(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013 년 5 월 10 일 (10.05.2013)

WIPO | PCT

(10) 국제공개번호
WO 2013/066076 A1

(51) 국제특허분류:
H04W 8/18 (2009.01) *H04W 12/00* (2009.01)

(21) 국제출원번호: PCT/KR2012/009128

(22) 국제출원일: 2012 년 11 월 1 일 (01.11.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0113479 2011 년 11 월 2 일 (02.11.2011) KR
10-2012-0122797 2012 년 11 월 1 일 (01.11.2012) KR

(71) 출원인: **주식회사 케이티 (KT CORPORATION)** [KR/KR]; 463-815 경기도 성남시 분당구 정자동 206, Gyeonggi-do (KR).

(72) 발명자: **이진형 (LEE, Jin Hyoung)**; 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR). **윤여민 (YOON, Yeu Min)**; 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR). **김성철 (KIM, Sung Chul)**; 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR). **정윤필 (JEUNG, Youn Pil)**; 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR).

(74) 대리인: **김은구 (KIM, Eungu)** 등; 135-908 서울시 강남구 역삼동 636-15 상원빌딩 2 층, Seoul (KR).

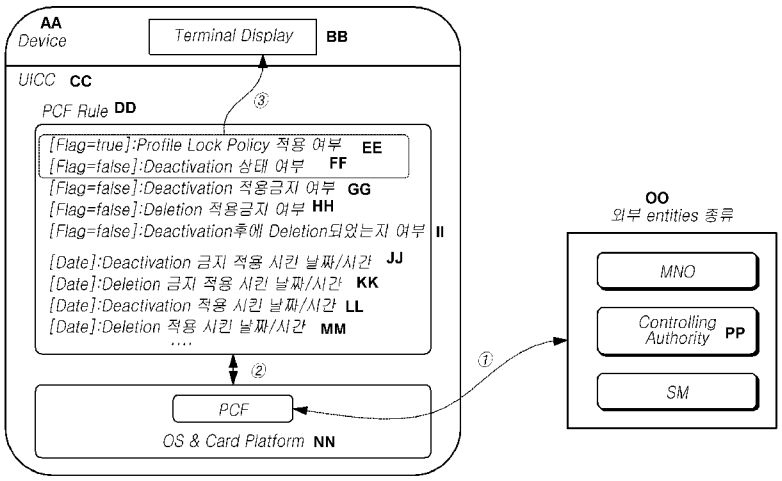
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ,

[다음 쪽 계속]

(54) **Title**: METHOD FOR MANAGING THE STATE OF AN EMBEDDED UICC, AND EMBEDDED UICC

(54) **발명의 명칭** : 내장 UICC 의 상태 관리 방법 및 내장 UICC



AA ... Device
BB ... Terminal Display
CC ... UICC
DD ... PCF Rule
EE ... [Flag=true]: Is a profile lock policy to be applied?
FF ... [Flag=false]: Is it a deactivation state?
GG ... [Flag=false]: Is the application of a deactivation prevented?
HH ... [Flag=false]: Is the application of a deletion prevented?
II ... [Flag=false]: Is deletion applied after deactivation?
JJ ... [Date]: Date/time when the prevention of a deactivation was applied
KK ... [Date]: Date/time when the prevention of a deletion is applied
LL ... [Date]: Date/time when a deactivation is applied
MM ... [Date]: Date/time when a deletion is applied
NN ... OS and Card Platform
OO ... Types of external entities
PP ... Controlling Authority

(57) **Abstract**: The present invention relates to a method for managing the state of an eUICC, and more particularly, to method for managing the state of an eUICC, which supports the enforcement of a PCF rule for controlling whether the state of an eUICC is a locked or unlocked state.

(57) **요약서**: 본 발명은 eUICC 의 상태 관리 방법에 관한 것으로서, 더욱 상세하게는, eUICC 의 상태가 잠금(Lock)인지 열림(Unlock)인지를 제어하기 위한 PCF 규칙을 강제하는 것을 지원하는 것을 특징으로 하는 eUICC 의 상태 관리 방법 및 e U I C C 에 관한 것이다.

WO 2013/066076 A1

TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

— 청구범위 보정 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

명세서

발명의 명칭: 내장 UICC의 상태 관리 방법 및 내장 UICC

기술분야

[1] 본 발명은 내장 UICC(Embedded Universal Integrated Circuit Card; 이하 "eUICC"라 함)의 정책 제어 기능(Policy Control Function; 이하 "PCF"라 함) 규칙에 따른 프로파일 잠금 상태 관리 방법 및 장치에 관한 것이다.

배경기술

[2] UICC(Universal Integrated Circuit Card)는 단말기 내에 삽입되어 사용자 인증을 위한 모듈로서 사용될 수 있는 스마트 카드이다. UICC는 사용자의 개인 정보 및 사용자가 가입한 이동 통신 사업자에 대한 사업자 정보를 저장할 수 있다. 예를 들면, UICC는 사용자를 식별하기 위한 IMSI(International Mobile Subscriber Identity)를 포함할 수 있다. UICC는 GSM(Global System for Mobile communications) 방식의 경우 SIM(Subscriber Identity Module) 카드, WCDMA(Wideband Code Division Multiple Access) 방식의 경우 USIM(Universal Subscriber Identity Module) 카드로 불리기도 한다.

[3] 사용자가 UICC를 사용자의 단말에 장착하면, UICC에 저장된 정보들을 이용하여 자동으로 사용자 인증이 이루어져 사용자가 편리하게 단말을 사용할 수 있다. 또한, 사용자가 단말을 교체할 때, 사용자는 기존의 단말에서 탈거한 UICC를 새로운 단말에 장착하여 용이하게 단말을 교체할 수 있다.

[4] 소형화가 요구되는 단말, 예를 들면 기계 대 기계(Machine to Machine, M2M) 통신을 위한 단말은 UICC를 착탈할 수 있는 구조로 제조할 경우 단말의 소형화가 어려워진다. 그리하여, 착탈할 수 없는 UICC인 eUICC 구조가 제안되었다. eUICC는 해당 UICC를 사용하는 사용자 정보가 IMSI 형태로 수록되어야 한다.

[5] 기존의 UICC는 단말에 착탈이 가능하여, 단말의 종류나 이동 통신 사업자에 구애받지 않고 사용자는 단말을 개통할 수 있다. 그러나, 단말을 제조할 때부터 제조된 단말은 특정 이동 통신 사업자에 대해서만 사용된다는 전제가 성립되어야 eUICC 내의 IMSI를 할당할 수 있다. 단말을 발주하는 이동 통신 사업자 및 단말 제조사는 모두 제품 재고에 신경을 쓸 수 밖에 없고 제품 가격이 상승하는 문제가 발생하게 된다. 사용자는 단말에 대해 이동 통신 사업자를 바꿀 수 없는 불편이 있다. 그러므로, eUICC의 경우에도 이동 통신 사업자에 구애받지 않고 사용자가 단말을 개통할 수 있는 방법이 요구된다.

[6] 한편, 최근 eUICC의 도입으로 인하여 여러 이통 통신 사업자의 가입자 정보를 원격에서 UICC로 업데이트 할 필요가 생기게 되었고, 그에 따라 가입자 정보 관리를 위한 가입 관리 장치(Subscription Manager; 이하 "SM"이라 함) 또는 프로파일 관리장치(Profile Manager; 이하 "PM"이라 함)가 논의되고 있다.

[7] 이러한 SM은 주로 eUICC에 대한 정보 관리와, 여러 이통통신 사업자에 대한 정보 관리와, 이동통신 사업자 변경시 그에 대한 인증 및 원격 정보 변경 등의 기능을 담당하는 것으로 논의되고 있으나, 정확한 기능이나 역할에 대해서는 아직 결정된 바가 없는 실정이다.

[8] 또한, eUICC를 둘러싼 여러 개체 또는 엔터티의 eUICC 관련 정책을 정의하기 위하여 PCF가 논의되고 있으나, 그 기능이나 구조 등에 대해서 정해진 바가 없는 실정이다.

발명의 상세한 설명

기술적 과제

[9] 본 발명의 목적은 eUICC의 PCF를 정의하는 방법을 제공한다.

[10] 본 발명의 다른 목적은 eUICC의 PCF 규칙에 따라 eUICC 내부의 프로파일을 관리하는 방법을 제공하는 것이다.

[11] 본 발명의 또 다른 목적은 eUICC의 PCF 규칙에 따라 eUICC 내부의 프로파일의 상태를 관리할 수 있는 방법을 제공하는 것이다.

[12] 본 발명의 또 다른 목적은 eUICC의 PCF 규칙에 따라 eUICC 내부의 프로파일을 잠금 상태로 관리할 수 있는 방법을 제공하는 것이다.

과제 해결 수단

[13] 일 측면에서, 본 발명은, MNO(Mobile Network Operator) 및 SM(Subscription Manager)과 연동 되어 있는 eUICC(embedded Universal Integrated Circuit Card)로서, 파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 형태로서 프로비저닝(Provisioning) 되거나 존재하는 프로파일을 포함하고, 상기 eUICC의 상태가 잠금(Lock) 또는 열림(Unlock)이 되는지를 제어하는 PCF 규칙을 강제하는(Enforcing) 것을 지원하는 것을 특징으로 하는 eUICC를 제공한다.

[14] 다른 측면에서, 본 발명은, MNO(Mobile Network Operator) 및 SM(Subscription Manager)과 연동 되어 있는 eUICC(embedded Universal Integrated Circuit Card)의 상태 관리 방법으로서, 상기 eUICC가 파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 프로파일을 저장하는 단계; 및 상기 eUICC가 상기 eUICC의 상태가 잠금 또는 열림이 되는지를 제어하는 PCF 규칙을 강제하는(enforcing) 것을 지원하는 단계를 포함하는 eUICC의 상태 관리 방법을 제공한다.

[15] 또 다른 측면에서, 본 발명은, MNO(Mobile Network Operator) 및 SM(Subscription Manager)과 연동 되어 있는 eUICC(embedded Universal Integrated Circuit Card)로서, 파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 프로파일을 저장하는 프로파일 저장부; 상기 eUICC의 상태가 잠금 또는 열림이 되는지를 제어하는데 참조 되는 PCF 규칙을 저장하는 PCF 규칙 저장부; 및 상기 PCF 규칙에 따라, 상기 eUICC의 상태가 잠금 또는 열림이 되는지를 제어하는 eUICC 상태 제어부를 포함하는 eUICC를 제공한다.

[16] 또 다른 측면에서, 본 발명은, MNO(Mobile Network Operator) 및 SM(Subscription Manager)과 연동 되어 있는 eUICC(embedded Universal Integrated Circuit Card)의 상태 관리 방법으로서, 권한이 있는 외부 엔티티가 상기 eUICC에 로딩 된 MNO의 프로파일의 잠금과 관련된 상기 eUICC 내 PCF 규칙(Policy Control Function Rule)을 설정하는 단계; 및 상기 권한이 있는 외부 엔티티가 상기 PCF 규칙에 따라 상기 eUICC에 로딩 된 상기 MNO의 프로파일에 대한 잠금 상태를 제어하는 단계를 포함하는 eUICC의 상태 관리 방법을 제공한다.

[17] 또 다른 측면에서, MNO(Mobile Network Operator)와 연동하여 통신 서비스를 제공하는 기기로서, 상기 MNO, CA(Controlling Authority) 및 SM(Subscription Manager) 중 하나 이상의 외부 엔티티와 연동하고, 파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 형태로서 프로비저닝(Provisioning) 되거나 존재하는 프로파일을 포함하며, 상기 eUICC의 상태가 잠금 또는 열림이 되는지를 제어하는 PCF 규칙(Policy Control Function Rule)을 강제하는 것을 지원하는 eUICC(embedded Universal Integrated Circuit Card); 및 상기 eUICC 내부의 상기 PCF 규칙의 일부를 읽어와 디스플레이하는 터미널 디스플레이를 포함하는 통신 서비스를 제공하는 기기를 제공한다.

도면의 간단한 설명

[18] 도 1은 본 발명이 적용되는 eUICC를 포함한 전체 서비스 아키텍처를 도시한다.

[19] 도 2는 본 발명이 적용될 수 있는 SM 분리 환경의 시스템 아키텍처를 도시한다.

[20] 도 3은 본 발명이 적용되는 eUICC 또는 eSIM와 관련된 개체들의 라이프 싸이클을 예시하는 도면이다.

[21] 도 4는 본 발명이 적용되는 eUICC 및 그를 포함하는 단말의 내부 구조와, 외부 엔터티 들을 도시한다.

[22] 도 5는 본 발명의 일 실시예에 의한 eUICC 내부 구조에 대한 예시도이다.

[23] 도 6은 본 발명의 일 실시예에 의한 eUICC 내부 구조에 대한 다른 예시도이다.

[24] 도 7은 본 발명에 의한 PCF 규칙에 따른 프로파일 관리 방법이 적용되는 경우의 신호 흐름을 나타낸 도면이다.

[25] 도 8은 본 발명의 일 실시예에 의한 eUICC의 상태 관리 방법에 대한 흐름도이다.

[26] 도 9는 본 발명의 일 실시예에 의한 eUICC에 대한 블록도이다.

[27] 도 10은 본 발명의 일 실시예에 의한 eUICC의 상태 관리 방법에 대한 다른 흐름도이다.

발명의 실시를 위한 형태

[28] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성

또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[29] 현재 GSMA에서 활발하게 논의되는 M2M(Machine-to-Machine) 단말은 특성상 크기가 작아야 하는데, 기존 UICC를 사용하는 경우에는, M2M 단말에 UICC를 장착하는 모듈을 별도 삽입해야 하므로, UICC를 탈착가능한 구조로 M2M단말을 제조하게 되면, M2M 단말의 소형화가 힘들게 된다.

[30] 따라서, UICC 착탈이 불가능한 내장(Embedded) UICC 구조가 논의되고 있는데, 이때 M2M 단말에 장착되는 eUICC에는 해당 UICC를 사용하는 이동통신 사업자(Mobile Network Operator; 이하 "MNO"라 함)정보가 국제 모바일 가입자 식별자(International Mobile Subscriber Identity, IMSI) 형태로 UICC에 저장되어 있어야 한다.

[31] 그러나, M2M 단말을 제조할 때부터 제조된 단말은 특정 MNO에서만 사용한다는 전제가 성립되어야 eUICC내의 IMSI를 할당할 수 있으므로, M2M 단말 또는 UICC를 발주하는 MNO나 제조하는 M2M 제조사 모두 제품 재고에 많은 신경을 할당할 수밖에 없고 제품 가격이 상승하게 되는 문제가 있어, M2M 단말 확대에 큰 걸림돌이 되고 있는 상황이다.

[32] 이와 같이, 기존의 착탈식 형태의 SIM과는 달리 단말에 일체형으로 탑재되는 eUICC 또는 eSIM은 그 물리적 구조 차이로 인해 개통 권한, 부가 서비스 사업 주도권, 가입자 정보 보안 등에 대한 많은 이슈들이 존재한다. 이를 위해 GSMA 및 ETSI의 국제 표준화 기관에서는 사업자, 제조사, SIM 제조사 등의 유관 회사들과 최상위 구조를 포함한 필요한 요소에 대해 표준화 활동을 전개하고 있다. eSIM이 표준화 단체들을 통해 논의되면서 이슈의 중심에 있는 것은 Subscription Manager라고 불리는 SM으로 사업자 정보 (Operator Credential, MNO Credential, Profile, eUICC Profile, Profile Package 등 다른 표현으로 사용될 수 있음)를 eSIM에 발급하고 가입(Subscription) 변경 또는 MNO 변경에 대한 프로세스를 처리하는 등 eSIM에 대한 전반적인 관리 역할을 수행하는 개체 또는 그 기능/역할을 의미한다.

