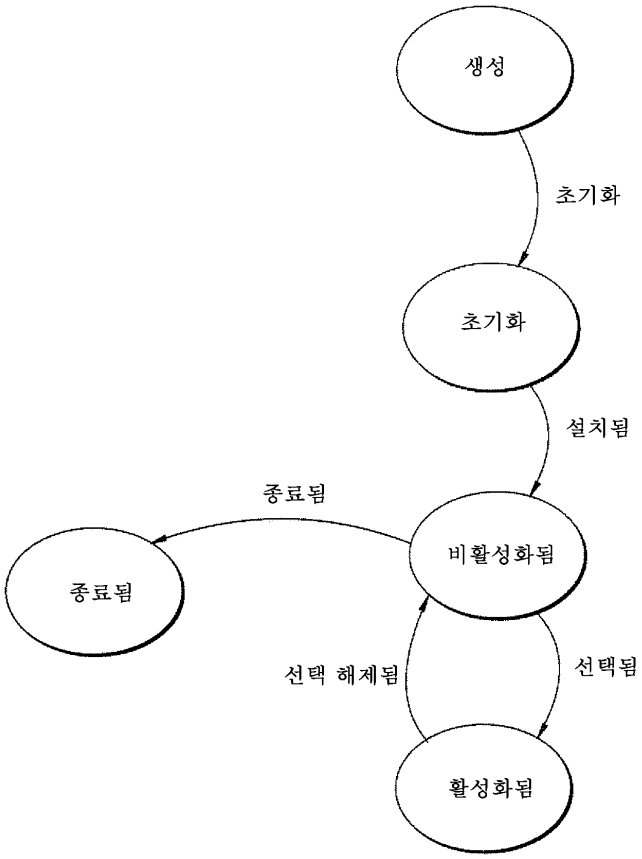
도면1



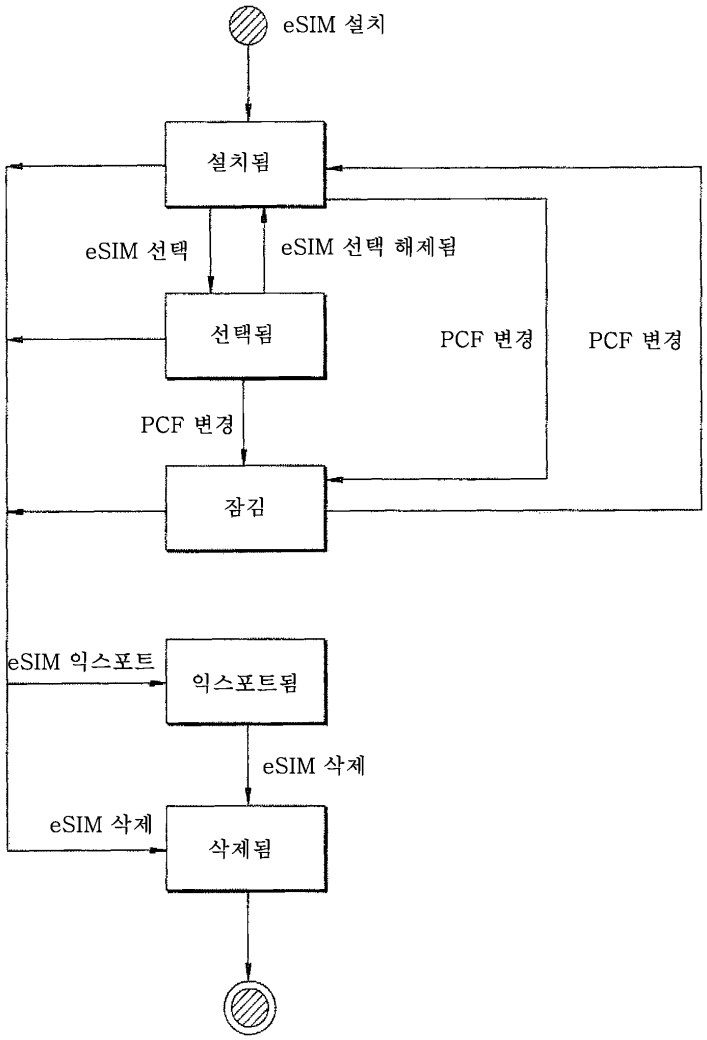
도면2


MF
EFeSimDir
EFcsn
DFsecurity
DFepcf
EFeUICCcert
EFsL1cert
EFsL2cert
SDFiccid1
EFsL3cert
EFOEMcert
EFdir
EFpl
EFarr
EFiccid
DFprofile
EFname
EFtype
DFppcf
EFsysvermin
EFnvmin
EFrammin
EFnvrsvd
EFramrsvd
DFcodes
EFgPin1/gPuk1
EFgPin8/gPuk8
EFuPin/uPuk
EFadmin1
EFadmin10
EFota 1
EFota 16
DFtelecom
ADFusim
EFopa
EFauthpar
EFalgId
EFsqn
EFk
EFlpin1/1puk1
EFlpin8/1puk8
SDFiccid2
SDFiccid3

