

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013년 3월 14일 (14.03.2013)



(10) 국제공개번호

WO 2013/036009 A1

(51) 국제특허분류:

H04W 12/04 (2009.01) H04W 8/18 (2009.01)
H04W 12/08 (2009.01)

(21) 국제출원번호:

PCT/KR2012/007062

(22) 국제출원일:

2012년 9월 4일 (04.09.2012)

(25) 출원언어:

한국어

(26) 공개언어:

한국어

(30) 우선권정보:

10-2011-0089639 2011년 9월 5일 (05.09.2011) KR
10-2011-0102428 2011년 10월 7일 (07.10.2011) KR

(71) 출원인(US을(를) 제외한 모든 지정국에 대하여): 주식회사 케이티(KT CORPORATION) [KR/KR]; 463-815 경기도 성남시 분당구 정자동 206, Gyeonggi-do (KR).

(72) 발명자: 겸

(75) 발명자/출원인(US에 한하여): 박재민(PARK, Jaemin) [KR/KR]; 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR). 이진형(LEE, Jinhyoung) [KR/KR]; 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR).

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

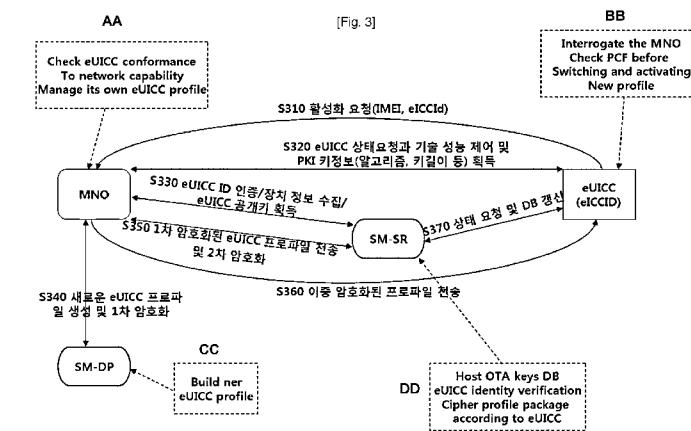
(81) 지정국(별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, 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, 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).

[다음 쪽 계속]

(54) Title: METHOD FOR MANAGING EMBEDDED UICC AND EMBEDDED UICC, MNO SYSTEM, PROVISION METHOD, AND METHOD FOR CHANGING MNO USING SAME

(54) 발명의 명칭: 내장 UICC의 키정보 관리방법 및 그를 이용한 내장 UICC, MNO 시스템, 프로비저닝 방법 및 MNO 변경 방법



- AA ... Check eUICC conformance To network capability Manage its own eUICC profile
BB ... Interrogate the MNO Check PCF before Switching and activating New profile
CC ... Build new eUICC profile
DD ... Host OTA keys DB eUICC identity verification Cipher profile package according to eUICC
S310 ... Activation request(IMEI, eICCID)
S320 ... eUICC status request, technology performance control, and acquisition of PKI key information(algorithm, key length etc)
S330 ... eUICC ID authentication/device information collection/eUICC publication key acquisition
S340 ... Generation of new eUICC profile and first encoding
S350 ... Transmission of first encoded eUICC profile and second encoding
S360 ... Transmission of dual encoded profile
S370 ... Status request and DB renewal

(57) Abstract: The present invention relates to profile access credentials used for encoding profiles in a system comprising a mobile network operator(MNO), a subscription manager (SM), an embedded UICC (eUICC) and the like, that is, a method for storing/managing an eUICC publication key and a corresponding secret or the like inside the eUICC. In addition, the invention also provides a method for transmitting information on profile access credentials inside the eUICC to external entities for encoding and the like.

(57) 요약서: 본 발명은 MNO(Mobile Network Operator), SM(Subscription Manager), eUICC(Embedded UICC) 등으로 구성된 시스템에서 프로파일의 암호화에 사용되는 프로파일 접근 크레덴셜(Profile Access Credentials), 즉 eUICC 공개키 및 그에 대응되는 비밀키 등을 eUICC 내부에 저장/관리하는 방안을 제공한다. 또한, eUICC 내부에 있는 프로파일 접근 크레덴셜에 대한 정보를 외부 엔터티로 전송하여 암호화 등에 이용할 수 있도록 하는 방안도 함께 제공한다.



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 키정보 관리방법 및 그를 이용한 내장 UICC, MNO 시스템, 프로비저닝 방법 및 MNO 변경 방법 기술분야

- [1] 본 발명은 내장 UICC(Embedded Universal Integrated Circuit Card; 이하 ‘eUICC’라 함)의 키정보 관리방법 및 그를 이용한 eUICC, MNO 시스템, 프로비저닝 방법 및 MNO 변경 방법, 특히 eUICC의 각종 프로파일을 관리할 수 있는 프로파일 접근 크레덴셜(Profile access credentials)인 eUICC 공개키 및 그에 대한 키정보를 관리하여 사용하는 방안에 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 제공에 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 이동통신 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 이동통신 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.