[33] 최근 GSMA에서는 SM의 역할을 사업자 정보를 생성하는 역할을 수행하는 SM-DP (Data Preparation)과 eSIM에 사업자 정보의 직접적 운반을 수행하는 SM-SR (Secure Routing)로 분류한 구조와, 프로파일을 암호화하여 전송하는 방안을 제안하였으나 세부적인 내용이 부족하다.

[34] 이에 본 발명의 일 실시예에서는 eUICC와 관련된 개체 또는 엔터티들의 정책 제어 기능(PCF) 규칙으로서 프로파일 잠금 정책을 수행하는 방안을 제안한다.

[35] 더 구체적으로는 PCF 규칙으로서 프로파일 잠금 정책 적용 여부를 나타내는 파라미터와, 프로파일 비활성화(Deactivation) 상태를 확인하는 파라미터, 프로파일 비활성화/삭제 적용 금지 여부를 나타내는 파라미터 등을 정의하여 사용함으로써, 프로파일 보안 정도에 따라서 해당 프로파일을 적절히 관리하는 방안을 제안한다.

[36] 본 명세서에서는 eSIM과 eUICC를 동등한 개념으로 사용한다.

[37] eSIM은 단말 제조 단계에서 IC칩을 단말 회로판 상에 부착시킨 후, 소프트웨어 형태의 SIM 데이터 (개통 정보, 부가 서비스 정보 등)를 OTA (Over The Air) 또는 오프라인 (PC와의 USB 등의 기술 기반 연결)을 통해 발급하는 방식의 새로운 개념의 SIM 기술이다. eSIM에서 사용되는 IC칩은 일반적으로 하드웨어 기반의 CCP (Crypto Co-Processor)를 지원하여 하드웨어 기반의 공개키 생성을 제공하며, 이를 애플리케이션 (예, 애플릿) 기반에서 활용할 수 있는 API를 SIM 플랫폼 (예, Java Card Platform 등)에서 제공한다. 자바 카드 플랫폼(Java Card Platform)은 스마트카드 등에서 멀티 애플리케이션을 탑재하고 서비스를 제공할 수 있는 플랫폼 중 하나이다.

[38] SIM은 제한된 메모리 공간과 보안상의 이유로 누구나 SIM 내에 애플리케이션을 탑재해서는 안되며, 이로 인해 애플리케이션 탑재를 위한 플랫폼 이외에 SIM을 애플리케이션 탑재 및 관리를 담당하는 SIM 서비스 관리 플랫폼을 필요로 한다. SIM 서비스 관리 플랫폼은 관리키를 통한 인증 및 보안을 통해 SIM 메모리 영역에 데이터를 발급하며, 글로벌 플랫폼(GlobalPlatform)과 ETSI TS 102.226의 RFM (Remote File Management) 및 RAM (Remote Application Management)은 이와 같은 SIM 서비스 관리 플랫폼의 표준 기술이다.

[39] eSIM 환경에서 중요한 요소 중의 하나인 SM은 eSIM은 원격으로 관리키(UICC OTA Key, GP ISD Key 등)를 통해 통신 및 부가 서비스 데이터를 발급하는 역할을 수행한다.

[40] GSMA에서는 SM의 역할을 SM-DP와 SM-SR로 분류하였다. SM-DP는 오퍼레이션 프로파일(또는 사업자 정보) 이외에 IMSI, K, OPc, 부가 서비스 애플리케이션, 부가 서비스 데이터 등을 안전하게 빌드(Build)하여 크레덴셜 패키지(Credential Package) 형태로 만드는 역할을 수행하며, SM-SR은 SM-DP가 생성한 크레덴셜 패키지를 OTA(Over-The-Air) 또는 GP SCP (Secure Communication Protocol)과 같은 SIM 원격 관리 기술을 통해 eSIM에 안전하게 다운로드하는 역할을 수행한다.

[41] 그리고 아래 도 1의 신뢰 서클(Circle of Trust)"이라는 구조를 제안하여 각 유사 개체 또는 엔터티 들간에 신뢰 관계의 중첩을 통해 MNO와 eSIM 간의 엔드-투-엔드(End-to-End) 신뢰 관계를 구축한다는 개념을 제안하였다. 즉, MNO1는 SM1과, SM1은 SM4, SM4는 eSIM과 신뢰관계를 형성하여, 이를 통해 MNO와 eSIM 간의 신뢰관계를 형성한다는 개념이다.

[42] 본 발명을 설명하기 전에 우선 본 명세서에서 사용할 용어에 대하여 설명한다.

[43] MNO(Mobile Network Operator)는 이동통신 사업자를 의미하며, 모바일 네트워크를 통해 고객에게 통신 서비스를 제공하는 엔터티를 의미한다.

[44] eUICC 공급자(eUICC Supplier)는 eUICC 모듈과 내장 소프트웨어(펌웨어와 오퍼레이팅 시스템 등)를 공급하는 자를 의미한다.

[45] 장치 공급자(Device Vendor)는 장치의 공급자, 특히 MNO에 의해서 구동되는

모바일 네트워크를 통한 무선 모뎀 기능을 포함하며, 따라서 결과적으로 UICC(또는 eUICC) 형태가 필요한 장치의 공급자를 의미한다.

[46] 프로비저닝(Provisioning)은 eUICC 내부로 프로파일을 로딩하는 과정을 의미하며, 프로비저닝 프로파일은 다른 프로비저닝 프로파일 및 오퍼레이션 프로파일을 프로비저닝할 목적으로 장치가 통신 네트워크에 접속하는데 사용되는 프로파일을 의미한다.

[47] 가입(Subscription)은 가입자와 무선통신 서비스 제공자 사이의 서비스 제공을 위한 상업적인 관계를 의미한다.

[48] eUICC 접근 크레덴셜(eUICC access credentials)은 eUICC 상의 프로파일을 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 eUICC 내의 데이터를 의미한다.

[49] 프로파일 엑세스 크레덴셜(Profile access credentials)은 프로파일 내부 또는 eUICC 내부에 존재하는 데이터로서, 프로파일 구조 및 그 데이터를 보호 또는 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 데이터를 의미한다.

[50] 프로파일(Profile)은 eUICC로 프로비저닝 되거나 eUICC 내에서 관리될 수 있는 파일 구조, 데이터 및 애플리케이션의 조합으로서, 사업자 정보인 오퍼레이션 프로파일, 프로비저닝을 위한 프로비저닝 프로파일, 기타 정책 제어 기능(PCF; Policy Control Function)을 위한 프로파일 등 eUICC 내에 존재할 수 있는 모든 정보를 의미한다.

[51] 오퍼레이션 프로파일(Operation Profile) 또는 사업자 정보는 사업자 가입(Operational Subcription)과 관련된 모든 종류의 프로파일을 의미한다.

[52] 활성화 프로파일(Active Profile)은 파일 혹은 애플리케이션이 MNO와 연관된 PCF의 통제 하에 UICC-Terminal interface에 의해 선택 가능 할 때 액티브 프로파일이라고 부른다.

[53] PCF 규칙 (Policy Control Function Rule)은 eUICC안의 Provisioning 혹은 Operational profile의 관리를 control하는 MNO에 의해 정의된 규칙이다. PCF 규칙은 network, eUICC platform , 혹은 Provisioning 혹은 Operational profile안에 존재 할 수 있다.

[54] PCF (Policy Control Function)는 PCF 규칙을 강제할 수 있는 application/service를 말한다. PCF 규칙은 eUICC platform안에 혹은/그리고 Subscription Manager 레벨 혹은 MNO 레벨에서 수행될 수 있다.

[55] CA (Controlling Authority)는 오퍼레이셔널 프로파일(Operational Profile) 또는 프로비저닝 프로파일(Provisioning Profile)의 스왑(Swap)하는 과정에서 원격에서 업데이트/삭제/활성화/비활성화(update/delete/activate/deactivate)의 MNO에 의 신뢰(trust)에 의해 권한이 있는 엔티티(entity)를 의미한다.

[56] SM(Subscription manager)는 가입 관리 장치로서, eUICC의 관리 기능을 수행하는 엔터티로서, 오퍼레이셔널 프로파일(Operational Profile) 또는

프로비저닝 프로파일(Provisioning Profile)의 스왑(Swap)하는 과정에서 원격에서 업데이트/삭제/활성화/비활성화(update/delete/activate/deactivate)의 MNO에 의 신뢰(trust)에 의해 권한이 있는 엔티티(entity)를 의미한다.

[57] 도 1은 본 발명이 적용되는 eSIM(eUICC)을 포함한 전체 서비스 아키텍처를 도시한다.

[58] 전체 시스템에 대해서 설명하면 다음과 같다.

[59] 본 발명이 적용될 수 있는 eUICC 시스템 아키텍처는 다수의 MNO 시스템과, 1 이상의 SM 시스템, eUICC 제조사 시스템, eUICC를 포함하는 장치(Device) 제조사 시스템 및 eUICC 등을 포함할 수 있으며, 각 엔터티 또는 주체에 대한 설명은 다음과 같다.

[60] 도 1에서 점선은 신뢰 서클을 도시하고, 2개 실선은 안전한 링크를 의미한다.

[61] 가입정보가 저장되어 전달되는 시나리오가 필요하면, MNO의 승인과 MNO의 컨트롤 하에서 이루어져야 한다. 특정 시각에 단일의 eUICC 상에는 1개만의 액티브 프로파일이 있어야 하며, 이때 액티브 프로파일은 특정 시간에 단일 HLR에 부가되는 것을 의미한다.

[62] MNO와 eUICC는 MNO 크레덴셜(Credentials) 정보, 즉 프로파일(오퍼레이션 프로파일, 프로비저닝 프로파일 등)를 복호할 수 있어야 한다. 이에 대한 유일한 예외는 예를 들면 SIM 벤더와 같이 특정 MNO으로부터 위임받은 제3 기관이 될 수 있다. 하지만, 이를 수행하기 위한 제3 기관의 일반적인 기능은 아니다.

[63] 가입(Subscription)은 오퍼레이터 정책 제어의 외부에서는 eUICC 내에서 스위칭될 수 없다. 사용자는 MNO 컨텐스트와 그의 활성화 가입의 어떠한 변경도 알고 있어야 하며, 시큐리티 위험을 피할 수 있어야 하고, 현재의 UICC 모델과 대적할 수 있을 정도의 시큐리티 레벨이 필요하다.

[64] MNO 크레덴셜 또는 프로파일은 K, 알고리즘, 알고리즘 파라미터, 부가 서비스 애플리케이션, 부가 서비스 데이터 등을 포함하는 가입 크레덴셜을 의미할 수 있다.

[65] MNO 크레덴셜 또는 프로파일의 전달은 종단에서 종단까지 안전한 방식으로 이루어져야 한다. 전송은 시큐리티 체인을 깨지 않는 연속적인 단계로 이루어질 수 있으며, 전송 체인의 모든 단계는 MNO의 인식 및 승인 하에서 이루어져야 한다. 전송 체인 내의 어떠한 엔터티도 MNO 크레덴셜을 명확하게 볼 수 없어야 하지만, 유일한 예외는 예를 들면 SIM 벤더와 같이 특정 MNO으로부터 위임받은 제3 기관이 될 수 있다. 하지만, 이를 수행하기 위한 제3 기관의 일반적인 기능은 아니다.

[66] 오퍼레이터는 자신의 크레덴셜에 대해서 완전한 제어권을 가져야 하며, 오퍼레이터는 SM 오퍼레이션에 대해서 강한 감독권과 제어권한을 가져야 한다.

[67] SM 기능은 MNO 또는 제3 기관에 의하여 제공되어야 하며, 만약 제3 기관에 의하여 제공된다면 SM과 MNO 사이에는 상업적인 관계가 설정되어 있는 경우 등일 것이다.

[68] SM은 가입 관리를 위해서 MNO 가입자와 어떠한 직접적인 관련도 없다. MNO가 가입자와 관계를 가지며 고객 가입을 위한 진입 포인트가 되어야 하지만, 이는 M2M 서비스 제공자(M2M 서비스 제공자는 MNO 가입자 임)가 자신의 고객과 가질 수 있는 계약 관계에 편승할 의도는 아니다.

[69] MNO가 스왑(swap)되는 동안, 도너(Donor) 및 리시빙 MNO는 서로 사전 계약이 있을 수도 있고 없을 수도 있다. 사전 계약을 승인할 수 있는 메커니즘이 있어야 한다. 도너 오퍼레이터의 정책 제어(Policy Control) 기능은 자신의 크레덴셜의 제거 조건에 대하여 정의할 수 있으며, 정책 제어 기능(Policy Control Function; PCF)이 이러한 기능을 구현할 수 있다.

[70] 아키텍처는 SM이라고 정의되는 기능을 도입하며, SM의 주요한 역할은 MNO 크레덴셜을 포함하는 패키지 또는 프로파일을 준비해서 eUICC로 전달하는 것이다. SM 기능은 MNO에 의하여 직접적으로 제공될 수도 있고, MNO가 SM 서비스를 획득하기 위하여 제3 기관과 계약할 수도 있을 것이다.

[71] SM의 역할은 SM-SR, SM-DP와 같은 2개의 서브 기능으로 나뉘어 질 수 있다.

[72] 실제로, 이러한 SM-SR, SM-DP 기능들은 다른 엔터티에 의하여 제공될 수도 있고, 동일한 엔터티에 의해서 제공될 수도 있다. 따라서, SM-DP와 SM-SR의 기능을 명확하게 경계지을 필요가 있고, 이들 엔터티들 사이의 인터페이스를 정의할 필요가 있다.

[73] SM-DP는 eUICC로 전달될 패키지 또는 프로파일의 안전한 준비를 담당하며, 실제 전송을 위하여 SM-SR과 함께 동작한다. SM-DP의 핵심 기능은 1) eUICC의 기능적 특성 및 인증 레벨(Certification Level)을 관리하는 것과, 2) MNO 크레덴셜 또는 프로파일(예를 들면, IMSI, K, 부가 서비스 애플리케이션, 부가 서비스 데이터 중 하나 이상이며, 이들 중 일부는 잠재적으로 MNO에 의하여 암호화(Enciphered)되어 있을 수 있음)을 관리하는 것과, 3) SM-SR에 의한 다운로드를 위하여 OTA 패키지를 계산하는 기능 등이며, 추후 부가적인 기능이 추가될 수 있을 것이다.

[74] 만일, SM-DP 기능이 제3주체(Third party)에 의하여 제공되는 경우에는 보안과 신뢰 관계가 아주 중요해진다. SM-DP는 실시간 프로비저닝(Provisioning) 기능 이외에도 상당한 정도의 백그라운드 프로세싱 기능을 보유할 수 있으며, 퍼포먼스, 스케러빌러티(Scalability) 및 신뢰도에 대한 요구사항이 중요할 것으로 예상된다.

[75] SM-SR은 크레덴셜 패키지를 해당되는 eUICC로 안전하게 라우팅하고 전달하는 역할을 담당한다. SM-SR의 핵심 기능은 1) 사이퍼(Ciphered)된 VPN을 통한 eUICC와의 OTA 통신을 관리하는 것과, 2) eUICC까지 엔드-투-엔드(end-to-end)를 형성하기 위하여 다른 SM-SR과의 통신을 관리하는 기능과, 3) eUICC 공급자에 의하여 제공되는 SM-SR OTA 통신을 위해 사용되는 eUICC 데이터를 관리하는 기능과, 4) 오직 허용된 엔터티만을 필터링함으로써 eUICC와의 통신을 보호하는 기능(방화벽 기능) 등이다.