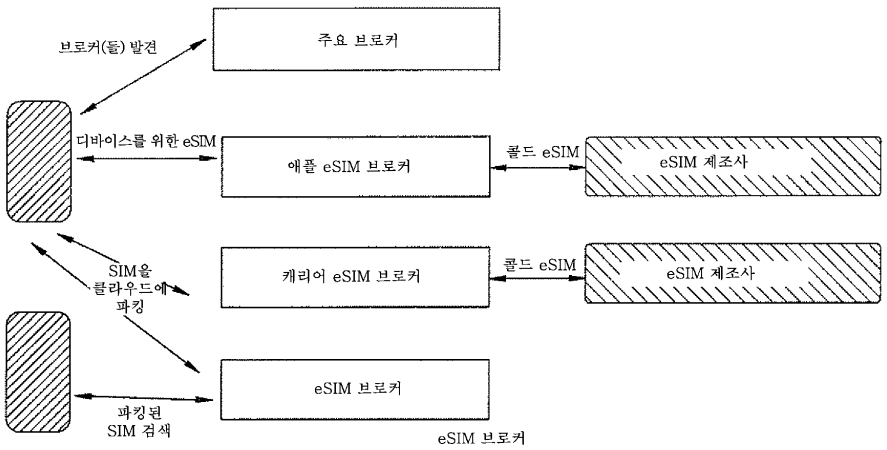
도면3



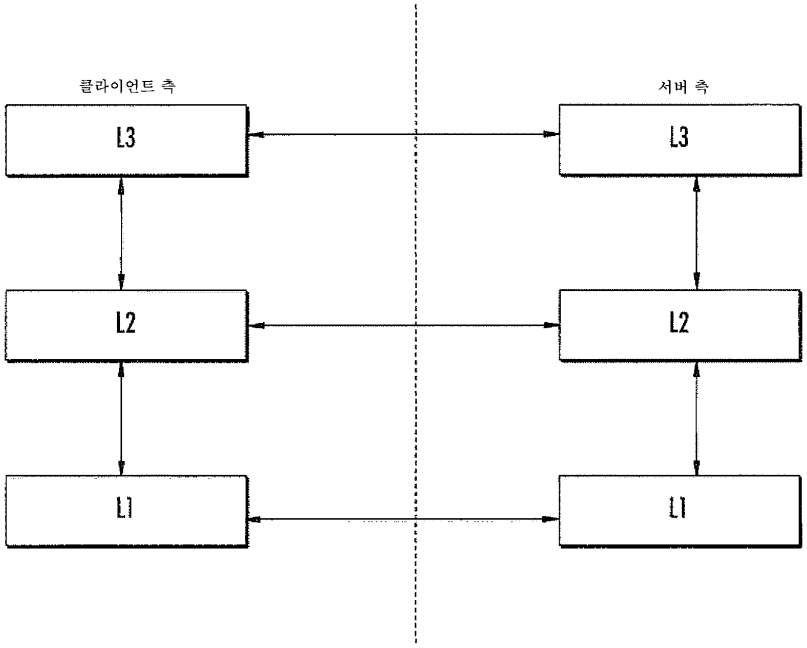
도면4


eSIM 설치
설치됨
eSIM 선택
eSIM 선택 해제됨
선택됨
PCF 변경
PCF 변경
PCF 변경
잠김
eSIM 익스포트
익스포트됨
eSIM 삭제
eSIM 삭제
삭제됨

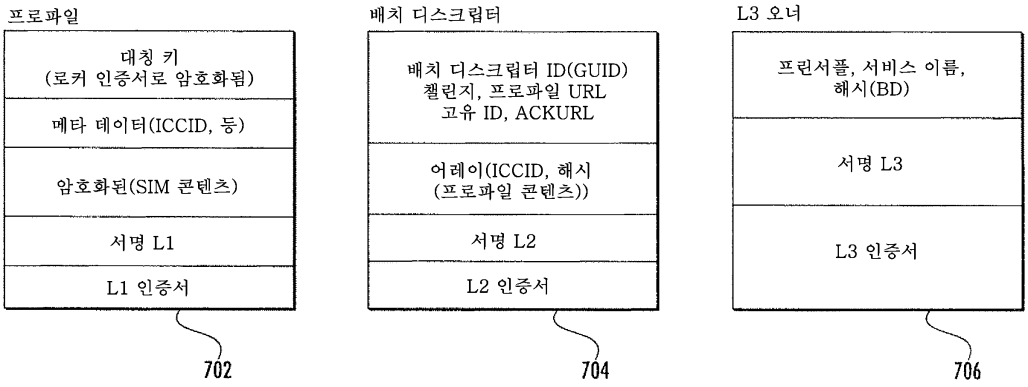
도면5


브로커(들) 발견
주요 브로커
디바이스를 위한 eSIM
애플 eSIM 브로커
콜드 eSIM
eSIM 제조사
SIM을
클라우드에
파킹
캐리어 eSIM 브로커
콜드 eSIM
eSIM 제조사
eSIM 브로커
파킹된
SIM 검색
eSIM 브로커