발명의 상세한 설명

기술적 과제

- [8] 본 발명은 eUICC의 프로파일 접근 크레덴셜에 대한 정보를 관리하기 위한 방법을 제공한다.
- [9] 본 발명의 다른 목적은 암호화된 프로파일을 복호화할 수 있는 프로파일 접근 크레덴셜로서의 eUICC 공개키에 대한 키정보를 관리하는 방법을 제공한다.
- [10] 본 발명의 다른 목적은 SM이 SM-SR(Secure Routing) 및 SM-DP(Data Preparation)으로 분리 구현되는 환경에서, eUICC의 키(Key)를 관리하는 방법을 제공하는 것이다.
- [11] 본 발명의 또 다른 목적은 SM이 SM-SR(Secure Routing) 및 SM-DP(Data Preparation)으로 분리 구현되는 환경에서, SM-SR이 보안 정보를 암/복호화할 수 있는 암호키(공개키 또는 그에 대응되는 비밀키 등)를 eUICC가 보유/관리하는 방법을 제공하는 것이다.
- [12] 본 발명의 다른 목적은 eUICC가 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)로의 접근에 사용되는 프로파일 접근 크레덴셜을 저장 및 관리하며, 프로파일 접근 크레덴셜에 대한 정보를 외부 엔터티에게 전송하는 방법을 제공한다.
- #### 과제 해결 수단
- [13] 본 발명의 일 실시에는, 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)에서, 상기 eUICC는 상기 MNO 시스템 또는 SM 등과 같은 외부 엔터티와 상태 및 능력 확인과정을 수행하며, 그 과정에서 eUICC는 자신의 상태 및 능력에 대한 정보로서 키생성 알고리즘, 키 길이, 키 생성방식 등의 정보를 포함하는 키정보를 제공하는 eUICC의 키정보 관리방법을 제공한다.
- [14] 본 발명의 또 다른 실시에는 통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 그와 연동된 내장 UICC(eUICC)를 포함하는 eUICC 시스템에서의 프로비저닝 방법으로서, 상기 MNO 시스템이 상기 eUICC로부터 프로파일을 암호화할 수 있는 eUICC 공개키에 대한 PKI 키정보를 수신하는 단계와, 상기 MNO 시스템 또는 상기 SM이 상기 프로파일을 상기 eUICC 공개키로 1차 암호화하는 단계와, 상기 MNO 시스템이 암호화된 상기 프로파일을 상기 eUICC로 전송하는 단계를

포함하는 프로비저닝 방법을 제공한다.

- [15] 본 발명의 다른 실시예는 통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 그와 연동된 내장 UICC(eUICC)를 포함하는 eUICC 시스템에서의 프로비저닝 방법으로서, 상기 MNO 시스템이 상기 eUICC로부터 프로파일을 암호화할 수 있는 eUICC 공개키에 대한 PKI 키정보를 수신하는 단계와, 상기 MNO 시스템 또는 상기 SM이 상기 프로파일을 상기 eUICC 공개키로 1차 암호화하는 단계와, 상기 MNO 시스템이 상기 SM에게 1차 암호화된 프로파일을 전송하여 2차 암호화를 요청하며, 그에 대한 응답으로 2차 암호화된 프로파일을 수신하는 단계와, 상기 MNO 시스템이 상기 2차 암호화된 프로파일을 상기 eUICC로 전송하는 단계를 포함하는 프로비저닝 방법을 제공한다.
- [16] 본 발명의 다른 실시예는 통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 그와 연동된 내장 UICC(eUICC)를 포함하는 eUICC 시스템에서의 MNO 변경 방법으로서, 리시빙 MNO 시스템이 상기 eUICC로부터 프로파일을 암호화할 수 있는 eUICC 공개키에 대한 PKI 키정보를 수신하는 단계와, 상기 리시빙 MNO 시스템 또는 상기 SM이 상기 프로파일을 상기 eUICC 공개키로 1차 암호화하는 단계와, 상기 리시빙 MNO 시스템이 도너 MNO 시스템으로 MNO 변경 통지를 한 후 인증을 받는 단계와, 상기 리시빙 MNO 시스템이 상기 SM에게 1차 암호화된 프로파일을 전송하여 2차 암호화를 요청하며, 그에 대한 응답으로 2차 암호화된 프로파일을 수신하는 단계와, 상기 리시빙 MNO 시스템이 상기 2차 암호화된 프로파일을 상기 eUICC로 전송하는 단계를 포함하는 MNO 변경 방법을 제공한다.
- [17] 본 발명의 다른 실시예는 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서, 상기 eUICC는 상기 MNO 시스템 또는 SM 등의 외부 엔터티로부터 전송된 프로파일을 복호화할 수 있는 프로파일 접근 크레덴셜을 포함하며, eUICC는 외부 엔터티 중 하나에게 자신의 상태 및 능력에 대한 정보인 키정보-키정보는 키생성 알고리즘, 키길이 정보, 키 생성방식에 대한 정보 등을 포함함-를 제공하는 eUICC를 제공한다.
- [18] 본 발명의 다른 실시예는 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서, 상기 eUICC는 칩 오퍼레이션 시스템(Chip OS; COS)과, SIM 플랫폼과, SIM 서비스 관리 플랫폼, 및 상기 MNO 시스템 또는 SM으로부터 전송된 프로파일을 복호화할 수 있는 프로파일 접근 크레덴셜에 대한 키정보를 저장 및 관리하는 PKI 키정보 프로파일을 포함하는 eUICC를 제공한다.
- [19] 본 발명의 다른 실시예는 가입 관리시스템(SM) 및 내장 UICC(eUICC)와 연동되어 있는 통신사업자(MNO) 시스템으로서, 상기 MNO 시스템은 eUICC의 프로비저닝 또는 MNO 변경 과정에서, 상기 eUICC로부터 프로비저닝 또는 MNO 변경에 필요한 eUICC 프로파일을 암호화할 수 있는 eUICC 공개키에 대한 PKI 키정보를 수신하고, 상기 eUICC 프로파일을 상기 eUICC로 암호화한 후