[76] SM-SR 데이터베이스는 eUICC 벤더와 장치(M2M 단말 등) 벤더 및 잠재적으로 MNO에 의하여 제공되며, SM-SR 메시 네트워크를 통해서 MNO에 의하여 사용될 수 있다.

[77] 신뢰 서클(Circle of trust)은 프로비저닝 프로파일 전달 동안 엔드-투-엔드 시큐리티 링크를 가능하게 하며, SM-SR은 프로비저닝 프로파일의 안전한 라우팅 및 eUICC 디스커버리를 위하여 신뢰 서클을 공유한다. MNO는 신뢰 써클내의 SM-SR 및 SM-DP 엔터티와 링크될 수 있으며, 자체적으로 이런 기능을 제공할 수도 있을 것이다. 고객과 관련된 MNO의 계약상 및 법률상 의무를 어기지 않고, eUICC의 불법적인 사용(클로닝, 크레덴셜의 불법 사용, 서비스 거부, 불법적인 MNO 컨텍스트 변경 등)을 방지하기 위하여, eUICC와 MNO 크레덴셜 사이의 안전한 엔드-투-엔드 링크가 필요하다.

[78] 즉, 도 1에서 110은 SM들 끼리, 더 구체적으로는 SM-SR 멤버 사이에 형성되는 신뢰 서클을 나타내고, 120은 MNO 파트너들의 신뢰 서클이며, 130은 엔드투엔드 신뢰 링크를 도시한다.

[79] 도 2는 SM 분리 환경에서 SM-SR 및 SM-DP가 시스템에 위치하는 구성을 도시한다.

[80] 도 2와 같이, SM은 eUICC와 관련된 여러 프로파일(MNO의 오퍼레이션 프로파일, 프로비저닝 프로파일 등)을 안전하게 준비하는 SM-DP와, 그를 라우팅하기 위한 SM-SR로 구분되며, SM-SR은 다른 여러 SM-SR과 신뢰관계로 연동될 수 있고, SM-DP는 MNO 시스템에 연동되어 있다.

[81] 물론, SM-DP와 MNO 시스템의 배치는 도 2와 다르게 구현될 수 있다. (즉, SM-DP가 SM-SR과 연동되고, MNO 시스템이 SM-DP와 연동될 수 있다.

[82] 이상과 같이, 기존의 착탈식 형태의 SIM과는 달리 단말에 일체형으로 탑재되는 Embedded SIM (이하 eSIM)은 그 물리적 구조 차이로 인해 개통 권한, 부가 서비스 사업 주도권, 가입자 정보 보안 등에 대한 많은 이슈들이 존재한다. 그 중에서도 SM(Subscription Manager)를 통해 원격(remote)으로 오퍼레이셔널 프로파일(operational profile) 등이 관리되기 때문에 기존의 착탈식 USIM과는 다른 메커니즘이 필요한 부분이 많다.

[83] 즉, SM, 대표 기관 (Controlling Authority), 혹은 대표 MNO가 원격에서 MNO를 변경 시 변경 이전 MNO Profile (Operational profile)을 비활성화(deactivate) 또는 삭제(delete)를 하게 된다. 이때, 활성화된 오퍼레이셔널 프로파일(Active operational Profile)의 PCF 규칙(Policy Control Function Rule)에 따라 해당 원격의 엔티티(SM, controlling authority, 혹은 대표 MNO)가 오퍼레이셔널 프로파일(Active operational Profile)의 잠금(deactivation or deletion)을 할 수 있다. 하지만, 항상 다른 MNO로 변경을 위해 원격의 엔티티(SM, controlling authority, 혹은 대표 MNO) 이전의 MNO의 활성화/비활성화된 오퍼레이셔널 프로파일(active/inactive operational profile)을 비활성화(deactivate)하거나 삭제(delete)할 수 있도록 하는 것은 위험하다. (ex. 보조금 걸려 있는 단말, 요금

연체 단말, 혹은 도난 된 단말 등의 경우 등의 악의적이거나 의도되지 않은 상태에서 다른 MNO로의 변경을 금지시킬 PCF(Policy Control Function)이 eUICC에 적용 되어야 한다)

[84] 따라서 MNO의 PCF 규칙(Policy Control Function Rule)에 따라 오퍼레이셔널 프로파일(operational profile)의 잠금 상태(Lock Status)를 알 필요가 있다. 이를 알아야 오퍼레이셔널 프로파일(operational profile)의 잠금 상태(Lock Status)에 따라 원격의 엔티티(SM, controlling authority, 혹은 대표 MNO)가 수행(deactivate, delete, 혹은 delete/deactivate 불가)를 수행할 수 있을 것이다.

[85] 현재 착탈식의 SIM구조에서 USIM 차원의 서브스크립션 잠금(Subscription lock)은 SIM-LOCK 기능을 목적으로 하고 있고 IMSI기반의 체크 하는 형태로 이루어 지고 있다. eUICC상에서 프로파일 활성화/비활성화/삭제/로딩(Profile Active/Inactive/Delete/Loading)에 관한 규칙(Rule)을 관리하는 메커니즘은 종래 기술에는 존재하지 않는다.

[86] 도 3은 본 발명이 적용되는 eUICC 또는 eSIM와 관련된 개체들의 라이프 싸이클을 예시하는 도면이다.

[87] eUICC환경에서는 특정 MNO들의 가입(subscription)을 위한 MNO 프로파일 (Operational profile)들이 eUICC상에 다운로드가 가능하다. 이를 위해 프로파일(Operational profile)를 잠금(Lock)하는 방법은 GP의 애플리케이션 라이프 ㅅ사사이클(Application life cycle)을 이용할 수 있다. (도 1 참고)

[88] 따라서 eUICC환경에서는 원격에서 eUICC상의 카드/애플릿 잠금(ex. Global Platform의 RAM(Remote Application Management))을 이용하여 MNO 프로파일(Operational profile)들을 로딩(loading), 활성화/비활성화(active/inactive), 삭제(delete) 등을 관리하는 시스템을 가져 갈 것이다.

[89] 그러나 원격으로 오퍼레이셔널 프로파일(Operational Profile) 또는 프로비저닝 프로파일(Provisioning Profile)을, 1) MNO 변경 (Operational Profile Swap), 2) 가입자의 요구, 3) 계약, 미납, 도난, 등의 이유로 프로파일을 비활성화/삭제(deactivation/deletion)를 할 때 외부 권한 있는 엔티티(MNO, SM Controlling Authority)등에 의해 PCF 규칙에 따라 오퍼레이셔널 프로파일(Operational Profile) 또는 프로비저닝 프로파일(Provisioning Profile) 잠금 상태(Lock status)에 대해 접근해 읽기/갱신(read/update)을 할 수 있는 기능이 필요하다.

[90] 본 발명이 요구되는 경우를 정리하면 다음과 같다.

[91] 1) eUICC를 탑재한 기기의 가입 잠금(subscription lock) 상태를 사용자 혹은 소매상 관계자가 장치(device)의 디스플레이(display)를 통해 알아야 할 뿐만 아니라 SM 도 eUICC의 잠금 상태를 확인 할 수 있어야 한다.

[92] 1-1) Use case: MNO는 잠금 정보를 가입(subscription) 시작시점에 단말기 보조금 혹은 계약 관계에 따라 설정할 수 있어야 한다.

[93] 1-2) Use case: 또한 MNO는 이 잠금 컨디션(lock condition)을 사용자가 사용하는

동안에도 lock을 없애거나 가입자의 조항의 변경 같은 이유로 잠금(lock)의 기간의 만료 일을 업데이트 하거나 할 수 있어야 한다.

[94] 2) 사용자/소매상 관계자 혹은 다른 MNO, SM 등에 의해 우연히 혹은 의도적으로 Subscription(active operational profile)의 삭제/비활성화(deletion/deactivation)가 되지 않도록 해야 한다.

[95] 2-1)Use case: MNO 변경 시에도 이전 MNO 프로파일(active operational profile)이 악의적인 혹은 의도되지 않은 혹은 PCF 규칙에 어긋나는 MNO 혹은 SM에 의해 삭제/비활성화가 되지 않도록 해야 한다

[96] 2-2) Use case: 사용자/소매상 관계자에 의해 악의적으로 MNO 프로파일(active operational profile)이 삭제/비활성화가 되지 않도록 해야 한다

[97] 3) eUICC를 탑재한 device를 도난당한 경우 MNO에게 신고하면 MNO는 해당 IMSI의 기기(device)의 네트워크 액세스를 금지시켜 가입 잠금(Subscription lock)을 한다(네트워크 측면). 이때, 해당 MNO 프로파일(operational profile)은 외부 엔티티(다른 MNO혹은 SM, 사용자)에 의해 비활성화/삭제 혹은 다른 MNO의 오퍼레이셔널 프로파일(operational profile)로 교체되지 않도록 해야 한다. 또한, 거짓 도난 리포트였거나, 다시 device를 찾은 경우는 원격에서 다시 해당 MNO의 오퍼레이셔널 프로파일을 활성화하고 사용자의 단말(Device)의 디스플레이를 통해 상태 변경을 알릴 수 있어야 한다.

[98] 4) eUICC의 PCF 규칙에는 MNO 오퍼레이셔널 프로파일이 비활성화 된 이후에 삭제가 되었는지 여부에 대해 권한이 있는 외부 엔티티(ex. MNO, SM 등)가 알 수 있어야 한다.

[99] eUICC의 PCF 규칙에는 MNO 오퍼레이셔널 프로파일이 삭제(deletion)/비활성화(deactivation) 금지의 명령을 권한이 있는 외부 엔티티(ex. MNO, SM 등)가 수행한 시간을 기록할 수 있어서 권한이 있는 해당 외부 엔티티가 원할 경우 알려줄 수 있어야 한다.

[100] 도 4 내지 도 6은 본 발명의 여러 실시예에 의한 eUICC 내부 구조를 도시한다.

[101] 본 명세서에서 권한이 있는 외부 엔티티들의 종류로는 eUICC 아키텍처(architecture)에 따라, 1) 특정 MNO or 최초 프로비저닝(Provisioning)을 수행한 MNO, 2) CA(Controlling Authority), 3) SM (Subscription Manager)등이 될 수 있다.

[102] 본 발명이 적용될 수 있는 전제 조건은 다음과 같다.

[103] CA or SM이 오퍼레이셔널 프로파일(Operational Profile)을 스왑(MNO 변경)을 수행하는 엔티티가 될 수 있다. 물론, 본 발명에서는 최초 eUICC에 로딩된 오퍼레이셔널 프로파일(Operational Profile)의 주인인 MNO(도 4의 MNO1)가 오퍼레이셔널 프로파일을 스왑(MNO 변경)을 수행하는 주체가 될 수 있는 가정을 배제하지는 않는다. 즉, 이 외부 엔티티들 중 ((CA or SM) and MNO) 권한의 주체에 따라 eUICC 플랫폼(platform)에 PCF를 통해 PCF 규칙에 따라 프로파일 로딩, 활성화, 비활성화, 삭제 등을 원격에서 수행할 수 있다.

[104] PCF rule은 정의에 따라 오퍼레이셔널 프로파일, 프로비저닝 프로파일 안에 있거나 eUICC 플랫폼(그림 상의 OS & Card Platform)에 도 5와 같이 존재할 수도 있다.

[105] 물론, 본 발명에서는 도 5와 같은 구조로 한정되는 것은 아니며, 도 6과 같이, PCF가 오퍼레이셔널 프로파일 당 각각 하나의 애플리케이션(applet)형태로도 존재 할 수 있는 경우를 배제하지 않는다. (정의 중 PCF가 MNO 레벨에서 수행되는 상황)

[106] 이하에서는 본 발명의 일 실시예에 의한 구성을 설명한다.

[107] 우선, 기본 기능으로서 위의 PCF 규칙은 오퍼레이셔널/프로비저닝 프로파일 모두에 해당/적용되며, 오퍼레이셔널/프로비저닝 프로파일마다 하나의 PCF 규칙을 갖는다. 또한, PCF 규칙은 액세스 컨디션(access condition)에 따라, 1) 모든 엔티티들이 접근할 수 있는 내용, 2) 권한이 있는 엔티티들만이 접근할 수 있는 내용, 3) 프로파일 오너(Profile owner)만 접근할 수 있는 내용으로 나뉘고 구체적 내용은 아래와 같다.

[108] PCF 규칙은 프로파일의 상태가 활성화된 오퍼레이셔널 또는 프로비저닝 프로파일과 비활성화된 오퍼레이셔널 또는 프로비저닝 프로파일의 어떤 경우에도 권한이 있는 엔티티들(프로파일의 오너(owner) 및 권한이 있는 외부 엔티티들)이 읽을 수 있어야 하고, 터미널(Device 상)은 일부만(아래 그림의 점선 박스 안의 값) 읽을 수 있다. 즉, PCF 규칙에 대해서는 도 7의 1번의 화살표와 연결된 외부 엔티티들은 모두 읽기(Read)가 가능하고 3번의 화살표와 연결된 터미널 디스플레이(Terminal display)는 오직 PCF 규칙 값 중 일부만 읽기가 가능하다.

[109] 반면 PCF 규칙에 활성화된 오퍼레이셔널 또는 프로비저닝 프로파일과 비활성화된 오퍼레이셔널 또는 프로비저닝 프로파일 모두 어떤 경우에도 업데이트에 대해서는 오직 권한이 있는 외부 엔티티들(profile의 owner 및 권한이 있는 외부 entities) 에 의해서만 수행되어야 한다. 즉, PCF 규칙에 대해서는 아래 그림의 오직 1번의 화살표에 연결되어 있는 엔티티들(MNO and CA or/and SM)에 의해서만 업데이트가 가능하다. 다만, 그 예외로, 아래의 PCF 규칙 중 "Profile Deactivation 적용 금지 여부 value"는 관련 오퍼레이셔널 프로파일의 권한을 가진 MNO만이 업데이트가 가능하며, 또 하나의 예외로서 아래의 PCF 규칙 중 "Profile Deletion 적용 금지 여부 value"는 관련 오퍼레이셔널 프로파일의 권한을 가진 MNO만이 업데이트가 가능하다.

[110] PCF 규칙의 디폴트 값(default value) 이후 초기 설정 값은 MNO의 오퍼레이셔널 프로파일이 최초 로딩 되는 시점에 설정된다.

[111] MNO변경 할 때 어떤 이유에서든, 액티브 오퍼레이셔널 프로파일에 PCF 규칙 값이 셋팅(설정) 되지 않았다면 MNO 변경의 권한 주체인 외부 엔티티들(MNO, CA, SM)중 하나는 해당 오퍼레이셔널 프로파일의 MNO에게 가입 잠금(오퍼레이셔널 프로파일을 비활성화시키겠다는 내용)을 알리고 eUICC상의

오퍼레이셔널 프로파일을 비활성화(inactive) 상태로 만든다.

[112] 본 발명에 적용될 수 있는 PCF 규칙의 여러 파라미터 또는 값들을 정리하면 다음과 같다. 이러한 값 또는 파라미터는 아래 예시에 한정되는 것은 아니며 둘 이상이 하나로 구현될 수도 있으며, 하나가 둘 이상의 파라미터 등으로 분리되어 구현될 수도 있을 것이다. 또한, 경우에 따라서 하나 이상의 파라미터 또는 값들이 선택적으로 사용될 수도 있다.

[113] 1. 프로파일 잠금 정책(Profile Lock Policy) 적용 여부 정보(value)

[114] A. Flag = True or False

[115] B. Default Flag = True

[116] C. 프로파일 잠금(비활성화 또는 삭제) 하기 위한 적용 여부를 나타냄

[117] D. 액티브 프로파일에 대한 이값이 True이면 권한이 있는 외부 엔티티들(MNO, CA, SM 등)중 하나가 도 7의 1번, 2번 과정을 통해 해당 액티브 프로파일은 잠금(비활성 또는 삭제)가 가능하게 된다.