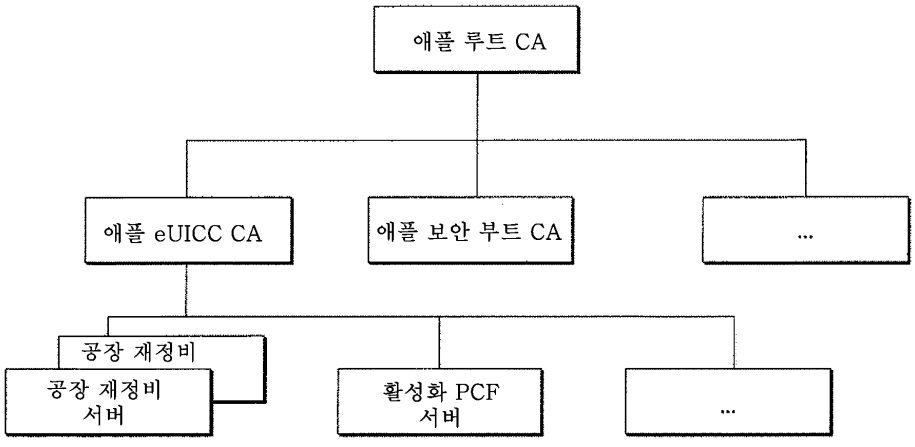
도면6


클라이언트 측
서버 측
L3
L3
L2
L2
L1
L1

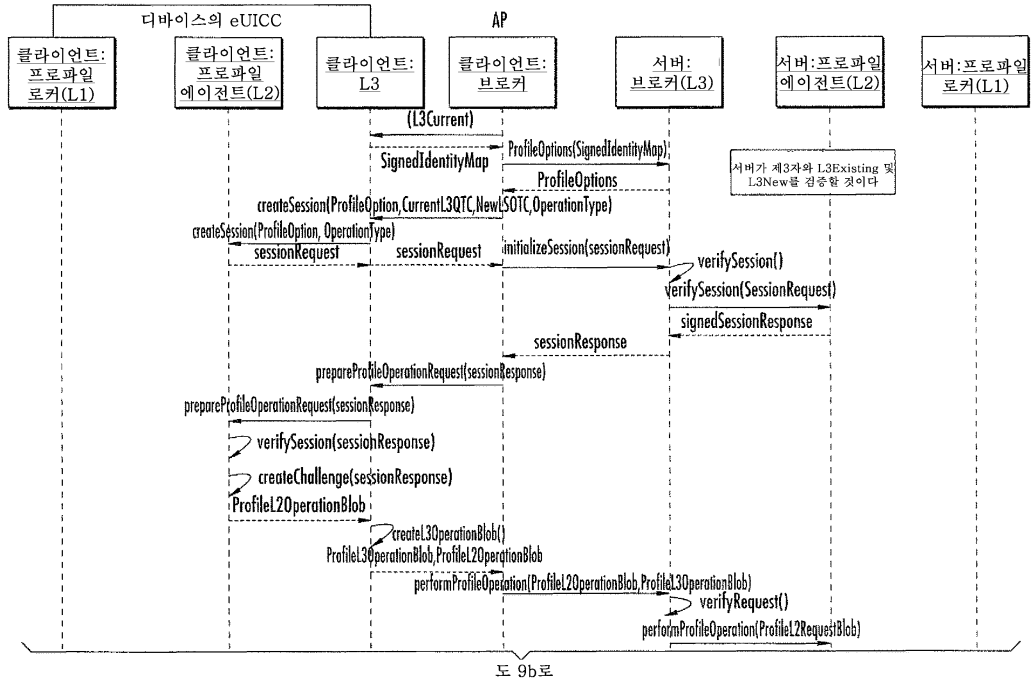
도면7


프로파일
대칭 키
(로커 인증서로 암호화됨)
메타 데이터(ICCID, 등)
암호화된(SIM 콘텐츠)
서명 L1
L1 인증서
702
배치 디스크립터
배치 디스크립터 ID(GUID)
챌린지, 프로파일 URL
고유 ID, ACKURL
어레이(ICCID, 해시
(프로파일 콘텐츠))
서명 L2
L2 인증서
704
L3 오너
프린서플, 서비스 이름,
해시(BD)
서명 L3
L3 인증서
706