상기 eUICC로 전송하는 MNO 시스템을 제공한다.

도면의 간단한 설명

- [20] 도 1은 본 발명이 적용되는 eUICC를 포함한 전체 서비스 아키텍처를 도시한다.
- [21] 도 2는 본 발명이 적용될 수 있는 SM 분리 환경의 시스템 아키텍처를 도시한다.
- [22] 도 3은 본 발명의 일 실시예에 의한 프로비저닝 과정의 전체 흐름도이다.
- [23] 도 4는 본 발명의 일 실시예에 의한 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.
- [24] 도 5는 본 발명의 일 실시예에 의한 eUICC 또는 eSIM의 내부 구조를 도시한다.
- [25] 도 6은 본 발명의 일 실시예에 적용되는 eUICC의 파일 구조의 일 예를 도시한다

발명의 실시를 위한 형태

- [26] 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.
- [27] 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 탈착 가능한 구조로 M2M 단말을 제조하게 되면, M2M 단말의 소형화가 힘들게 된다.
- [28] 따라서, UICC 착탈이 불가능한 내장(Embedded) UICC 구조가 논의되고 있는데, 이 때 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.
- [29] 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 수 밖에 없고 제품 가격이 상승하게 되는 문제가 있어, M2M 단말 확대에 큰 걸림돌이 되고 있는 상황이다.
- [30] 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.

- [31] 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.
- [32] 이에 본 발명의 일 실시예에서는 MNO, SM, eUICC 등으로 구성된 시스템에서 프로파일의 암호화에 사용되는 프로파일 접근 크레덴셜(Profile Access Credentials), 즉 eUICC 공개키 및 그에 대응되는 비밀키 등을 eUICC 내부에 저장/관리하는 방안을 제안한다. 또한, eUICC 내부에 있는 프로파일 접근 크레덴셜에 대한 정보를 외부 엔터티로 전송하여 암호화 등에 이용할 수 있도록 하는 방안도 함께 제안한다.
- [33] 본 명세서에서는 eSIM과 eUICC를 동등한 개념으로 사용한다.
- [34] 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 어플리케이션 (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 어플리케이션을 탑재하고 서비스를 제공할 수 있는 플랫폼 중 하나이다.
- [35] SIM은 제한된 메모리 공간과 보안상의 이유로 누구나 SIM 내에 어플리케이션을 탑재해서는 안되며, 이로 인해 어플리케이션 탑재를 위한 플랫폼 이외에 SIM을 어플리케이션 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.
- [36] 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.
- [37] 여기서, 관리키 또는 eSIM 관리키 또는 eUICC 관리키 또는 보안키로 표현될 수 있는 키는 eSIM으로의 접근 인증키로서 사업자 정보를 안전하게 eSIM으로 전달하기 위한 것이며, 본 발명에서 주로 다루는 프로파일 접근 크레덴셜로서의 eUICC 공개키/비밀키와는 구별되는 개념이다.

- [38] GSMA에서는 SM의 역할을 SM-DP와 SM-SR로 분류하였다. SM-DP는 오퍼레이션 프로파일(또는 사업자 정보) 이외에 IMSI, K, OPc, 부가 서비스 어플리케이션, 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.
- [39] 그리고 아래 도 1의 “신뢰 서클(Circle of Trust)”이라는 구조를 제안하여 각 유사 개체 또는 엔터티들간에 신뢰 관계의 중첩을 통해 MNO와 eSIM 간의 엔드-투-엔드(End-to-End) 신뢰 관계를 구축한다는 개념을 제안하였다. 즉, MNO1은 SM1과, SM1은 SM4, SM4는 eSIM과 신뢰관계를 형성하여, 이를 통해 MNO와 eSIM 간의 신뢰관계를 형성한다는 개념이다.
- [40] 본 발명을 설명하기 전에 우선 본 명세서에서 사용할 용어에 대하여 설명한다.
- [41] MNO(Mobile Network Operator)는 이동통신 사업자를 의미하며, 모바일 네트워크를 통해 고객에게 통신 서비스를 제공하는 엔터티를 의미한다.
- [42] SM(Subscription manager)는 가입 관리 장치로서, eUICC의 관리 기능을 수행한다.
- [43] eUICC 공급자(eUICC Supplier)는 eUICC 모듈과 내장 소프트웨어(펌웨어와 오퍼레이팅 시스템 등)를 공급하는 자를 의미한다.
- [44] 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.
- [45] 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.
- [46] 가입(Subscription)은 가입자와 무선통신 서비스 제공자 사이의 서비스 제공을 위한 상업적인 관계를 의미한다.
- [47] 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.
- [48] 프로파일 액세스 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.
- [49] 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.