[118] i) 권한이 있는 외부 엔티티들(MNO and CA or/and SM 등)에 의해 읽기/업데이트 가능 값.

[119] ii) 터미널이 읽기가 가능한 값

[120]

[121] 2. 프로파일 비활성화(Profile Deactivation) 상태 여부 정보

[122] A. Flag = True or False

[123] B. Default Flag = False

[124] C. 이 Flag는 위의 1번의 Profile Lock Policy값이 True일 때 비활성화되었다는 의미.

[125] i) 1번의 Profile Lock Policy값이 False일 때 이 값은 True가 될 수 없음.

[126] D. 권한이 있는 외부 엔티티들(MNO and CA or/and SM 등)에 의해 read/update 가능 값.

[127] E. 터미널이 읽기가 가능한 값

[128]

[129] 3. 프로파일 비활성화(Profile Deactivation) 적용 금지 여부 정보

[130] A. Flag = True or False

[131] B. Default Flag = False

[132] C. 이 Flag가 True가 되면, 프로파일은 위의 1번의 Profile Lock Policy값이 True/False이건 상관없이 비활성화될 수 없다. 이값이 위의 1번 값보다 더 우선한다.

[133] D. 발명목적 섹션의 (2)번 요구사항 만족 시키기 위한 값

[134] E. 권한이 있는 외부 엔티티들(MNO and CA or/and SM 등)에 의해 읽기 가능 값.

[135] F. MNO 만이 update가 가능한 값

[136]

[137] 4. 프로파일 삭제(Profile Deletion) 적용 금지 여부 정보

[138] A. Flag = True or False

[139] B. Default Flag = False

[140] C. 이 Flag가 True가 되면, 프로파일은 위의 1번의 프로파일 잠금 정책 값이 True/False이건 상관없이 삭제될 수 없다. 이값이 위의 1번 값보다 더 우선 한다.

[141] D. 발명목적 섹션의 (2)번 요구사항 만족 시키기 위한 값

[142] E. 권한이 있는 외부 엔티티들(MNO and CA or/and SM 등)에 의해 읽기 가능 값.

[143] F. MNO 만이 업데이트(갱신)가 가능한 값

[144]

[145] 5. 프로파일 비활성화 후에 삭제되었는지 여부 정보

[146] A. Flag = True or False

[147] B. Default Flag = False

[148] C. 프로파일이 비활성화된 상태에서 삭제이 되었는지를 나타내는 상태 flag

[149] D. 권한이 있는 외부 엔티티들(MNO and CA or/and SM)에 의해 읽기/업데이트 가능 값.

[150]

[151] 6. 프로파일 비활성화 적용 금지시킨 날짜/시간 정보

[152] A. 프로파일 비활성화 적용을 금지시킨 날짜/시간 값 저장

[153] B. 즉, 위의 2번 flag값이 True가 된 시점을 기록 하게 됨

[154] C. 권한이 있는 외부 엔티티들(MNO and CA or/and SM)에 의해 읽기/업데이트 가능 값.

[155]

[156] 7. 프로파일 삭제 적용 금지시킨 날짜/시간 정보

[157] A. 프로파일 삭제 적용을 금지 시킨 날짜/시간 값 저장

[158] B. 즉, 위의 3번 flag값이 True가 된 시점을 기록 하게 됨

[159] C. 권한이 있는 외부 엔티티들(MNO and CA or/and SM)에 의해 읽기/업데이트 가능 값.

[160]

[161] 8. 프로파일 비활성화(Profile Deactivation) 적용 시킨 날짜/시간 value

[162] A. 프로파일 비활성화 적용 시킨 날짜/시간 값 저장

[163] B. 권한이 있는 외부 엔티티들(MNO and CA or/and SM)에 의해 읽기/업데이트 가능 값.

[164]

[165] 9. 프로파일 삭제(Profile Deletion) 적용 시킨 날짜/시간 value

[166] A. 프로파일 비활성화 적용 시킨 날짜/시간 값 저장

[167] B. 권한이 있는 외부 엔티티들(MNO and CA or/and SM)에 의해 읽기/업데이트 가능 값.

[168]

[169] 이하에서는 본 발명이 적용되는 예를 설명한다.

[170] [사용예 1]

[171] 최초 eUICC에 MNO1 오퍼레이셔널 프로파일이 로딩될 때 다음과 같이 MNO1이 PCF 규칙을 설정하였다.

[172] 1.프로파일 잠금 정책(Profile Lock Policy) 적용 여부 value = true

[173] 2.프로파일 비활성화(Profile Deactivation) 상태 여부 value = false

[174] 3.프로파일 비활성화(Profile Deactivation) 적용 금지 여부 value = false

[175] 4.프로파일 삭제(Profile Deletion) 적용 금지 여부 value = false

[176] 5.프로파일 비활성화(Profile Deactivation) 후에 삭제되었는지 여부 value = false

[177] 6.프로파일 비활성화(Profile Deactivation) 적용 금지시킨 날짜/시간 value = null

[178] 7.프로파일 삭제(Profile Deletion) 적용 금지시킨 날짜/시간 value = null

[179] 8.프로파일 비활성화(Profile Deactivation) 적용 시킨 날짜/시간 value = null

[180] 9.프로파일 삭제(Profile Deletion) 적용 시킨 날짜/시간 value = null

[181] 이 상태에서는 권한이 있는 MNO1과 CA or/and SM이 MNO1 오퍼레이셔널 프프프로파일을 잠금(비활성화 또는 삭제)이 가능한 상태이다. 현 상태에서 가능 use case는 다음과 같다.

[182] Use case1)

[183] 가입자가 계약 위반, 가입 해제 등의 사유로 휴지기(dormant) 상태 혹은 가입 해제 상태를 요청하면 MNO1은 오퍼레이셔널 프로파일을 비활성화 또는 삭제하게 된다.

[184] eUICC서버의 백앤드(backend)의 아키텍처(Architecture) 및 플로우(Flow)에 따라 (본 발명은 백앤드의 어떤 플로우도 수용하기 위해 사전에 최초 MNO(MNO1), SM 혹은 CA 어떤 경우도 MNO변경을 위해 오퍼레이셔널 프로파일을 잠금(비활성화 또는 삭제)을 하는 주체가 될 수 있다는 것을 위에서 가정을 하였다. 그러나 본 예제의 use case는 MNO 변경(Operational Profile Swap)의 주체를 SM(Subscription Manager)으로 가정하도록 하겠다.

[185] Use case2)

[186] 가입자가 MNO1에서 MNO2로 변경을 요청했으면 MNO2의 오퍼레이셔널 프로파일이 eUICC에 로딩한 후 SM(Subscription Manager)은 MNO1의 오퍼레이셔널 프로파일을 비활성화시킨 후 MNO1의 오퍼레이셔널 프로파일의 PCF 규칙 값 중 2.Profile Deactivation 상태 여부 value = true , 8.Profile Deactivation 적용 시킨 날짜/시간 value = 날짜/시간 으로 만든다. 다음으로 MNO2의 오퍼레이셔널 프로파일을 active 시킨다. 이 후에 커머셜(commercial) 정책에 따라 혹은 MNO의 서비스 정책에 따라 MNO1의 오퍼레이셔널 프로파일을 삭제시킬 수도 있고 비활성화 상태로 유지할 수도 있다.

[187] [사용예 2]

[188] eUICC에 MNO1 오퍼레이셔널 프로파일이 로딩되었다고 가정하고 MNO1이 해당 PCF 규칙을 다음과 같이 세팅(설정)하였다.

[189] 1.프로파일 잠금 정책(Profile Lock Policy) 적용 여부 value = true

[190] 2.프로파일 비활성화(Profile Deactivation) 상태 여부 value = false

[191] 3.프로파일 비활성화(Profile Deactivation) 적용 금지 여부 value = true

[192] 4.프로파일 삭제(Profile Deletion) 적용 금지 여부 value = true

[193] 5.프로파일 비활성화(Profile Deactivation) 후에 삭제되었는지 여부 value = false

[194] 6.프로파일 비활성화(Profile Deactivation) 적용 금지시킨 날짜/시간 value = 날짜/시간

[195] 7.프로파일 삭제(Profile Deletion) 적용 금지시킨 날짜/시간 value = 날짜/시간

[196] 8.프로파일 비활성화(Profile Deactivation) 적용 시킨 날짜/시간 value = null

[197] 9.프로파일 삭제(Profile Deletion) 적용 시킨 날짜/시간 value = null

[198] 이 경우는 1.프로파일 잠금 정책 적용 여부 value = true 일지라도 우선순위가 높은 3.프로파일 비활성화 적용 금지 여부 value = true, 4.프로파일 삭제 적용 금지 여부 value = true 값이 True이기 때문에 3, 4번의 정책에 의해 적용이 된다. 이 의미는 MNO1의 오퍼레이셔널 프로파일은 어떤 경우에도 비활성화/삭제될 수 없다는 것을 의미한다.

[199] Use case1)

[200] 가입자가 통신사/제조사 보조금이 지원되어 약정이 있는 상태인 경우 MNO1이 잠금(비활성화/삭제) 적용 금지를 시킬 수 있다. 또한 해당 단말의 도난신고를 받았을 경우 MNO1이 동일한 조치를 취할 수 있다.

[201] Use case2)

[202] 도난된 단말을 주었거나, 보조금이 해제되지 않은 단말을 양도하기 위해 MNO1에서 MNO2로 가입 변경을 요청했으면 SM(Subscription Manager)는 MNO1의 PCF Rule을 check하여 3번 4번의 값이 true를 확인하고 MNO2 오퍼레이셔널 프로파일을 로딩 하지 않고, MNO1, MNO2에게 통보(notification)를 한다.

[203] 이상의 본 발명을 이용하면, MNO의 PCF 규칙에 따라 오퍼레이셔널 프로파일의 잠금 상태를 알 수 있으며, 이를 통해서 오퍼레이셔널 프로파일의 잠금 상태에 따라 원격의 엔티티(SM, controlling authority, 혹은 대표 MNO)가 수행(비활성화, 삭제, 혹은 삭제/비활성화 불가)를 수행함으로써, eUICC 프로파일의 적절한 관리가 가능하다는 효과가 있다.

[204] 이상에서는, eUICC 내부의 프로파일에 대한 로딩, 활성화, 비활성화, 삭제 등을 PCF 규칙에 따라 원격의 외부 엔티티에서 수행하는 것과 관련된 각종 제어를 수행함으로써, eUICC의 상태를 관리하는 방법을 설명하였다.

[205] 전술한 바와 같은 본 발명의 일 실시예에 따르면, eUICC는 eUICC의 상태가 잠금(Lock)인지 열림(Unlock)인지를 제어하기 위한 PCF 규칙을 강제하는(Enforcing) 것을 지원할 수 있다.

[206] 또한, 전술한 바와 같이, 본 발명의 실시예에 따르면, eUICC에 대한 잠금 만료 시간(Lock Expiration Time)을 제어하는 PCF 규칙을 강제하는 메커니즘을 제공한다.

[207] 또한, 본 발명의 실시예에 따르면, 원격으로, eUICC(또는 eUICC 내부의 프로파일)가 잠금이 되는 상태(Locked state)로 진입하는 것을 제공해주는 권한이 부여된 메커니즘(Authorized mechanism)을 제공한다.

[208] 또한, 본 발명의 실시예에 따르면, 원격으로, eUICC(또는 eUICC 내부의 프로파일)가 잠금이 되는 상태(Locked state)를 벗어나도록 허락해주는 것을 제공해주는 권한이 부여된 메커니즘(Authorized mechanism)을 제공한다.

[209] 아래에서는, 이상에서 설명한 본 발명의 일 실시예에 따른 eUICC의 상태 관리 방법과 이를 위한 eUICC에 대하여, 도 8 내지 도 10을 참조하여 다시 한번 간략하게 정리하여 설명한다.

[210] 도 8은 본 발명의 일 실시예에 의한 eUICC의 상태 관리 방법에 대한 흐름도이다.

[211] 도 8을 참조하면, 본 발명의 일 실시예에 의한 MNO 및 SM과 연동 되어 있는 eUICC의 상태 관리 방법은, eUICC가 파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 프로파일을 저장하는 단계(S800)와, eUICC가 eUICC의 상태가 잠금(Lock)이 되어야 하는지 열림(Unlock)이 되어야 하는지를 제어하는 PCF 규칙(Policy Control Function Rule)을 강제하는(enforcing) 것을 지원하는 단계(S802) 등을 포함한다.

[212] 도 9는 본 발명의 일 실시예에 의한 eUICC에 대한 블록도이다.

[213] 도 9를 참조하면, 본 발명의 일 실시예에 의한 eUICC는, 파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 프로파일을 저장하는 프로파일 저장부(910)와, eUICC의 상태가 잠금(Lock)이 되어야 하는지 열림(Unlock)이 되어야 하는지를 제어하는데 참조 되는 PCF 규칙을 저장하는 PCF 규칙 저장부(920)와, PCF 규칙에 따라, eUICC의 상태가 잠금(Lock)이 되어야 하는지 열림(Unlock)이 되어야 하는지를 제어하는 eUICC 상태 제어부(930) 등을 포함한다.

[214] 전술한 바와 같이, eUICC는, 파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 형태로서 프로비저닝(Provisioning) 되거나 존재하는 프로파일을 포함하고, eUICC의 상태가 잠금(Lock)이 되어야 하는지 열림(Unlock)이 되어야 하는지를 제어하는 PCF 규칙(Policy Control Function Rule)을 강제하는(enforcing) 것을 지원한다.

[215] 전술한 바와 같이, eUICC의 상태 관리는, PCF 규칙의 설정 및 참조 등을 통해 이루질 수 있다. 이에, 아래에서는, PCF 규칙에 대하여 더욱 상세하게 설명한다.

[216] PCF 규칙은, 권한이 있는 외부 엔티티 중 하나 이상에 의해 설정된다. 여기서, 외부 엔티티는, 일 예로, MNO(Mobile Network Operator), CA(Controlling Authority) 및 SM(Subscription Manager) 등 중 하나 이상을 포함할 수 있다.

[217] 이러한 PCF 규칙은 각 프로파일마다 대응되어 설정될 수 있다. 여기서, 프로파일은, 일 예로, 오퍼레이셔널 프로파일(Operational Profile) 또는 프로비저닝 프로파일(Provisioning Profile) 등 일 수 있다.

[218] 또한, 이러한 PCF 규칙은, 모든 외부 엔티티들이 접근할 수 있는 내용(정보), 권한이 있는 외부 엔티티만이 접근할 수 있는 내용(정보), 외부 엔티티 중 프로파일 오너(Owner) 만 접근할 수 있는 내용(정보)으로 나뉠 수 있다.

[219] 이러한 PCF 규칙은, 프로파일의 잠금과 관련하여 여러 가지 정보(내용 또는 파라미터)를 포함할 수 있다.

[220] PCF 규칙은, eUICC 내부의 프로파일의 비활성화(Deactivation) 및 삭제(Deletion) 등 중 하나 이상이 가능한지를 설정하기 위한 프로파일 잠금 정책 적용 여부 정보(Profile Lock Policy 적용 여부 value)를 포함할 수 있다.

[221] 또한, PCF 규칙은, eUICC 내부의 프로파일의 비활성화 상태 여부를 나타내기 위한 프로파일 비활성화 여부 정보(Profile Deactivation 상태 여부 value)을 더 포함할 수 있다.