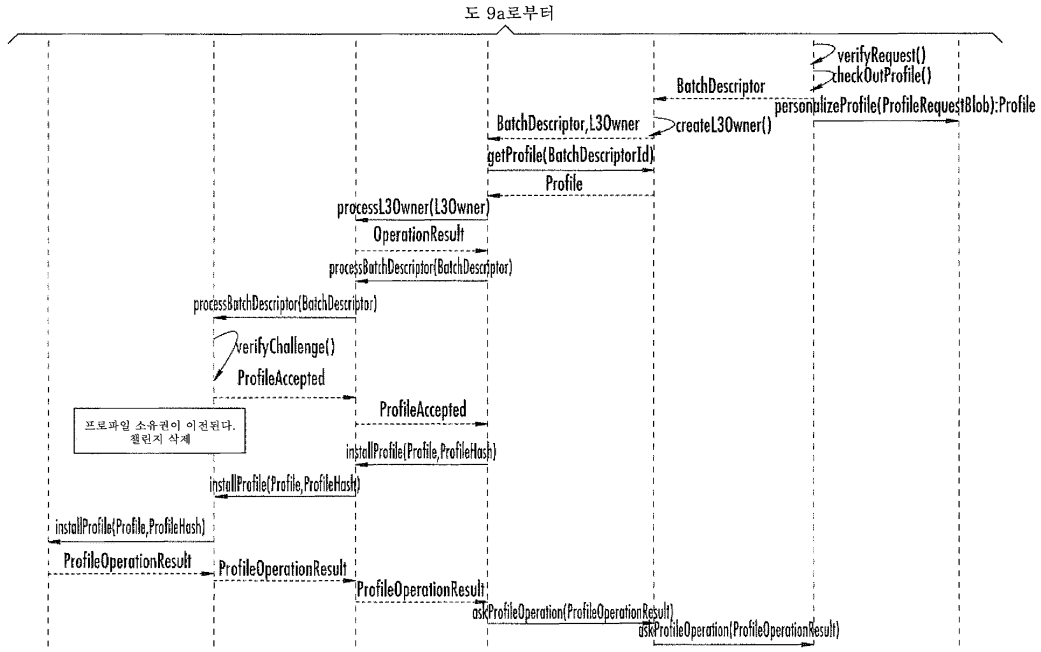
도면8


애플 루트 CA
애플 eUICC CA
애플 보안 부트 CA
...
공장 재정비
공장 재정비
서버
활성화 PCF
서버
...

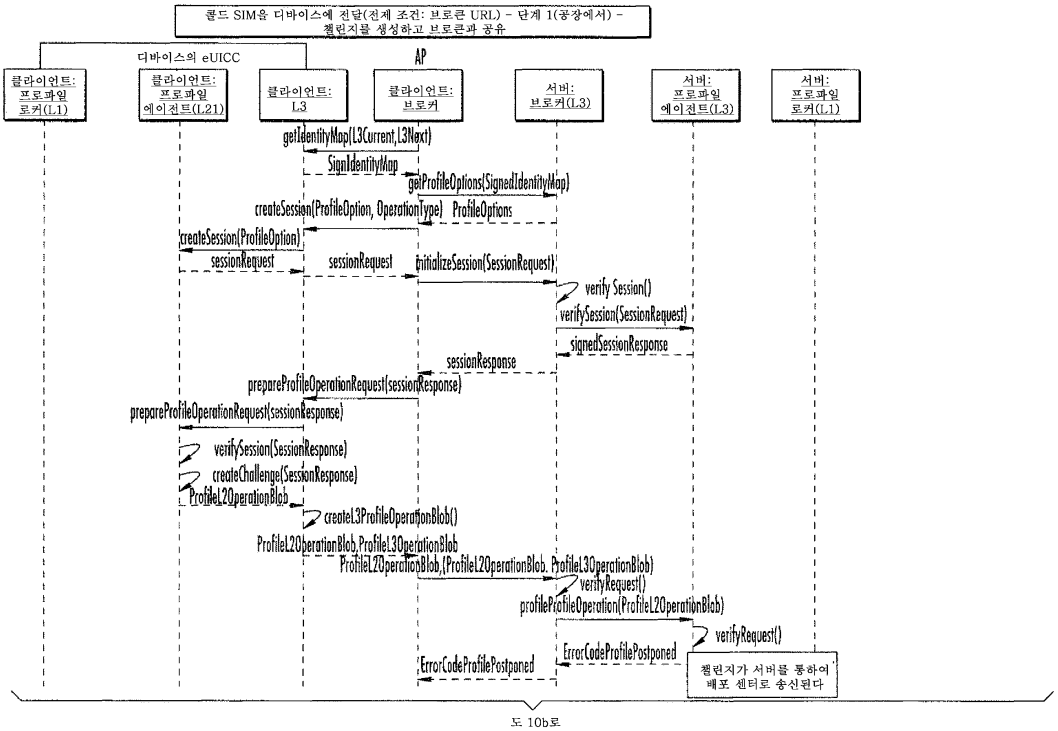
도면9a


디바이스의 eUICC
AP
클라이언트: 프로파일 로커(L1)
클라이언트: 프로파일 에이전트(L2)
클라이언트: L3
클라이언트: 브로커
서버: 브로커(L3)
서버:프로파일 에이전트(L2)
서버:프로파일 로커(L1)
(L3Current)
SignedIdentityMap
ProfileOptions(SignedIdentityMap)
ProfileOptions
서버가 제3자와 L3Existing 및 L3New를 검증할 것이다
createSession(ProfileOption,CurrentL3QTC,NewLSOTC,OperationType)
createSession(ProfileOption, OperationType)
sessionRequest
sessionRequest
initializeSession(sessionRequest)
verifySession()
verifySession(SessionRequest)
signedSessionResponse
sessionResponse
prepareProfileOperationRequest(sessionResponse)
prepareProfileOperationRequest(sessionResponse)
verifySession(sessionResponse)
createChallenge(sessionResponse)
ProfileL2OperationBlob
createL3OperationBlob()
ProfileL3OperationBlob,ProfileL2OperationBlob
performProfileOperation(ProfileL2OperationBlob,ProfileL3OperationBlob)
verifyRequest()
performProfileOperation(ProfileL2RequestBlob)
도 9b로