- [50] 오퍼레이션 프로파일(Operation Profile) 또는 사업자 정보는 사업자 가입(Operational Subscription)과 관련된 모든 종류의 프로파일을 의미한다.
- [51] 도 1은 본 발명이 적용되는 eSIM(eUICC)을 포함한 전체 서비스 아키텍처를 도시한다.
- [52] 전체 시스템에 대해서 설명하면 다음과 같다.
- [53] 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.
- [54] 도 1에서 점선은 신뢰 서클을 도시하고, 2개 실선은 안전한 링크를 의미한다.
- [55] 가입정보가 저장되어 전달되는 시나리오가 필요하면, MNO의 승인과 MNO의 컨트롤 하에서 이루어져야 한다. 특정 시각에 단일의 eUICC 상에는 1개만의 액티브 프로파일이 있어야 하며, 이 때 액티브 프로파일은 특정 시간에 단일 HLR에 부가되는 것을 의미한다.
- [56] 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.
- [57] 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.
- [58] MNO 크레덴셜 또는 프로파일은 K, 알고리즘, 알고리즘 파라미터, 부가 서비스 어플리케이션, 부가 서비스 데이터 등을 포함하는 가입 크레덴셜을 의미할 수 있다.
- [59] 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.
- [60] 오퍼레이터는 자신의 크레덴셜에 대해서 완전한 제어권을 가져야 하며, 오퍼레이터는 SM 오퍼레이션에 대해서 강한 감독권과 제어권한을 가져야 한다.
- [61] SM 기능은 MNO 또는 제3 기관에 의하여 제공되어야 하며, 만약 제3 기관에 의하여 제공된다면 SM과 MNO 사이에는 상업적인 관계가 설정되어 있는 경우

등일 것이다.

- [62] 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 가입자임)가 자신의 고객과 가질 수 있는 계약 관계에 편승할 의도는 아니다.
- [63] 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.
- [64] 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.
- [65] SM의 역할은 SM-SR, SM-DP와 같은 2개의 서브 기능으로 나뉘어 질 수 있다.
- [66] 실제로, 이러한 SM-SR, SM-DP 기능들은 다른 엔티티에 의하여 제공될 수도 있고, 동일한 엔티티에 의해서 제공될 수도 있다. 따라서, SM-DP와 SM-SR의 기능을 명확하게 경계지울 필요가 있고, 이들 엔티티들 사이의 인터페이스를 정의할 필요가 있다.
- [67] 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 어플리케이션, 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.
- [68] 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, 스캐러빌리티(Scalability) 및 신뢰도에 대한 요구사항이 중요할 것으로 예상된다.
- [69] 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.

- [70] 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.
- [71] 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.
- [72] 즉, 도 1에서 110은 SM들끼리, 더 구체적으로는 SM-SR 멤버 사이에 형성되는 신뢰 서클을 나타내고, 120은 MNO 파트너들의 신뢰 서클이며, 130은 엔드투엔드 신뢰 링크를 도시한다.
- [73] 도 2는 SM 분리 환경에서 SM-SR 및 SM-DP가 시스템에 위치하는 구성을 도시한다.
- [74] 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.
- [75] 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)
- [76] 이러한 eUICC 시스템 아키텍처 하에서, 본 발명의 일 실시예에 의한 eUICC는 각종 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)의 로딩을 위하여 무결성(Integrity), 비밀성(Confidentiality) 및 인증성(Authenticity)을 보장할 수 있는 메커니즘을 포함할 수 있다. 이러한 메커니즘의 일 예로서 아래 도 3 이하에서 설명할 바와 같이 프로파일 접근 크레덴셜인 eUICC의 공개키 및 비밀키를 이용한 암/복호화 메커니즘 및 선택적으로 SM의 공개키 및 비밀키를 이용한 전자서명을 포함할 수 있다.
- [77] 즉, 무결성, 비밀성 및 인증성을 보장할 수 있는 안전한 메커니즘에 의하여 eUICC 아키텍처 내에서 각종 프로파일이 아주 안전하게 보호되어야 하며, 따라서 프로파일이 eUICC 내로 전송(제조 단계에서 프로비저닝되는 것이 아닌)되기 때문에 그러한 프로파일을 보호하기 위한 아주 안전한 메커니즘이 필요하다.
- [78] 본 발명의 일 실시예에 의한 eUICC는 eUICC 내에서 각종 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)을 관리 또는 핸들링 할 수 있는 프로파일 접근 크레덴셜 및 그에 대한 정보를 저장/관리하고, 외부 엔터티로 제공할 수

있다.