[222] 또한, PCF 규칙은, eUICC 내부의 프로파일이 비활성화된 이후 삭제되었는지를 나타내기 위한 프로파일 삭제 여부 정보Profile Deactivation 후에 Deletion 되었는지 여부 value)를 더 포함할 수 있다.

[223] 위에서 언급한 프로파일 잠금 정책 적용 여부 정보가 프로파일의 비활성화(Deactivation) 또는 삭제(Deletion)가 가능하다는 것을 나타내는 값(True)으로 설정되는 경우에, 프로파일 비활성화 여부 정보가 프로파일이 비활성화되었다는 것을 나타내는 값(True)으로 설정되고, 프로파일 삭제 여부 정보가 프로파일이 비활성화된 이후 삭제되었다는 것을 나타내는 값(True)으로 설정될 수 있다.

[224] 또한, PCF 규칙은, eUICC 내부의 프로파일의 비활성화를 적용시킨 날짜 및 시간 값이 설정되는 프로파일 비활성화 날짜/시간 정보와, eUICC 내부의 프로파일의 삭제를 적용시킨 날짜 및 시간 값이 설정되는 프로파일 삭제 날짜/시간 정보 등을 더 포함할 수 있다.

[225] 위에서 언급한 프로파일 잠금 정책 적용 여부 정보, 프로파일 비활성화 여부 정보, 프로파일 삭제 여부 정보, 프로파일 비활성화 날짜/시간 정보 및 프로파일 삭제 날짜/시간 정보는, 권한이 있는 외부 엔티티 모두에 의해 읽기(Read) 또는 갱신(Update) 가능하다.

[226] 한편, PCF 규칙은, eUICC 내부의 프로파일의 비활성화 적용 금지 여부를 설정하기 위한 프로파일 비활성 적용 금지 여부 정보(Profile Deactivation 적용 금지 여부 value)를 더 포함할 수 있다.

[227] 또한, PCF 규칙은, eUICC 내부의 프로파일의 삭제 적용 금지 여부를 설정하기 위한 프로파일 삭제 적용 금지 여부 정보(Profile Deletion 적용 금지 여부 value)을 더 포함할 수 있다.

[228] 위에서 언급한 프로파일 비활성 적용 금지 여부 정보 및 프로파일 삭제 적용 금지 여부 정보는, 프로파일 잠금 정책 적용 여부 정보가 설정된 값과 무관하게, 설정이 가능하다.

[229] 가령, 프로파일 잠금 정책 적용 여부 정보의 설정 값이 프로파일의 비활성화

및/또는 삭제가 가능하도록 설정된 값(True)이라고 하더라도, 프로파일 비활성 적용 금지 여부 정보 및/또는 프로파일 삭제 적용 금지 여부가 True로 설정되어 있다면, 프로파일의 비활성화 및/또는 삭제가 불가능하다.

[230] 즉, 프로파일의 비활성 또는 삭제 시, PCF 규칙이 참조될 때, 프로파일 비활성 적용 금지 여부 정보 및 프로파일 삭제 적용 금지 여부 정보가 프로파일 잠금 정책 적용 여부 정보보다 더 우선적으로 참조 또는 적용될 수 있다.

[231] 또한, PCF 규칙은, 프로파일 비활성 적용 금지 여부 정보가 True(프로파일의 비활성 적용이 금지되었다는 것을 나타내는 설정 값)로 설정됨으로써 프로파일의 비활성화 적용을 금지한 날짜 및 시간 값이 설정되는 프로파일 비활성화 적용 금지 날짜/시간 정보와, 프로파일 삭제 적용 금지 여부 정보가 True(프로파일의 삭제 적용이 금지되었다는 것을 나타내는 설정 값)로 설정됨으로써 프로파일의 삭제 적용을 금지한 날짜 및 시간 값이 설정되는 프로파일 삭제 적용 금지 날짜/시간 정보(value 7)를 더 포함할 수 있다.

[232] 위에서 언급한 프로파일 비활성 적용 금지 여부 정보 및 프로파일 삭제 적용 금지 여부 정보는, 권한이 있는 외부 엔티티(예: MNO, CA, SM 등) 모두에 의해 읽기(Read)가 가능하고, 권한이 있는 외부 엔티티 중 프로파일을 프로비저닝 한 외부 엔티티(예: MNO) 또는 특정 외부 엔티티(예: 특정 MNO)에 의해서만 갱신(Update)이 가능하다.

[233] 한편, 위에서 언급한 프로파일 비활성화 적용 금지 날짜/시간 정보 및 상기 프로파일 삭제 적용 금지 날짜/시간 정보는, 권한이 있는 외부 엔티티 모두에 의해 읽기(Read) 또는 갱신(Update)이 가능하다.

[234] 한편, 본 발명의 일 실시예에 따른 eUICC는, eUICC(eUICC 내부의 프로파일)의 잠금 만료 시간을 제어하는 PCF 규칙을 강제하는 것을 지원할 수 있다.

[235] 이하에서는, MNO 등 외부 엔티티 관점에서 eUICC의 상태 관리 방법에 대하여 설명한다.

[236] 도 10은 본 발명의 일 실시예에 의한 eUICC의 상태 관리 방법에 대한 다른 흐름도이다.

[237] 도 10을 참조하면, 본 발명의 일 실시예에 따른 MNO 및 SM 등과 연동 되어 있는 eUICC의 상태 관리 방법은, 권한이 있는 외부 엔티티가 eUICC에 로딩 된 제1 MNO의 프로파일의 잠금과 관련된 eUICC 내 PCF 규칙을 설정하는 단계(S1000)와, 권한이 있는 외부 엔티티가 PCF 규칙에 따라 eUICC에 로딩 된 제1 MNO의 프로파일에 대한 활성화, 비활성화, 삭제 및 갱신 등 중에서 하나 이상을 수행하는 것과 관련된 제1 MNO의 프로파일에 대한 잠금 상태를 제어하는 단계(S1002) 등을 포함한다.

[238] eUICC의 상태 관리 방법의 일 예로서, 전술한 S1000 단계에서, 제1 MNO가 권한이 있는 외부 엔티티에 의해 제1 MNO의 프로파일이 잠금 가능한 상태가 되도록 PCF 규칙을 설정하는 경우, S1002 단계에서, 가입자가 계약 위반, 가입 해제 등의 사유로, 휴지기(Dormant) 상태 또는 가입 해제 상태 등에 대한 요청이

있으면, 권한이 있는 외부 엔티티 중 제1 MNO는, PCF 규칙에 따라 제1 MNO의 프로파일을 비활성화 또는 삭제하고 PCF 규칙에서 제1 MNO의 프로파일의 비활성화 또는 삭제와 관련된 정보를 변경 설정할 수 있다.

[239] eUICC의 상태 관리 방법의 다른 예로서, 전술한 S1000 단계에서, 제1 MNO가 권한이 있는 외부 엔티티에 의해 제1 MNO의 프로파일이 잠금 가능한 상태가 되도록 PCF 규칙을 설정하는 경우, S1002 단계에서, 제1 MNO에서 제2 MNO로의 MNO 변경 요청 등이 있으면, 권한이 있는 외부 엔티티 중 SM은, 제1 MNO의 프로파일을 비활성화시키고 PCF 규칙에서 제1 MNO의 프로파일의 비활성화와 관련된 정보를 변경 설명하며, 제2 MNO의 로딩된 프로파일을 활성화시킬 수 있다. 이후에, 정책에 따라 혹은 MNO 서비스 정책에 따라 제1 MNO의 오퍼레이셔널 프로파일(operational profile)을 삭제(Deletion)을 시킬 수도 있고 비활성화(Inactive) 상태로 유지시킬 수도 있다.

[240] eUICC의 상태 관리 방법의 또 다른 예로서, 전술한 S1000 단계에서, 권한이 있는 외부 엔티티 중 제1 MNO는, 가입자가 통신사/제조사 보조금 지원에 따라 약정이 있는 상태인 경우 또는 해당 단말의 도난신고를 받았을 경우, 가입 정보 또는 단말 도난 정보 등에 따라, 제1 MNO의 프로파일에 대한 비활성 및 삭제 적용이 금지되도록 PCF 규칙을 설정할 수 있다.

[241] 이와 같이, S1000 단계에서, 제1 MNO의 프로파일에 대한 비활성 및 삭제 적용이 금지되도록 PCF 규칙이 설정된 경우, S1002 단계에서, 도난된 단말을 습득했거나 보조금이 해제되지 않은 단말을 양도하기 위해 제1 MNO에서 제2 MNO로의 MNO 변경 요청이 있는 경우, 권한이 있는 외부 엔티티 중 SM은, 제1 MNO의 프로파일에 대한 PCF 규칙을 체크하여, 제1 MNO의 프로파일에 대한 비활성 및 삭제 적용이 금지되도록 PCF 규칙이 설정되어 있는지를 확인하고, 제2 MNO의 프로파일의 로딩을 제한하며, 제1 MNO 및 제2 MNO에게 알려줄 수 있다.

[242] 본 발명의 일 실시예에 따르면, 전술한 eUICC의 상태 관리 방법을 이용하여 통신 서비스를 제공하는 기기(Device)를 제공할 수 있다.

[243] 본 발명의 일 실시예에 따른 기기는, 도 7에 도시된 바와 같이, MNO(Mobile Network Operator) 및 SM(Subscription Manager) 등의 외부 엔티티들과 연동하여 통신 서비스를 제공한다.

[244] 도 7을 참조하면, 본 발명의 일 실시예에 따른 MNO(Mobile Network Operator)와 연동하여 통신 서비스를 제공하는 기기(Device)는, MNO, CA(Controlling Authority) 및 SM(Subscription Manager) 등 중 하나 이상의 외부 엔티티와 연동하고, 파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 형태로서 프로비저닝(Provisioning) 되거나 존재하는 프로파일을 포함하며, 상기 eUICC의 상태가 잠금 또는 열림이 되는지를 제어하는 PCF 규칙(Policy Control Function Rule)을 강제하는 것을 지원하는 eUICC와, eUICC 내부의 PCF 규칙의 일부를 읽어와 디스플레이하는 터미널 디스플레이(Terminal Display) 등을

포함한다.

[245] 전술한 PCF 규칙은, MNO, CA(Controlling Authority) 및 SM(Subscription Manager) 등의 권한이 있는 외부 엔티티 중 하나 이상에 의해 설정되고, 프로파일마다 설정될 수 있다. 여기서, 프로파일은, 일 예로, 오퍼레이셔널 프로파일(Operational Profile) 또는 프로비저닝 프로파일(Provisioning Profile) 등일 수 있다.

[246] 또한, 전술한 PCF 규칙은, 외부 엔티티 접근 가능 여부에 따라, 모든 외부 엔티티들이 접근할 수 있는 내용, 권한이 있는 외부 엔티티만이 접근할 수 있는 내용 및 외부 엔티티 중 프로파일 오너(Owner) 만 접근할 수 있는 내용으로 나뉠 수 있다.

[247] 또한, 전술한 PCF 규칙 중 터미널 디스플레이에 읽힐 수 있는 PCF 규칙은, 일 예로, 프로파일의 비활성화(Deactivation) 및 삭제(Deletion) 중 하나 이상이 가능한지를 설정하기 위한 프로파일 잠금 정책 적용 여부 정보를 포함할 수 있다.

[248] 본 명세서에서 기재된 PCF(Policy Control Function)는, 정책(Policy)을 이행(Implement)하기 위한 "정책 규칙(Policy Rule)"을 정의하거나 업데이트 하거나 삭제하는 등의 기능을 포함하여 의미한다.

[249] 또한, 본 명세서에서 기재된 PCF 규칙은, 정책을 이행하기 위해 요구되는 동작과 정책이 이행되기 위한 조건 등을 의미하는 "정책 규칙(Policy Rule)" 또는 "규칙(Rule)"이라고 부를 수도 있다.

[250] 또한, 본 명세서에서 기재된 PCF(Policy Control Function)는, 정책 규칙(PCF 규칙)의 정의/업데이트/삭제 기능을 의미하는 것뿐만 아니라, 정책을 이행(Implement)하기 위한 정책 규칙을 실행(Execution)하는 기능을 의미하는 정책 적용 기능(PEF: Policy Enforcement Function)를 포함하는 개념일 수도 있다.

[251] 또한, 본 명세서에서 기재된 PCF 규칙은, 정책을 이행하기 위해 요구되는 동작과 정책이 이행되기 위한 조건 등을 의미하는 "정책 규칙(Policy Rule)"이라고 할 수 있다.

[252] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시 예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

[253] CROSS-REFERENCE TO RELATED APPLICATION

[254] 본 특허출원은 2011년 11월 2일 한국에 출원한 특허출원번호 제 10-2011-0113479 호 및 2012년 11월 1일 한국에 출원한 특허출원번호 제

10-2012-0122797 호에 대해 미국 특허법 119(a)조 (35 U.S.C § 119(a))에 따라 우선권을 주장하며, 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다. 아울러, 본 특허출원은 미국 이외에 국가에 대해서도 위와 동일한 이유로 우선권을 주장하면 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다.

청구범위

[청구항 1] MNO(Mobile Network Operator) 및 SM(Subscription Manager)과 연동 되어 있는 eUICC(embedded Universal Integrated Circuit Card)로서,
파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 형태로서 프로비저닝(Provisioning) 되거나 존재하는 프로파일을 포함하고, 상기 eUICC의 상태가 잠금 또는 열림이 되는지를 제어하는 PCF 규칙(Policy Control Function Rule)을 강제하는 것을 지원하는 것을 특징으로 하는 eUICC.

[청구항 2] 제1항에 있어서,
상기 PCF 규칙은,
권한이 있는 외부 엔티티 중 하나 이상에 의해 설정되고, 상기 프로파일마다 설정되는 것을 특징으로 하는 eUICC.

[청구항 3] 제1항에 있어서,
상기 PCF 규칙은,
모든 외부 엔티티들이 접근할 수 있는 내용, 권한이 있는 외부 엔티티만이 접근할 수 있는 내용 및 외부 엔티티 중 프로파일 오너(Owner) 만 접근할 수 있는 내용으로 나뉘는 것을 특징으로 하는 eUICC.

[청구항 4] 제1항에 있어서,
상기 eUICC의 잠금 만료 시간을 제어하는 PCF 규칙을 강제하는 것을 지원하는 것을 특징으로 하는 eUICC.

[청구항 5] 제1항에 있어서,
상기 PCF 규칙은,
상기 프로파일의 비활성화(Deactivation) 및 삭제(Deletion) 중 하나 이상이 가능한지를 설정하기 위한 프로파일 잠금 정책 적용 여부 정보를 포함하는 것을 특징으로 하는 eUICC.

[청구항 6] 제5항에 있어서,
상기 PCF 규칙은,
상기 프로파일의 비활성화 상태 여부를 나타내기 위한 프로파일 비활성화 여부 정보; 및
상기 프로파일이 비활성화된 이후 삭제되었는지를 나타내기 위한 프로파일 삭제 여부 정보를 더 포함하는 것을 특징으로 하는 eUICC.

[청구항 7] 제6항에 있어서,
상기 PCF 규칙은,
상기 프로파일의 비활성화를 적용시킨 날짜 및 시간 값이

설정되는 프로파일 비활성화 날짜/시간 정보; 및
상기 프로파일의 삭제를 적용시킨 날짜 및 시간 값이 설정되는 프로파일 삭제 날짜/시간 정보를 더 포함하는 것을 특징으로 하는 eUICC.

[청구항 8] 제5항에 있어서,
상기 PCF 규칙은,
상기 프로파일의 비활성화 적용 금지 여부를 설정하기 위한 프로파일 비활성 적용 금지 여부 정보; 및
상기 프로파일의 삭제 적용 금지 여부를 설정하기 위한 프로파일 삭제 적용 금지 여부 정보를 더 포함하는 것을 특징으로 하는 eUICC.