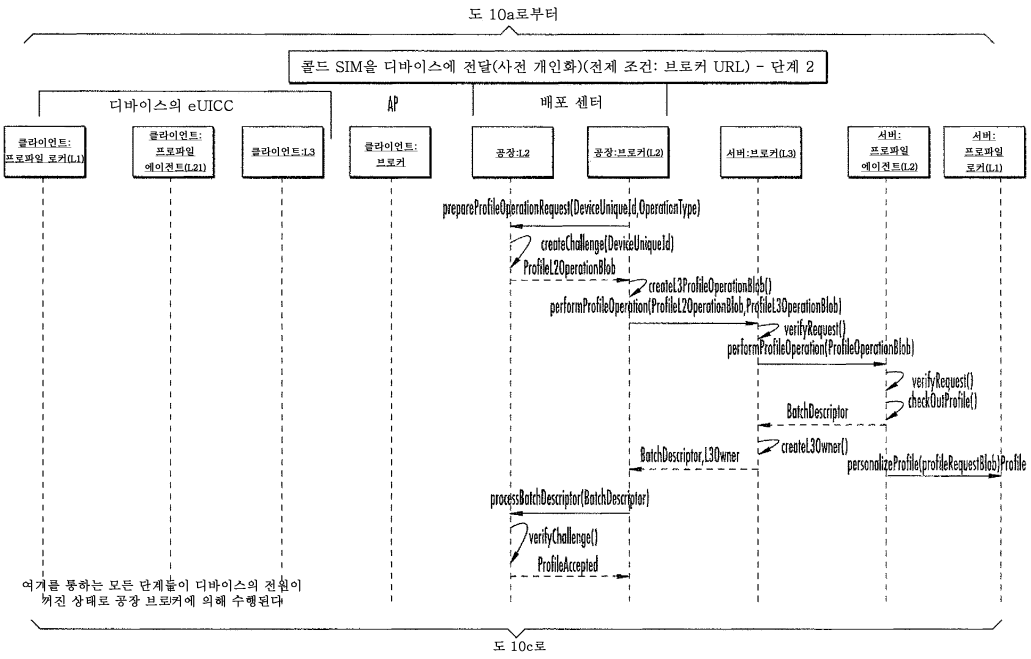
도면9b


도 9a로부터
verifyRequest()
checkOutProfile()
BatchDescriptor
personalizeProfile(ProfileRequestBlob):Profile
BatchDescriptor,L3Owner
createL3Owner()
getProfile(BatchDescriptorId)
Profile
processL3Owner(L3Owner)
OperationResult
processBatchDescriptor(BatchDescriptor)
processBatchDescriptor(BatchDescriptor)
verifyChallenge()
ProfileAccepted
ProfileAccepted
프로파일 소유권이 이전된다.
챌린지 삭제
installProfile(Profile,ProfileHash)
installProfile(Profile,ProfileHash)
installProfile(Profile,ProfileHash)
ProfileOperationResult
ProfileOperationResult
ProfileOperationResult
askProfileOperation(ProfileOperationResult)
askProfileOperation(ProfileOperationResult)