- [79] 더 구체적으로 설명하면, 본 발명에서는 eUICC에서 엔드 포인트(End point; 예를 들면 Subscription Manager)로부터 전송되는 각종 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)을 안전하게 프로비저닝 하기 위한 프로파일 접근 크레덴셜(예를 들면, eUICC의 공개키 등)을 최소한 1개 세트 이상 보유하며, 아래 실시예에서 설명할 바와 같이, 외부 엔터티로부터 전송된 암호화된 프로파일을 상기 프로파일 접근 크레덴셜을 이용하여 복호할 수 있다.
- [80] 본 명세서에서의 프로파일 접근 크레덴셜(Profile Access Credential)은 SM이나 MNO와 같은 외부 엔터티로부터 수신한 프로파일을 복호화하기 위하여 사용되는 데이터를 의미하는 것으로서, 반드시 상기 용어에 한정되는 것은 아니며, 동등한 기능을 수행하는 한 프로파일 설치 크레덴셜, 프로파일 인스톨러 크레덴셜 등 다른 용어로 표현될 수도 있을 것이다.
- [81] 또한, 본 발명의 일 실시예에서는 eUICC 내에는 오직 1개의 활성화 프로파일(Active Profile)만이 존재하는 것이 바람직하며, 프로파일 또는 프로파일 관리 데이터(Profile management data)는 그 프로파일 또는 프로파일 관리 데이터를 소유하는 오퍼레이터 시스템과 신뢰성 있게 연결된 엔드 포인트와 eUICC 사이에서 안전하게 전송되어야 할 뿐 아니라, 프로파일 또는 프로파일 관리 데이터는 단말 또는 터미널과 같은 외부 엔터티에 의해서 접근이 불가능해야 한다. 그를 위하여, 본 발명의 일 실시예에서는 아래 프로파일 또는 프로파일 관리 데이터를 암/복호화할 수 있는 프로파일 접근 크레덴셜로서 eUICC 공개키를 이용하는 방식을 포함한다.
- [82] 한편, 이러한 프로파일 접근 크레덴셜로의 eUICC 공개키/비밀키 쌍은 eUICC 제조 단계에서 생성되어 eUICC 내부에 저장될 수도 있고, 외부 인터티(SM 등)로부터의 요청에 따라 동적(Dynamic)으로 eUICC가 생성하여 저장할 수도 있을 것이다.
- [83] 또한, 공개키/비밀키 생성 방식은 RSA(Rivest Shamir Adleman), ECC((Elliptic Curve Cryptography), DH(Diffie-Hellman), DSA 또는 DSS(Digital Signature Standard) 등 여러 알고리즘이 존재하고, 각 공개키 생성 방식에 따라서 키 길이, 키 생성 알고리즘 등이 상이할 수 있다.
- [84] 따라서, 정적 또는 동적으로 생성된 프로파일 접근 크레덴셜로의 eUICC 공개키/비밀키와 그에 대한 PKI 키 정보(PKI Key Information)가 eUICC 내부에 안전하게 저장/관리되어야 하며, 암복호화에 관련된 외부 엔터티로 공개키와 PKI 키 정보를 전달하여, 원활한 공개키 방식의 암복호화가 수행되도록 할 필요가 있다.
- [85] 따라서, 본 발명의 일 실시예에서는, MNO, SM, eUICC 등으로 구성된 시스템에서 프로파일의 암호화에 사용되는 프로파일 접근 크레덴셜(Profile Access Credentials), 즉 공개키 및 그에 대응되는 비밀키 등과, 그 PKI에 대한 키 정보(키 생성 알고리즘, 키 길이, 키 생성방식 등)를 eUICC 내부에

저장/관리하는 방안을 제안한다. 또한, eUICC 내부에 있는 프로파일 접근 크레덴셜에 대한 정보를 외부 엔터티로 전송하여 암호화 등에 이용할 수 있도록 하는 방안도 함께 제안한다.

[86] 도 3은 본 발명이 적용되는 시스템에서 제1차 가입에 해당되는 프로비저닝 과정의 전체 흐름도이다.

[87] 프로비저닝 과정에서, eUICC는 기기 식별 정보 (IMEI 등)와 eUICC 식별 정보 (eICCID 등)를 포함하는 활성화 요청을 MNO로 전송한다.(Request activation; S310) 그런 다음, S320단계에서 MNO와 eUICC 사이에는 eUICC 상태 요청 및 기술적 능력 제어 요청/확인이 수행된다.(eUICC status request 및 technical capability control; S320)

[88] 이러한 S320단계는 eUICC가 자신의 상태 및 기술적 능력에 대한 정보를 외부 엔터티에게 제공하기 위한 과정으로서, 상기 표현에 한정되는 것은 아니며, 상태 및 능력 확인 과정 등으로 표현될 수도 있을 것이다.

[89] 또한, 상기 S320 단계에서는 eUICC가 본 실시예에 의한 상태 및 능력에 대한 정보로서의 PKI 키 정보(키 생성 알고리즘, 키 길이, 키 생성 방식 등)를 해당 MNO 시스템으로 제공할 수 있다. 또한, 도시하지는 않았지만, eUICC는 상기 PKI 키정보에 의하여 생성된 자신의 공개키를 해당 SM(특히, SM-SR)으로 제공할 수 있다.