[청구항 9] 제8항에 있어서,
상기 PCF 규칙은,
상기 프로파일의 비활성화 적용을 금지한 날짜 및 시간 값이 설정되는 프로파일 비활성화 적용 금지 날짜/시간 정보; 및
상기 프로파일의 삭제 적용을 금지한 날짜 및 시간 값이 설정되는 프로파일 삭제 적용 금지 날짜/시간 정보를 더 포함하는 것을 특징으로 하는 eUICC.

[청구항 10] MNO(Mobile Network Operator) 및 SM(Subscription Manager)과 연동 되어 있는 eUICC(embedded Universal Integrated Circuit Card)의 상태 관리 방법으로서,
상기 eUICC가 파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 프로파일을 저장하는 단계; 및
상기 eUICC가 상기 eUICC의 상태가 잠금(Lock) 또는 열림(Unlock)이 되는지를 제어하는 PCF 규칙(Policy Control Function Rule)을 강제하는(enforcing) 것을 지원하는 단계를 포함하는 eUICC의 상태 관리 방법.

[청구항 11] MNO(Mobile Network Operator) 및 SM(Subscription Manager)과 연동 되어 있는 eUICC(embedded Universal Integrated Circuit Card)로서,
파일 구조, 데이터 및 애플리케이션 중 하나 또는 둘 이상이 조합된 프로파일을 저장하는 프로파일 저장부;
상기 eUICC의 상태가 잠금 또는 열림이 되는지를 제어하는데 참조 되는 PCF 규칙(Policy Control Function Rule)을 저장하는 PCF 규칙 저장부; 및
상기 PCF 규칙에 따라, 상기 eUICC의 상태가 잠금 또는 열림이 되는지를 제어하는 eUICC 상태 제어부를 포함하는 eUICC.

[청구항 12] MNO(Mobile Network Operator) 및 SM(Subscription Manager)과

연동 되어 있는 eUICC(embedded Universal Integrated Circuit Card)의 상태 관리 방법으로서,
권한이 있는 외부 엔티티가 상기 eUICC에 로딩 된 MNO의 프로파일의 잠금과 관련된 상기 eUICC 내 PCF 규칙(Policy Control Function Rule)을 설정하는 단계; 및
상기 권한이 있는 외부 엔티티가 상기 PCF 규칙에 따라 상기 eUICC에 로딩 된 상기 MNO의 프로파일에 대한 잠금 상태를 제어하는 단계를 포함하는 eUICC의 상태 관리 방법.

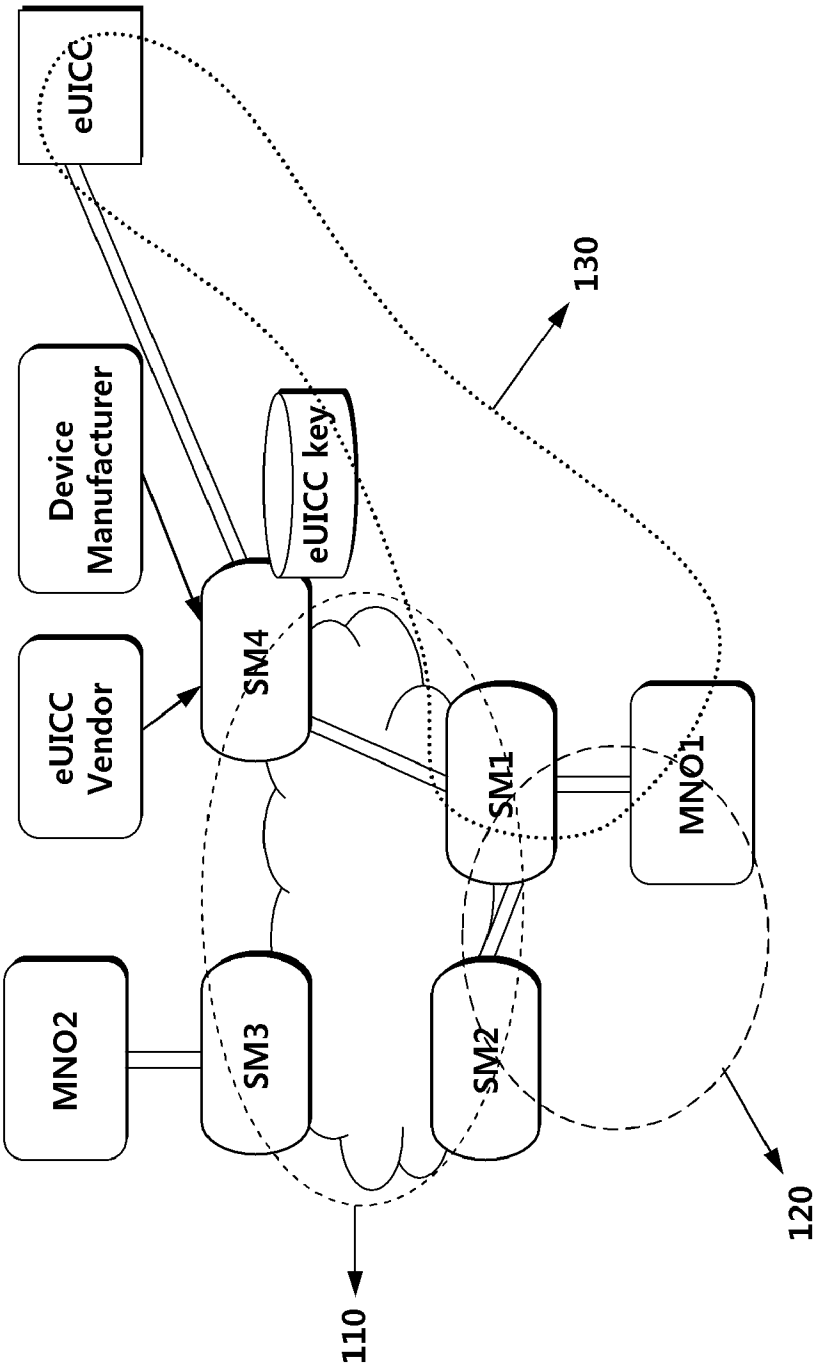
[청구항 13] 제12항에 있어서,
상기 설정하는 단계에서, 상기 MNO가 상기 권한이 있는 외부 엔티티에 의해 상기 MNO의 프로파일이 잠금 가능한 상태가 되도록 상기 PCF 규칙을 설정하는 경우,
상기 수행하는 단계는,
휴지기 상태 또는 가입 해제 상태에 대한 요청이 있을 경우, 상기 권한이 있는 외부 엔티티 중 상기 MNO는, 상기 PCF 규칙에 따라 상기 MNO의 프로파일을 비활성화 또는 삭제하고 상기 PCF 규칙에서 상기 MNO의 프로파일의 비활성화 또는 삭제와 관련된 정보를 변경 설정하고,
상기 MNO에서 다른 MNO로의 MNO 변경 요청이 있을 경우, 상기 권한이 있는 외부 엔티티 중 상기 SM은, 상기 MNO의 프로파일을 비활성화시키고 상기 PCF 규칙에서 상기 MNO의 프로파일의 비활성화와 관련된 정보를 변경 설명하며, 상기 다른 MNO의 로딩된 프로파일을 활성화시키는 것을 특징으로 하는 eUICC의 상태 관리 방법.

[청구항 14] 제12항에 있어서,
상기 설정하는 단계에서, 상기 권한이 있는 외부 엔티티 중 상기 MNO는,
가입 정보 또는 단말 도난 정보에 따라, 상기 MNO의 프로파일에 대한 비활성 및 삭제 적용이 금지되도록 상기 PCF 규칙을 설정하는 것을 특징으로 하는 eUICC의 상태 관리 방법.

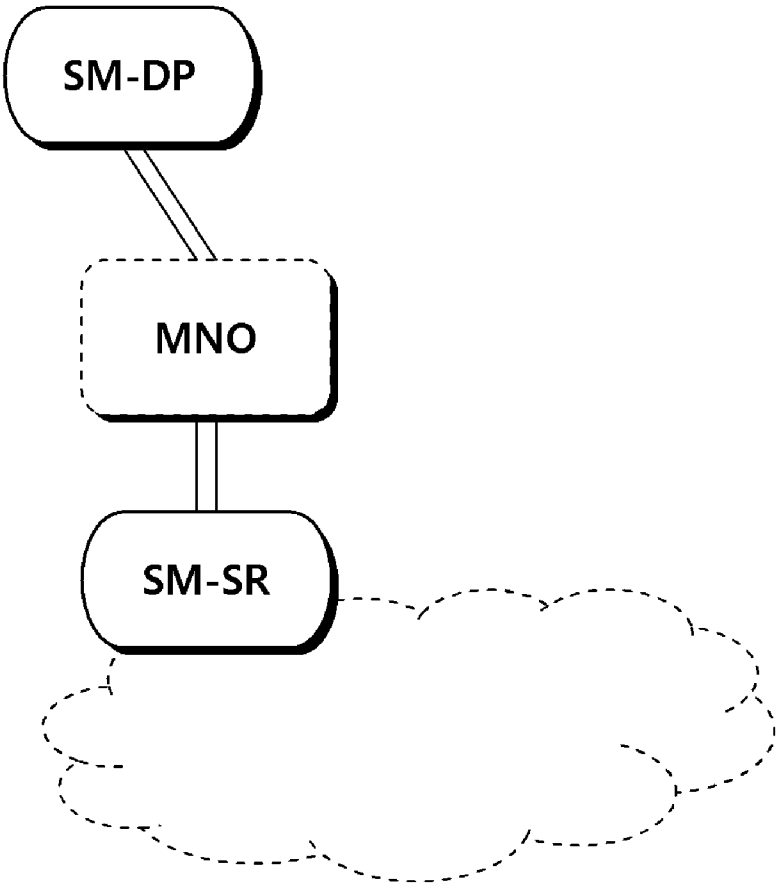
[청구항 15] 제14항에 있어서,
상기 수행하는 단계에서,
상기 MNO에서 다른 MNO로의 MNO 변경 요청이 있는 경우, 상기 권한이 있는 외부 엔티티 중 상기 SM은,
상기 MNO의 프로파일에 대한 상기 PCF 규칙을 체크하여, 상기 MNO의 프로파일에 대한 비활성 및 삭제 적용이 금지되도록 상기 PCF 규칙이 설정되어 있는지를 확인하고, 상기 다른 MNO의 프로파일의 로딩을 제한하며, 상기 MNO 및 상기 다른 MNO에게

알려주는 것을 특징으로 하는 eUICC의 상태 관리 방법.

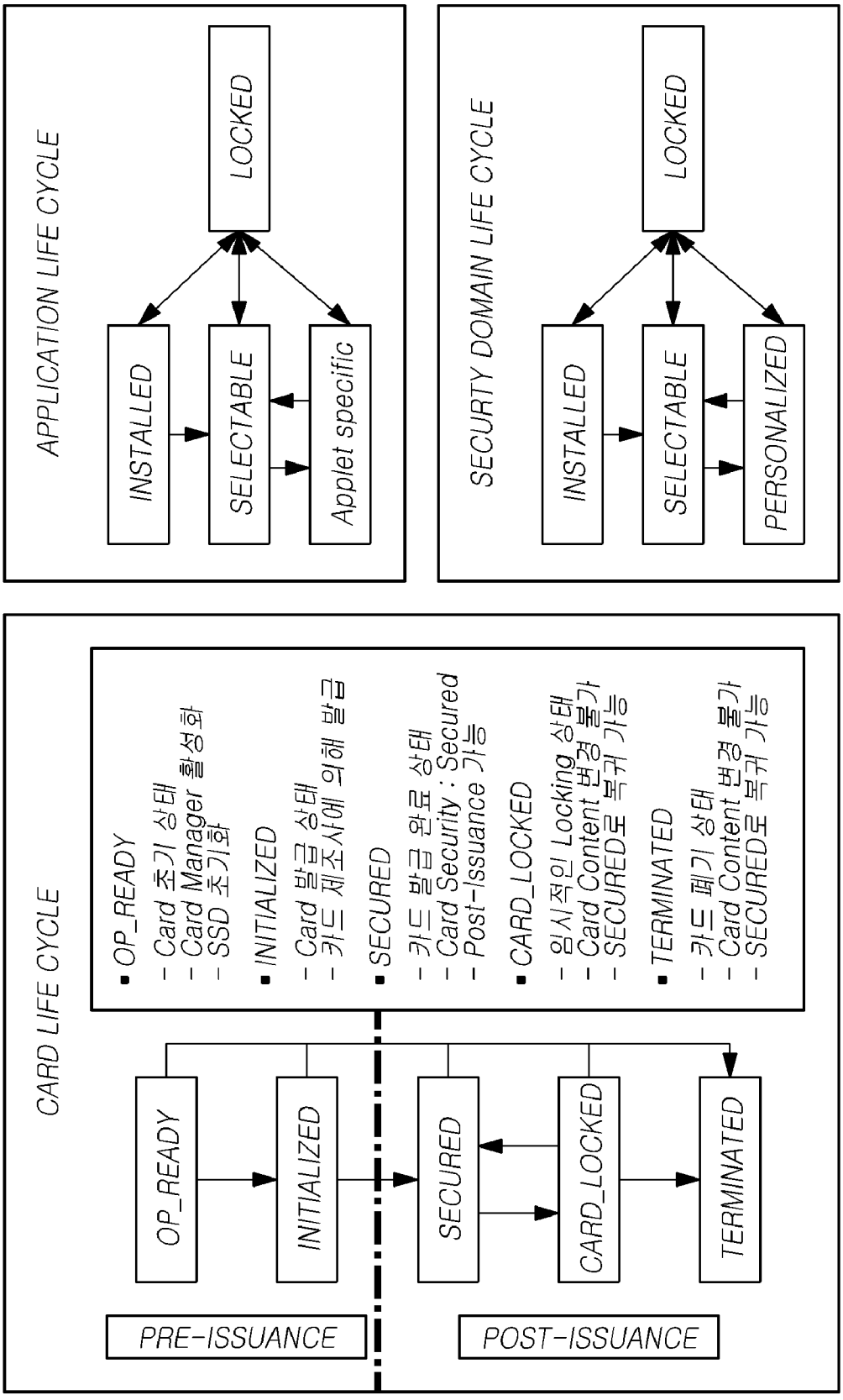
[Fig. 1]


eUICC
Device Manufacturer
eUICC Vendor
eUICC key
SM4
SM1
MNO1
MNO2
SM3
SM2
130
120
110