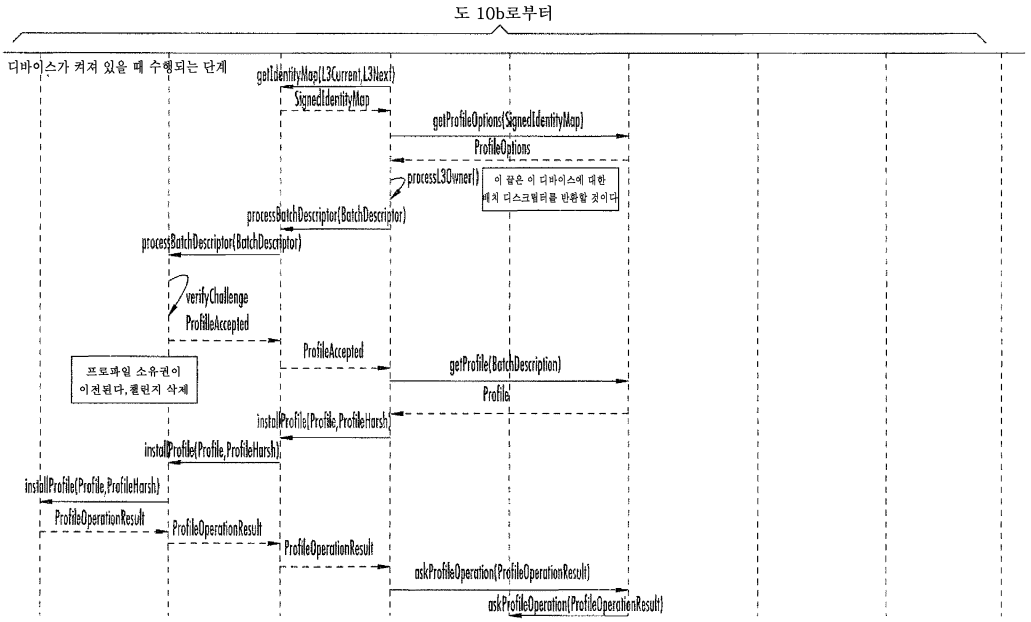
도면10a


콜드 SIM을 디바이스에 전달(전제 조건: 브로큰 URL) - 단계 1(공장에서) - 챌린지를 생성하고 브로큰과 공유
디바이스의 eUICC
AP
클라이언트: 프로파일 로커(L1)
클라이언트: 프로파일 에이전트(L21)
클라이언트: L3
클라이언트: 브로커
서버: 브로커(L3)
서버: 프로파일 에이전트(L3)
서버: 프로파일 로커(L1)
getIdentityMap(L3Current,L3Next)
SignIdentityMap
getProfileOptions(SignedIdentityMap)
createSession(ProfileOption, OperationType)
ProfileOptions
createSession(ProfileOption)
sessionRequest
sessionRequest
initializeSession(SessionRequest)
verifySession()
verifySession(SessionRequest)
signedSessionResponse
sessionResponse
prepareProfileOperationRequest(sessionResponse)
prepareProfileOperationRequest(sessionResponse)
verifySession(SessionResponse)
createChallenge(SessionResponse)
ProfileL2OperationBlob
createL3ProfileOperationBlob()
ProfileL2OperationBlob,ProfileL3OperationBlob
ProfileL2OperationBlob,(ProfileL2OperationBlob, ProfileL3OperationBlob)
verifyRequest()
profileProfileOperation(ProfileL2OperationBlob)
verifyRequest()
ErrorCodeProfilePostponed
ErrorCodeProfilePostponed
챌린지가 서버를 통하여 배포 센터로 송신된다
도 10b로

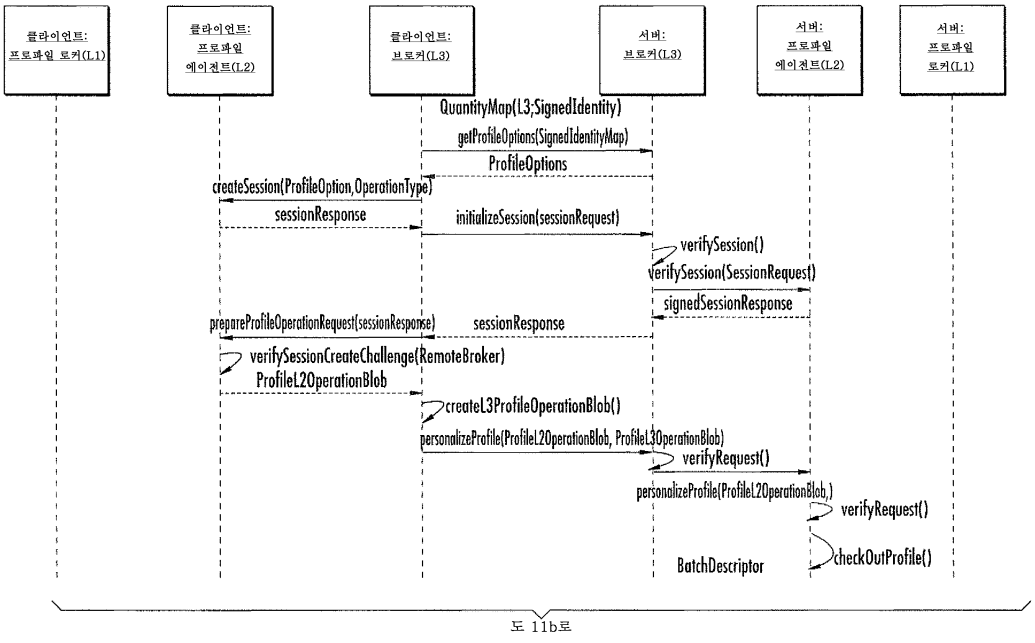
도면10b


도 10a로부터
콜드 SIM을 디바이스에 전달(사전 개인화)(전제 조건: 브로커 URL) - 단계 2
디바이스의 eUICC
AP
배포 센터
클라이언트: 프로파일 로커(L1)
클라이언트: 프로파일 에이전트(L21)
클라이언트:L3
클라이언트: 브로커
공장:L2
공장:브로커(L2)
서버:브로커(L3)
서버: 프로파일 에이전트(L2)
서버: 프로파일 로커(L1)
prepareProfileOperationRequest(DeviceUniqueId,OperationType)
createChallenge(DeviceUniqueId)
ProfileL2OperationBlob
createL3ProfileOperationBlob()
performProfileOperation(ProfileL2OperationBlob,ProfileL3OperationBlob)
verifyRequest()
performProfileOperation(ProfileOperationBlob)
verifyRequest()
checkOutProfile()
BatchDescriptor
createL3Owner()
BatchDescriptor,L3Owner
personalizeProfile(profileRequestBlob)Profile
processBatchDescriptor(BatchDescriptor)
verifyChallenge()
ProfileAccepted
여기를 통하는 모든 단계들이 디바이스의 전원이 꺼진 상태로 공장 브로커에 의해 수행된다
도 10c로