[90] S330단계에서 MNO는 SM-SR과 사이에서 eUICC 아이덴티티 검증과, 장치(eUICC)에 대한 정보를 수집한다(eUICC identity verification 및 collect information about device). S330단계에서, MNO는 본 발명의 일 실시예에 의하여 해당 eUICC에 대한 암호화 키, 구체적으로는 eUICC에 대응되는 공개키를 SM-SR로부터 획득할 수 있다.

[91] 이러한 공개키의 획득은 정적(static) 또는 동적(Dynamic)으로 이루어질 수 있는바, 정적으로 이루어지는 경우 eUICC 제조시에 이미 해당 eUICC 내부적으로, 세부적으로는 eUICC 내의 암호 연산 프로세서 (CCP 등)를 통해 공개키와 비밀키가 생성되어 eUICC에는 비밀키가 저장되고, 공개키는 모든 SM-SR이 공유함으로써 특정한 eUICC에 대한 공개키를 인식할 수 있도록 하고, MNO로부터 요청이 있는 경우 SM-SR은 해당되는 eUICC에 대한 공개키를 MNO로 전달하는 방식이다.

[92] 동적인 암호키 획득방법은, MNO로부터 요청(특정 eUICC 식별정보 포함)이 있는 경우, SM-SR은 해당되는 eUICC에게 공개키 전송을 요청하고, 해당 eUICC는 eUICC 탑재 단말 내의 발급 처리 모듈(이 용어에 한정되지 않으며, 통신모듈, 프로비저닝 모듈, 발급 모듈, 개통 모듈 등으로 칭할 수 있으며, eUICC 프로비저닝을 위한 eUICC 탑재 단말 외부와의 통신 및 프로비저닝 관리의 역할을 수행함) 또는 eUICC 내의 보안모듈(암호키 생성 모듈, 암호키 처리 모듈, Security Policy 모듈, Credential Manager, Profile Manager, 프로파일 인스톨러 등 eUICC 내의 암호키 생성 및 암호키를 활용한 보안 연산, 프로파일 복호화 연산

등을 수행하는 모듈)을 이용하여 공개키를 생성한 후 SM-SR로 전달하는 방식으로 수행될 수 있다.

- [93] 여기서, eUICC 내에 탑재되는 보안모듈은 eUICC 제작 단계 또는 그 이후 eUICC 정책에 따라 eUICC 내에 공통적으로 1개가 설치될 수 있으며, eUICC 정책 및 각 MNO 정책에 따라 각 MNO 별로 여러 개가 설치될 수 있다.
- [94] 해당 eUICC의 공개키(암호키)를 획득한 MNO는 SM-DP를 통해서 MNO에 맞는 새로운 eUICC 프로파일을 생성하고 그 프로파일을 획득한 eUICC 공개키(암호키)로 암호화한 후 MNO로 전달한다.(1차 암호화, S340 단계) 이 때, 인증성(Authenticity)을 제공하기 위해 SM-DP는 자신의 개인키로 추가적인 전자서명을 생성할 수 있다. 즉, S340 단계에서 SM-DP는 인증을 위한 자신의 개인키 또는 비밀키로 프로파일을 전자서명(Sign)할 수 있다.
- [95] 물론, 이러한 프로파일의 생성 및 eUICC 공개키를 이용한 암호화가 반드시 SM-DP에 의하여 수행될 필요는 없으며, MNO 시스템이 자체적으로 수행할 수도 있을 것이다.
- [96] 다음으로, MNO는 1차 암호화된 (eUICC) 프로파일을 SM-SR로 전달한 후 2차 암호화를 요청하면, SM-SR은 이미 저장하고 있는 eUICC 관리키(eUICC OTA 키, GP ISD 키 등)를 이용하여 eUICC 프로파일을 2차 암호화하여 MNO로 전달한다.(S350 단계)
- [97] 그런 다음, MNO는 이중 암호화(Double CIPHERED)된 eUICC 프로파일을 해당 eUICC로 전송한다.(S360 단계) 이 때, 인증성을 제공하기 위해 SM-DP의 공개키 또는 인증서(Certification)를 함께 eUICC로 전송할 수 있다.
- [98] eUICC는 이미 eUICC 관리키를 알고 있으므로 1차로 복호화한 후, 자신 공개키에 대응되는 비밀키(제조 또는 공개키 동적 생성 단계에서 이미 알고 있음)를 이용하여 2차 복호화함으로써 프로비저닝에 사용될 프로파일을 완전히 복호화 할 수 있다. 이 때, eUICC는 인증서 확인 (MNO로부터 획득한 공개키에 해당되는 SM-DP로부터 생성된 eUICC 프로파일인지 확인하기 위해)을 위해 SM-DP의 공개키 (인증서의 경우, 신뢰할 수 있는 제 3의 개체로부터 해당 인증서의 유효성을 검증 받을 수 있음)로 서명 검증을 수행할 수 있다.
- [99] S370 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.
- [100] 이러한 각 단계에 대한 주요 구성을 추가로 설명하면 다음과 같다.
- [101] S310 단계에서, eUICC 식별 정보(eICCid 등)는 공개된 데이터이며 eUICC 내부에 통합 보호되어야 한다.
- [102] S320, S330 단계에서 상태 요청 및 기술적 가능성 제어는 eUICC 아이덴티티의 증명을 제공(신뢰할 수 있는 eUICC)하며, MNO 서비스를 위한 eUICC 특성의 적격성을 확인할 수 있어야 한다.
- [103] S340~S360 단계에서는 eUICC 프로파일 생성 및 전송을 위하여 이중 암호화 메커니즘이 사용된다. 즉, SM-DP에 의하여 eUICC에 링크된 생성 프로파일은