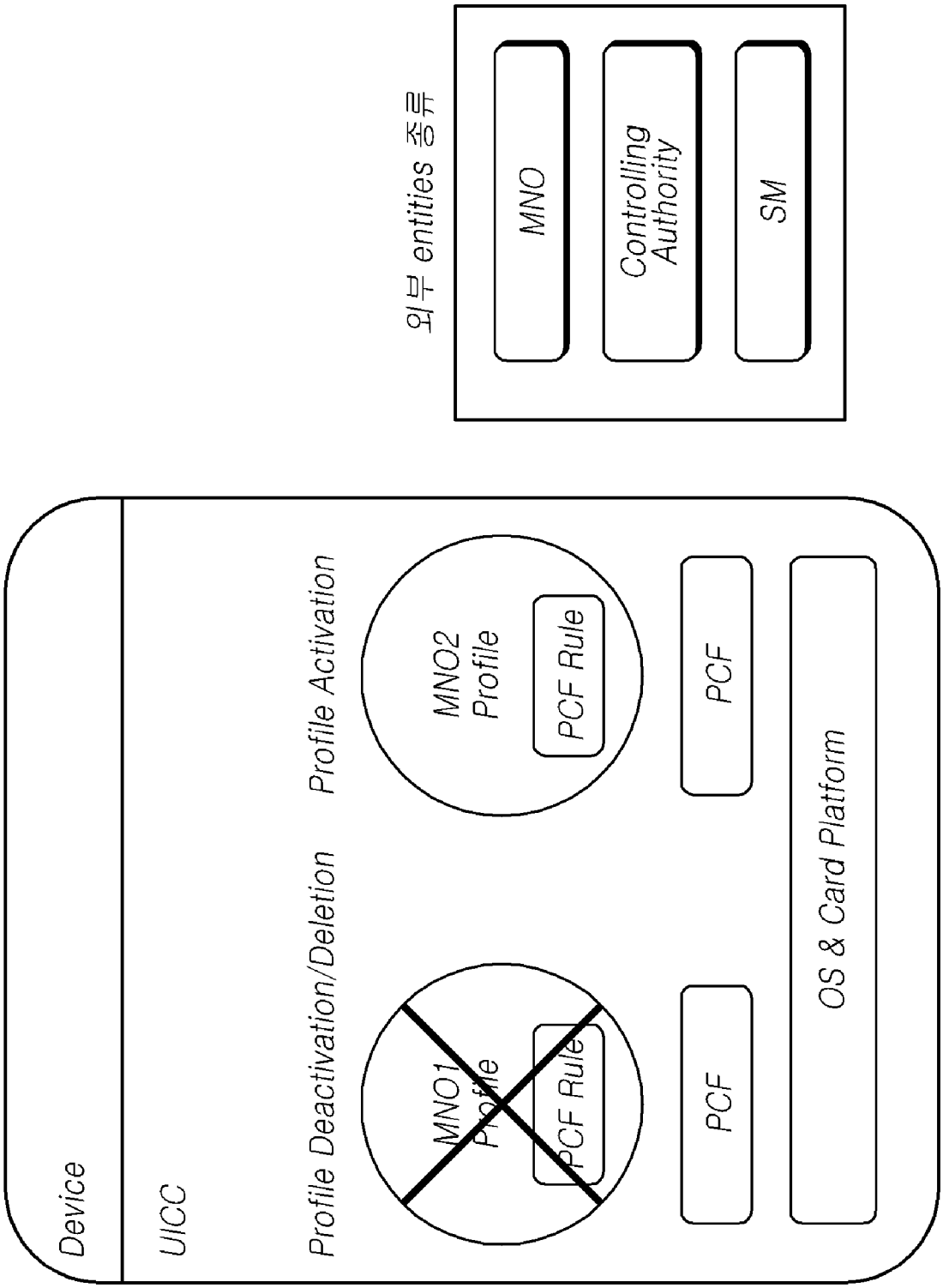
[Fig. 2]



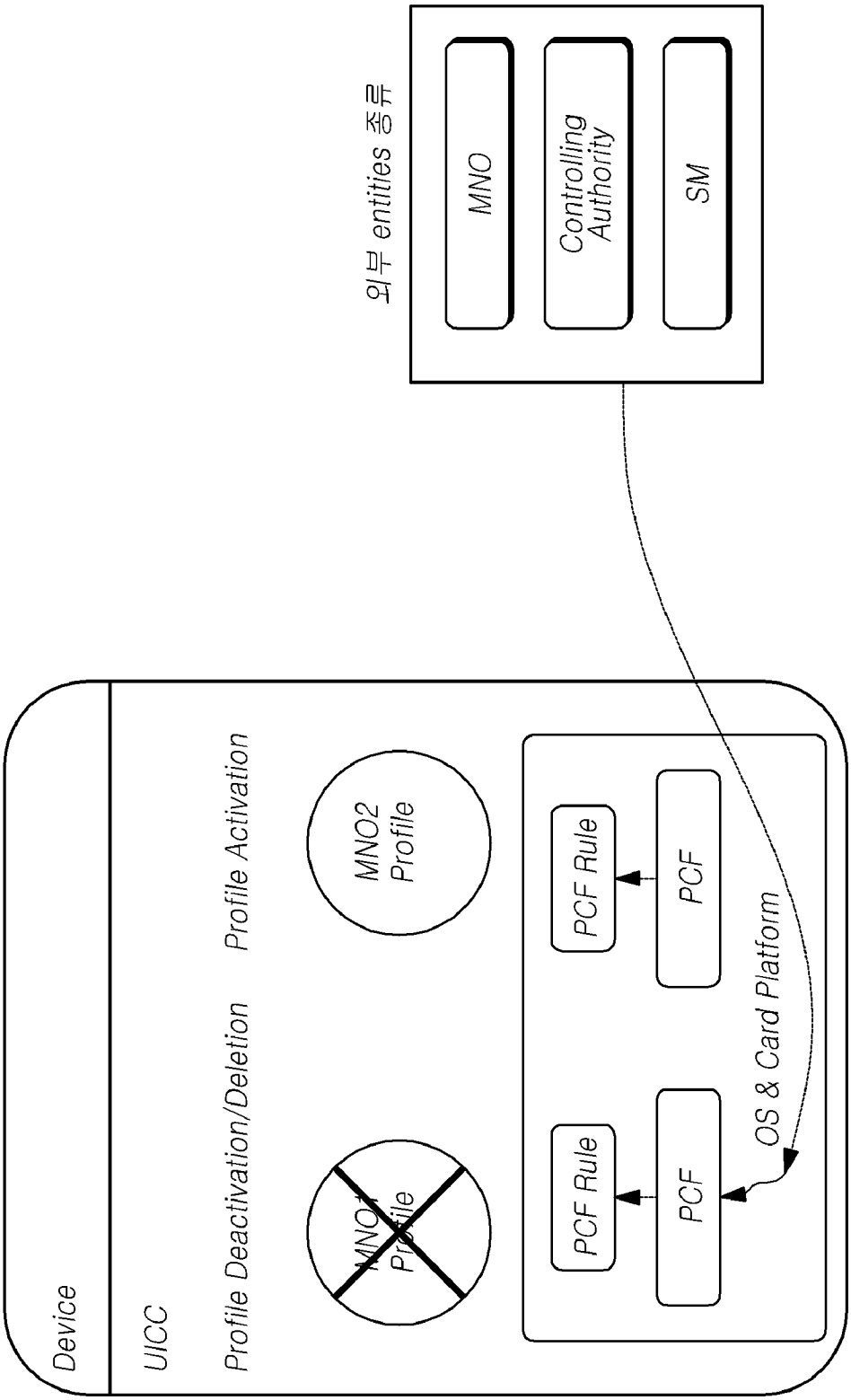
[Fig. 3]


APPLICATION LIFE CYCLE
LOCKED
INSTALLED
SELECTABLE
Applet specific
SECURTY DOMAIN LIFE CYCLE
LOCKED
INSTALLED
SELECTABLE
PERSONALIZED
CARD LIFE CYCLE
▪ OP_READY
- Card 초기 상태
- Card Manager 활성화
- SSD 초기화
▪ INITIALIZED
- Card 발급 상태
- 카드 제조사에 의해 발급
▪ SECURED
- 카드 발급 완료 상태
- Card Security : Secured
- Post-Issuance 가능
▪ CARD_LOCKED
- 임시적인 Locking 상태
- Card Content 변경 불가
- SECURED로 복귀 가능
▪ TERMINATED
- 카드 폐기 상태
- Card Content 변경 불가
- SECURED로 복귀 가능
OP_READY
INITIALIZED
SECURED
CARD_LOCKED
TERMINATED
PRE-ISSUANCE
POST-ISSUANCE

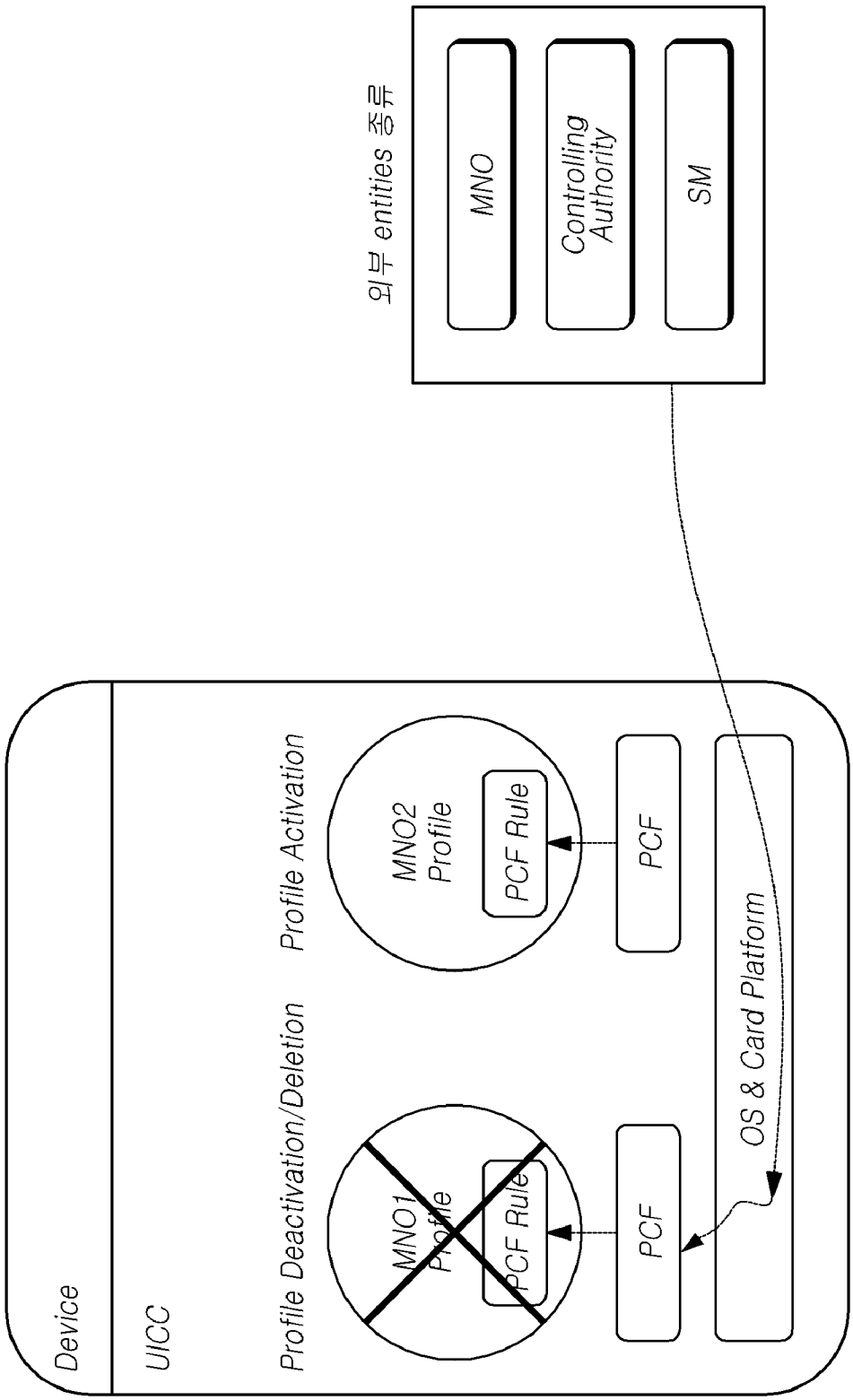
[Fig. 4]


외부 entities 종류
MNO
Controlling Authority
SM
Device
UICC
Profile Deactivation/Deletion
Profile Activation
MNO1 Profile
PCF Rule
MNO2 Profile
PCF Rule
PCF
PCF
OS & Card Platform

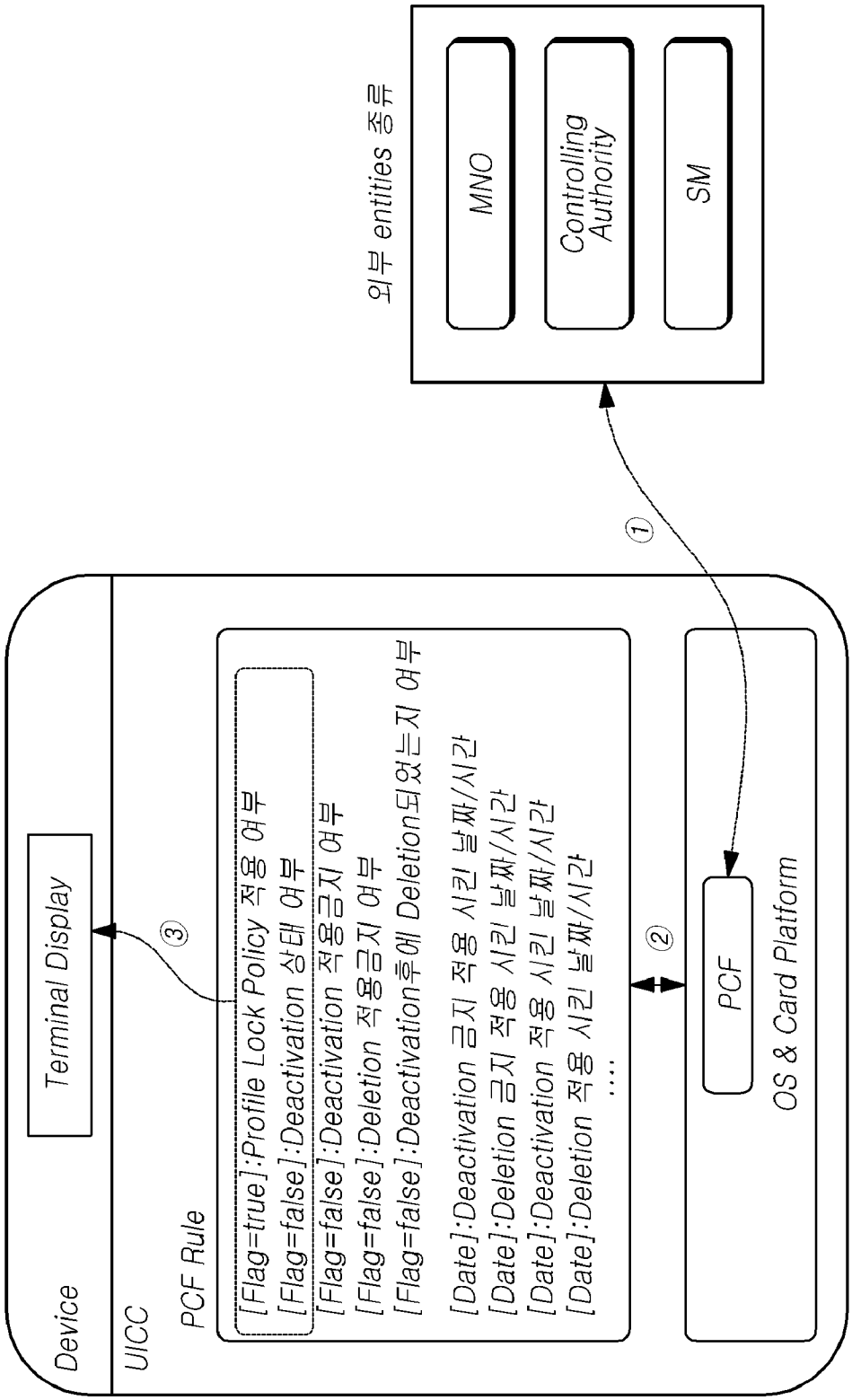
[Fig. 5]


외부 entities 종류
MNO
Controlling Authority
SM
Device
UICC
Profile Deactivation/Deletion
Profile Activation
MNO1 Profile
MNO2 Profile
PCF Rule
PCF
PCF Rule
PCF
OS & Card Platform