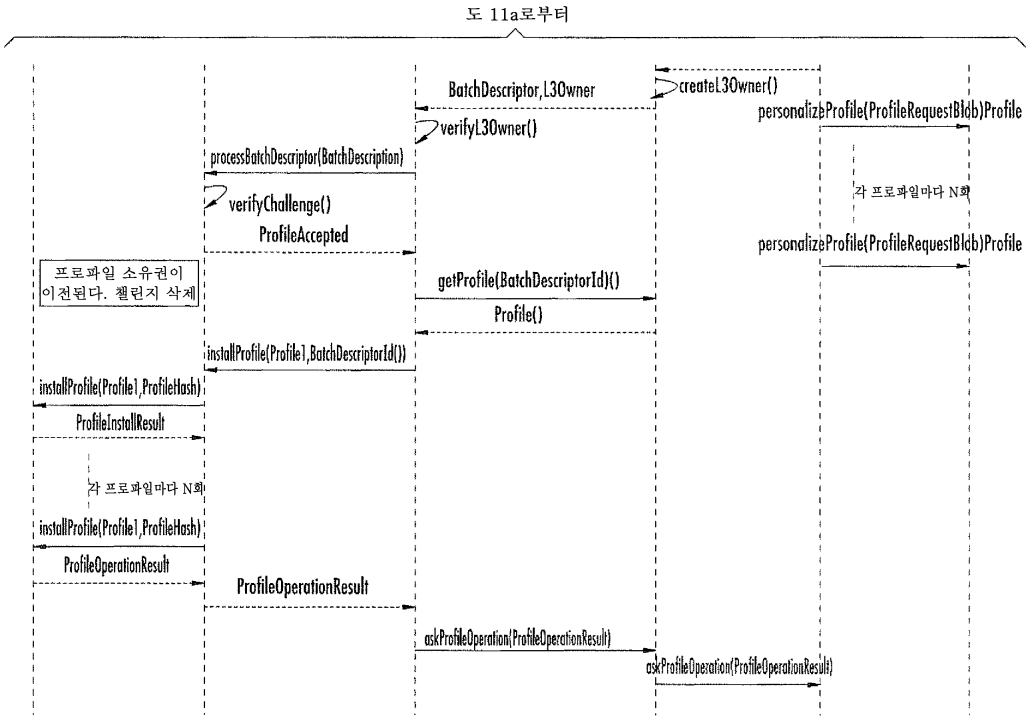
도면10c


도 10b로부터
디바이스가 켜져 있을 때 수행되는 단계
getIdentityMap(L3current,L3next)
SignedIdentityMap
getProfileOptions(SignedIdentityMap)
ProfileOptions
processL3Owner()
이 함은 이 디바이스에 대한
베치 디스크립터를 반환할 것이다
processBatchDescriptor(BatchDescriptor)
processBatchDescriptor(BatchDescriptor)
verifyChallenge
ProfileAccepted
ProfileAccepted
프로파일 소유권이
이전된다, 클린지 삭제
getProfile(BatchDescription)
Profile
installProfile(Profile,ProfileHarsh)
installProfile(Profile,ProfileHarsh)
installProfile(Profile,ProfileHarsh)
ProfileOperationResult
ProfileOperationResult
ProfileOperationResult
askProfileOperation(ProfileOperationResult)
askProfileOperation(ProfileOperationResult)

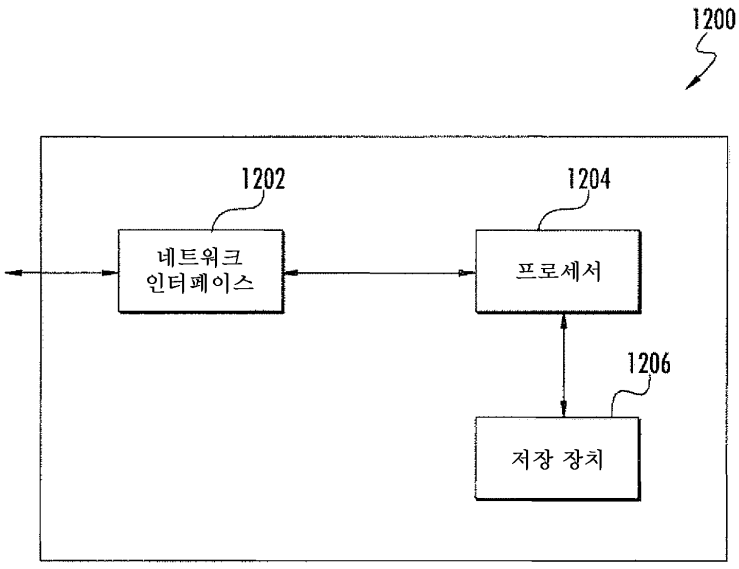
도면11a


클라이언트:
프로파일 로커(L1)
클라이언트:
프로파일
에이전트(L2)
클라이언트:
브로커(L3)
서버:
브로커(L3)
서버:
프로파일
에이전트(L2)
서버:
프로파일
로커(L1)
QuantityMap(L3;SignedIdentity)
getProfileOptions(SignedIdentityMap)
ProfileOptions
createSession(ProfileOption,OperationType)
sessionResponse
initializeSession(sessionRequest)
verifySession()
verifySession(SessionRequest)
signedSessionResponse
prepareProfileOperationRequest(sessionResponse)
sessionResponse
verifySessionCreateChallenge(RemoteBroker)
ProfileL2OperationBlob
createL3ProfileOperationBlob()
personalizeProfile(ProfileL2OperationBlob, ProfileL3OperationBlob)
verifyRequest()
personalizeProfile(ProfileL2OperationBlob,)
verifyRequest()
BatchDescriptor
checkOutProfile()
도 11b로