오직 목표 eUICC에 의해서만 읽힐 수 있는 암호화 메커니즘에 의하여 암호화되며, 정당한 SM-DP로부터 생성된 프로파일임을 확인하기 위해 SM-DP에 의해 전자서명이 수행될 수 있고, SM-SR은 생성 프로파일을 eUICC 관리키로 암호화하여 전달 동안 eUICC를 인증하고 보호한다.

- [104] S370 단계에서, SM-SR 데이터베이스는 가입 설치(Subscription installation)의 마무리 단계에서 업데이트 될 수 있다.
- [105] 도 4는 본 발명이 적용되는 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.
- [106] 전체적으로는 도 3의 프로비저닝 과정과 유사(즉, 변경 후 새로운 MNO가 도 3의 MNO에 해당)하며, 다만 새로운 MNO에 대한 프로파일 생성 전후에 새로운 MNO가 도너 MNO에게 협상 및 권리 전송 과정을 수행하는 점이 상이하다.(단계 S440’)
- [107] 즉, 도 4의 MNO 변경과정과 도 3의 프로비저닝 과정을 차이점은, 프로비저닝 또는 오퍼레이션 액티브 프로파일을 이용하여, 액티베이션 요청이 도너 MNO OTA 베어러(Bearer)로 전송되고, 새로운 MNO는 OTA 또는 OTI 중 하나로 새로운 프로파일을 다운로드 하도록 SM-SR로부터 경로를 요청하는 것이다.
- [108] 도 4에 의한 MNO 변경 과정을 구체적으로 설명하면 다음과 같다.
- [109] MNO 변경을 위하여, eUICC는 기기 식별 정보 (IMEI 등)와 eUICC 식별 정보 (eICCID 등)를 포함하는 활성화 요청을 변경될 MNO(Receiving MNO)로 전송한다.(Request activation; S410) 그런 다음, S420단계에서 리시빙 MNO와 eUICC 사이에는 eUICC 상태 요청 및 기술적 능력 제어 요청/확인이 수행된다.(eUICC status request 및 technical capability control; S420)
- [110] 또한, 상기 S420 단계에서는 아래에서 설명할 바와 같이, eUICC가 자신의 상태 및 기술적 능력에 대한 정보 중 하나로서 공개키(PK) 또는 프로파일 접근 크레덴셜 정보인 PKI 키에 대한 정보(키 생성 알고리즘, 키 길이, 키 생성 방식 등)를 해당 리시빙 MNO 시스템 또는 SM-SR로 제공하는 과정이 포함될 수 있음은 프로비저닝 과정인 S320과 동일하다.
- [111] S430단계에서 리시빙 MNO는 SM-SR과 사이에서 eUICC 아이덴티티 검증과, 장치(eUICC)에 대한 정보를 수집한다(eUICC identity verification 및 collect information about device). S430단계에서, MNO는 본 발명의 일 실시예에 의하여 해당 eUICC에 대한 암호화 키, 구체적으로는 eUICC에 대응되는 공개키를 SM-SR로부터 획득할 수 있다.
- [112] 이러한 공개키의 획득은 정적(static) 또는 동적(Dynamic)으로 이루어질 수 있는바, 정적으로 이루어지는 경우 eUICC 제조시에 이미 해당 eUICC 내부적으로, 세부적으로는 eUICC 내의 암호 연산 프로세서 (CCP 등)를 통해 공개키와 비밀키가 생성되어 eUICC에는 비밀키가 저장되고, 공개키는 모든 SM-SR이 공유함으로써 특정한 eUICC에 대한 공개키를 인식할 수 있도록 하고, MNO로부터 요청이 있는 경우 SM-SR은 해당되는 eUICC에 대한 공개키를 MNO로 전달하는 방식이다.