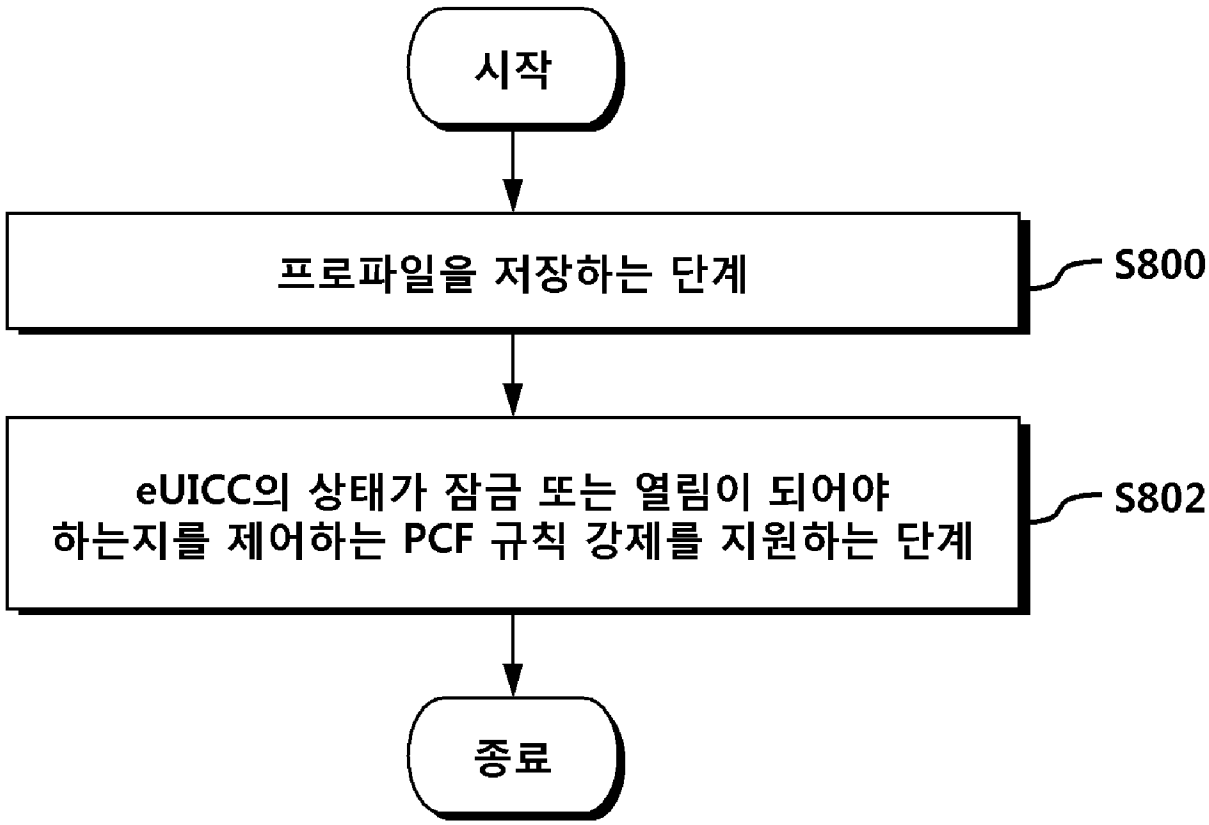
[Fig. 6]


외부 entities 종류
MNO
Controlling Authority
SM
Device
UICC
Profile Deactivation/Deletion
Profile Activation
MNO1 Profile
PCF Rule
MNO2 Profile
PCF Rule
PCF
PCF
OS & Card Platform

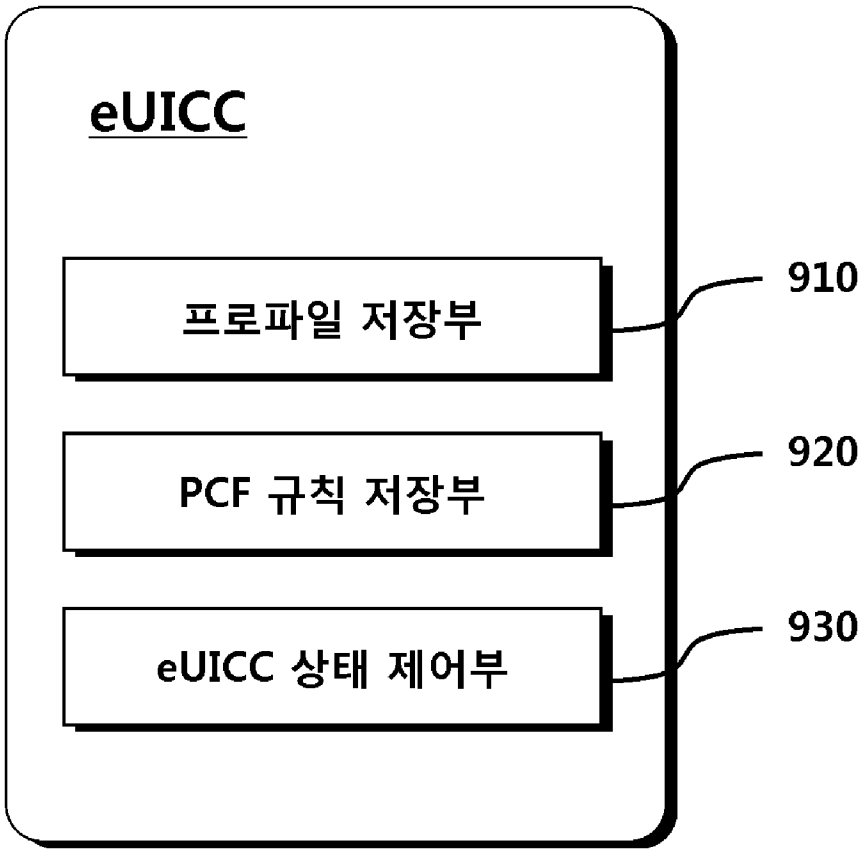
[Fig. 7]


외부 entities 종류
MNO
Controlling Authority
SM
①
Device
Terminal Display
③
UICC
PCF Rule
[Flag=true]:Profile Lock Policy 적용 여부
[Flag=false]:Deactivation 상태 여부
[Flag=false]:Deactivation 적용금지 여부
[Flag=false]:Deletion 적용금지 여부
[Flag=false]:Deactivation후에 Deletion되었는지 여부
[Date]:Deactivation 금지 적용 시킨 날짜/시간
[Date]:Deletion 금지 적용 시킨 날짜/시간
[Date]:Deactivation 적용 시킨 날짜/시간
[Date]:Deletion 적용 시킨 날짜/시간
....
②
PCF
OS & Card Platform

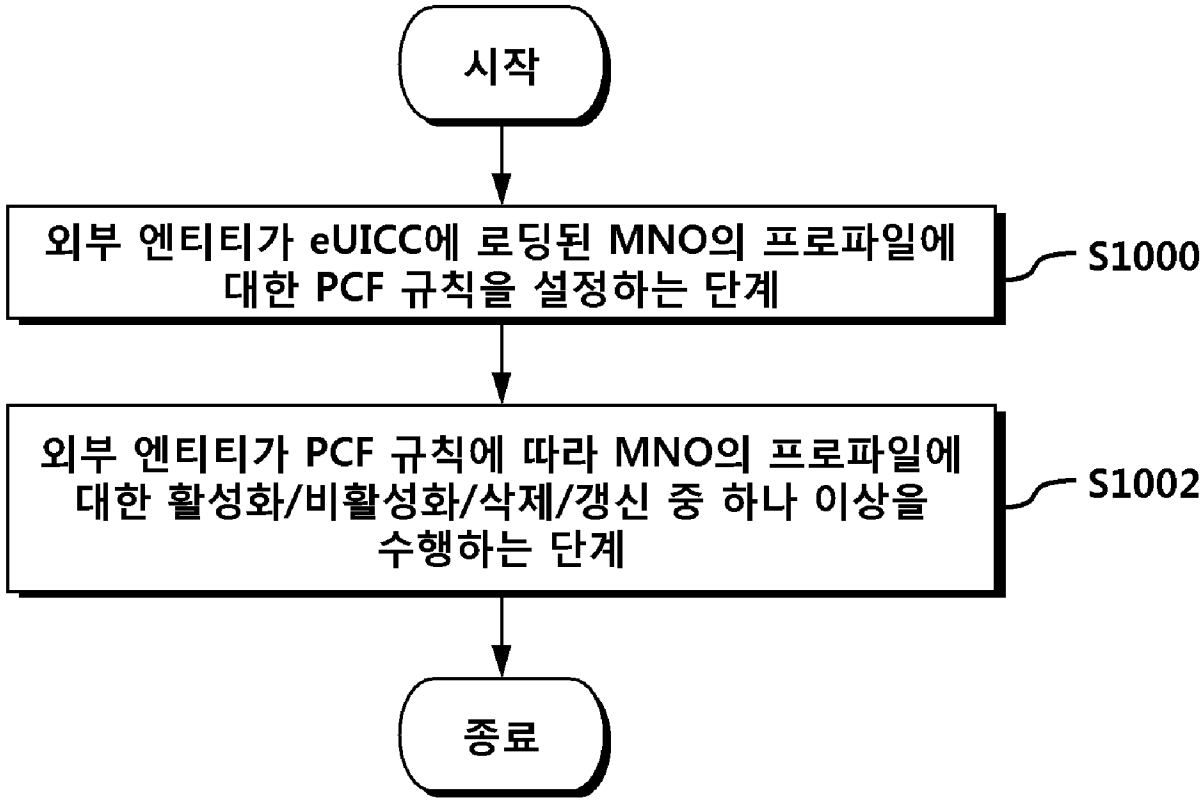
[Fig. 8]


시작
프로파일을 저장하는 단계
S800
eUICC의 상태가 잠금 또는 열림이 되어야 하는지를 제어하는 PCF 규칙 강제를 지원하는 단계
S802
종료

[Fig. 9]


eUICC
프로파일 저장부
910
PCF 규칙 저장부
920
eUICC 상태 제어부
930

[Fig. 10]


시작
외부 엔티티가 eUICC에 로딩된 MNO의 프로파일에 대한 PCF 규칙을 설정하는 단계
S1000
외부 엔티티가 PCF 규칙에 따라 MNO의 프로파일에 대한 활성화/비활성화/삭제/갱신 중 하나 이상을 수행하는 단계
S1002
종료

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2012/009128

A. CLASSIFICATION OF SUBJECT MATTER

H04W 8/18(2009.01)i, H04W 12/00(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 8/18; H04W 92/08; H04W 8/30; H04W 8/02; H04L 9/32; G06K 17/00; H04B 5/02; H04W 8/24; H04B 1/40; H04W 12/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: MNO(Mobile Network Operator), SM(Subscription Manager), eUICC(embedded Universal Integrated Circuit Card), PCF(Policy Control Function Rule)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GSM Association, "Embedded SIM Task Force Requirements and Use Cases", Embedded SIM Task Force: Requirement & Use Cases, Ver 1.0, 21 February 2011 See sections 6.3 and 7.	1-15
A	KR 10-2010-0072112 A (KT CORPORATION) 30 June 2010 See abstract; paragraphs [0024]-[0032]; figure 1; and claims 1-2, 7-8.	1-15
A	KR 10-2005-0053920 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 10 June 2005 See abstract; page 3; figure 1; and claims 1-4.	1-15
A	KR 10-2009-0085319 A (KT TECH, INC.) 07 August 2009 See abstract; paragraphs [27]-[48]; figure 1; and claim 1.	1-15
A	KR 10-2011-0067062 A (HUAWEI DEVICE CO., LTD.) 20 June 2011 See abstract; paragraphs [0039]-[0047]; figure 4; and claim 1.	1-15
A	JP 2005-128746 A (SONY CO., LTD.) 19 May 2005 See abstract; paragraphs [0040]-[0051]; figure 2; claim 1.	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 FEBRUARY 2013 (27.02.2013)	**28 FEBRUARY 2013 (28.02.2013)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

International application No.
PCT/KR2012/009128

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2010-0072112 A	30.06.2010	KR 10-1042526 B1	20.06.2011
KR 10-2005-0053920 A	10.06.2005	KR 10-0564755 B1	27.03.2006
KR 10-2009-0085319 A	07.08.2009	NONE	
KR 10-2011-0067062 A	20.06.2011	CN 101772204 A	07.07.2010
		KR 10-1198191 B1	12.11.2012
		WO 2010-045839 A1	29.04.2010
JP 2005-128746 A	19.05.2005	CN 1871617 A	29.11.2006
		CN 1871617 B	22.06.2011
		EP 1684211 A1	26.07.2006
		EP 1684211 A4	14.03.2012
		HK 1097327 A1	18.11.2011
		JP 04539071 B2	08.09.2010
		US 2007-0026893 A1	01.02.2007
		US 7766237 B2	03.08.2010
		WO 2005-041119 A1	06.05.2005

국 제 조 사 보 고 서

국제출원번호
PCT/KR2012/009128

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 8/18(2009.01)i, H04W 12/00(2009.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04W 8/18; H04W 92/08; H04W 8/30; H04W 8/02; H04L 9/32; G06K 17/00; H04B 5/02; H04W 8/24; H04B 1/40; H04W 12/00

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: MNO(Mobile Network Operator), SM(Subscription Manager), eUICC(embedded Universal Integrated Circuit Card), PCF(Policy Control Function Rule)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	GSM Association, "Embedded SIM Task Force Requirements and Use Cases", Embedded SIM Task Force: Requirements & Use Cases, Ver 1.0, 2011.02.21 섹션 6.3 및 7 참조.	1-15
A	KR 10-2010-0072112 A (케이티 주식회사) 2010.06.30 요약; 단락 [0024]-[0032]; 도면 1; 및 청구항 1-2, 7-8 참조.	1-15
A	KR 10-2005-0053920 A (한국전자통신연구원) 2005.06.10 요약; 페이지 3; 도면 1; 및 청구항 1-4 참조.	1-15
A	KR 10-2009-0085319 A (케이티테크 주식회사) 2009.08.07 요약; 단락 [27]-[48]; 도면 1; 및 청구항 1 참조.	1-15
A	KR 10-2011-0067062 A (후아웨이 디바이스 컴퍼니 리미티드) 2011.06.20 요약; 단락 [0039]-[0047]; 도면 4; 및 청구항 1 참조.	1-15
A	JP 2005-128746 A (SONY CO., LTD.) 2005.05.19 요약; 단락 [0040]-[0051]; 도면 2; 청구항 1 참조.	1-15

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2013년 02월 27일 (27.02.2013)	**2013년 02월 28일 (28.02.2013)**

ISA/KR의 명칭 및 우편주소

팩스 번호 82-42-472-7140

심사관

김병성

전화번호 82-42-481-8403

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2012/009128

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2010-0072112 A	2010.06.30	KR 10-1042526 B1	2011.06.20
KR 10-2005-0053920 A	2005.06.10	KR 10-0564755 B1	2006.03.27
KR 10-2009-0085319 A	2009.08.07	없음	
KR 10-2011-0067062 A	2011.06.20	CN 101772204 A	2010.07.07
		KR 10-1198191 B1	2012.11.12
		WO 2010-045839 A1	2010.04.29
JP 2005-128746 A	2005.05.19	CN 1871617 A	2006.11.29
		CN 1871617 B	2011.06.22
		EP 1684211 A1	2006.07.26
		EP 1684211 A4	2012.03.14
		HK 1097327 A1	2011.11.18
		JP 04539071 B2	2010.09.08
		US 2007-0026893 A1	2007.02.01
		US 7766237 B2	2010.08.03
		WO 2005-041119 A1	2005.05.06