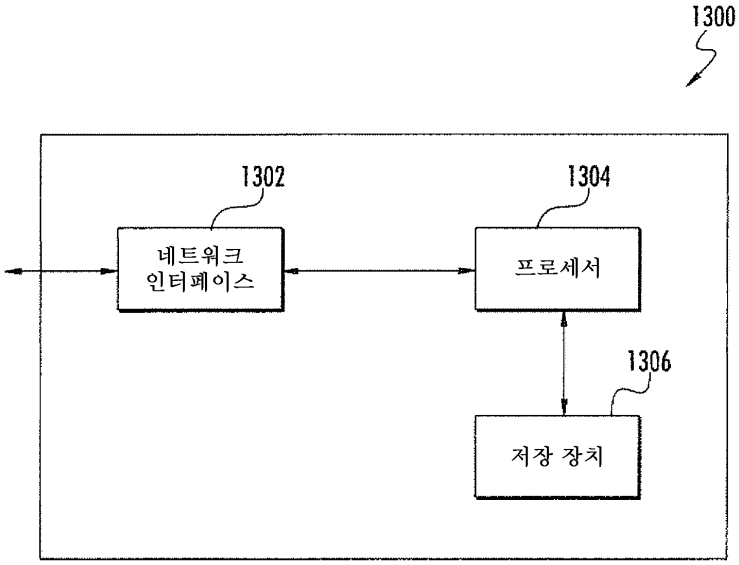
도면11b


도 11a로부터
BatchDescriptor,L3Owner
createL3Owner()
personalizeProfile(ProfileRequestBlob)Profile
verifyL3Owner()
processBatchDescriptor(BatchDescription)
각 프로파일마다 N회
verifyChallenge()
ProfileAccepted
personalizeProfile(ProfileRequestBlob)Profile
프로파일 소유권이 이전된다. 챌린지 삭제
getProfile(BatchDescriptorId)()
Profile()
installProfile(Profile1,BatchDescriptorId())
installProfile(Profile1,ProfileHash)
ProfileInstallResult
각 프로파일마다 N회
installProfile(Profile1,ProfileHash)
ProfileOperationResult
ProfileOperationResult
askProfileOperation(ProfileOperationResult)
askProfileOperation(ProfileOperationResult)

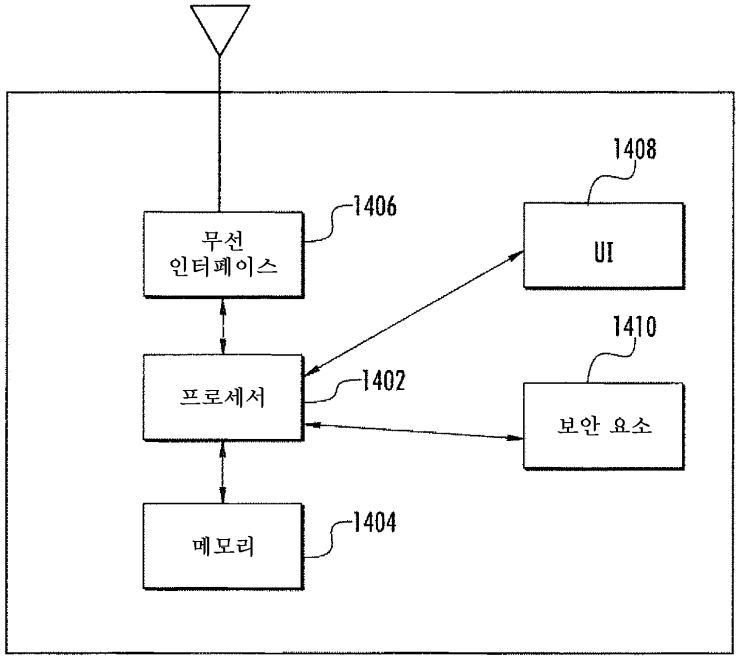
도면12


1200
1202
1204
네트워크 인터페이스
프로세서
1206
저장 장치

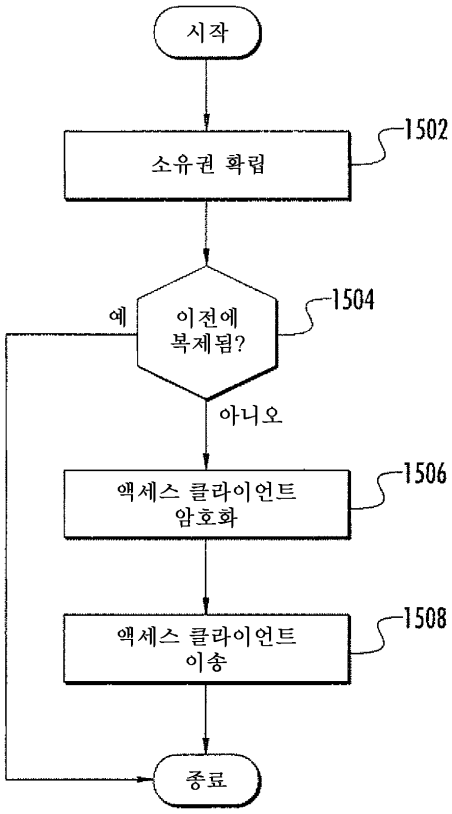
도면13


1300
1302
1304
네트워크
인터페이스
프로세서
1306
저장 장치

도면14


1408
1406
무선
인터페이스
UI
1410
프로세서
1402
보안 요소
메모리
1404

도면15


시작
소유권 확립
1502
이전에 복제됨?
1504
예
아니오
액세스 클라이언트 암호화
1506
액세스 클라이언트 이송
1508
종료