- [113] 동적인 암호키 획득방법은 도 3과 관련하여 설명한 바와 동일하므로, 중복을 피하기 위하여 설명을 생략한다.
- [114] 해당 eUICC의 공개키(암호키)를 획득한 리시빙 MNO는 SM-DP를 통해서 MNO에 맞는 새로운 eUICC 프로파일을 생성하고 그 프로파일을 획득한 eUICC 공개키(암호키)로 암호화한 후 MNO로 전달한다.(1차 암호화, S440 단계) 이때, 인증성(Authenticity)을 제공하기 위해 SM-DP는 자신의 개인키로 추가적인 전자서명을 생성할 수 있다. 즉, S440 단계에서 SM-DP는 인증을 위한 자신의 개인키 또는 비밀키로 프로파일을 전자서명(Sign)할 수 있다.
- [115] 또한, S440 단계 이전 또는 이후에 협상 및 권리 전송 단계(S440')가 수행될 수 있다. 이러한 협상 및 권리 전송 단계(S440')는 새로운 리시빙 MNO가 이전 MNO(도너 MNO)에게 해당 eUICC가 정당한지 여부와, MNO 변경에 따른 권리(정보)를 이전해 줄 것을 요청하는 등의 과정이다.
- [116] 즉, S440' 단계에서는 새로운 MNO(Receiving MNO)가 가입 스위칭 또는 MNO 변경에 대해서 통지한 후 도너 MNO의 인증을 요청하며, 이러한 인증은 정책 제어 기능(Policy Control Function)에 의해서 제공될 수 있다.
- [117] 다음으로, 리시빙 MNO는 1차 암호화된 (eUICC) 프로파일을 SM-SR로 전달한 후 2차 암호화를 요청하면, SM-SR은 이미 저장하고 있는 eUICC 관리키(eUICC OTA 키, GP ISD 키 등)를 이용하여 eUICC 프로파일을 2차 암호화하여 MNO로 전달한다.(S450 단계)
- [118] 그런 다음, MNO는 이중 암호화(Double CIPHERED)된 eUICC 프로파일을 해당 eUICC로 전송한다.(S460 단계) 이때, 인증성을 제공하기 위해 SM-DP의 공개키 또는 인증서(Certification)를 함께 eUICC로 전송할 수 있다.
- [119] eUICC는 이미 eUICC 관리키를 알고 있으므로 1차로 복호화한 후, 자신 공개키에 대응되는 비밀키(제조 또는 공개키 동적 생성 단계에서 이미 알고 있음)를 이용하여 2차 복호화함으로써 MNO 변경에 사용될 프로파일을 완전히 복호화 할 수 있다. 이때, eUICC는 인증서 확인 (MNO로부터 획득한 공개키에 해당되는 SM-DP로부터 생성된 eUICC 프로파일인지 확인하기 위해)을 위해 SM-DP의 공개키 (인증서의 경우, 신뢰할 수 있는 제 3의 개체로부터 해당 인증서의 유효성을 검증 받을 수 있음)로 서명 검증을 수행할 수 있다.
- [120] S470 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.
- [121] 한편, 상기 도 3 및 4와 같이 eUICC 제조 단계에서 공개키 및 개인키 쌍으로 생성한 후, eUICC의 라이프사이클(Lifecycle) 동안 지속적으로 활용함으로써 안전하게 사업자 정보를 eUICC 발급하기 위한 구조(동적 키 방식)와, 동적으로 eUICC가 공개키/비밀키를 생성하는 방식 모두에 있어서, 사용할 수 있는 PKI 기술은 다양할 수 있으며, 동일 PKI 내에서도 다양한 키 길이 및 키 생성 방식이 존재할 수 있으므로 이 정보를 eSIM 내에 저장하고 필요 시 MNO에 전달하는 세부 방안이 필요하다.

- [122] 본 발명의 일 실시예에서는, 이와 같이 eUICC 프로파일의 암호화에 사용되는 공개키/비밀키(개인키)를 eUICC가 관리하는 방식에 대하여 제안한다. 즉, 본 발명에서는 GSMA에서 제안한 SM 역할 분리 환경에서 eUICC 제조 단계에서 PKI 키 생성이 이뤄져 eUICC의 라이프싸이클 동안 활용되는 환경에서 다양한 PKI 기술을 적용할 수 있는 방안을 제시한다.
- [123] 본 발명의 일 실시예에서는, 본 발명에서의 eUICC은 SIM 제조사(Vendor)에 의한 제조 단계에서 다양한 PKI 기술 (예, RSA, ECC, DH 등)을 기반으로 PKI 키 쌍이 생성되며, 생성된 PKI 키에 대한 세부 정보 (이하, PKI 키정보라 함)는 eUICC 내부에 별도로 저장된다. 또한, 단말내의 발급처리 모듈 및 보안 모듈 등을 이용함으로써 공개키/비밀키가 동적으로 생성될 수 있으며, 이 경우에도 생성된 PKI에 대한 PKI 키정보가 eUICC 내부에 안전하게 저장되어야 한다.
- [124] 본 명세서에서의 PKI 키정보(PKI Key Information)는 키 생성 알고리즘, 키 길이, 키 생성 방식 중 하나 이상을 포함할 수 있으나 그에 한정되는 것은 아니며, PKI에 의하여 생성되는 공개키/비밀키 자체 이외의 모든 관련 정보를 포함하는 개념이다.
- [125] PKI 자체 또는 PKI 키정보를 eUICC에 저장하는 형식은 EF(Elementary File) 등과 같은 파일 형태이거나, TLV(Tag, Length, Value)와 같은 파일 구조 형태이거나 애플릿 등과 같은 애플리케이션 형태 등일 수 있으나 그에 한정되는 것은 아니다.
- [126] 또한, PKI 자체 및 PKI 키정보는 하나의 프로파일 형태로 eUICC 내부에 저장될 수 있으며, 이 때 PKI와 관련된 프로파일은 키 정보 프로파일 (key info profile), 관리 프로파일 (administration profile), 공통 프로파일 (common profile), 일반 프로파일 (general profile) 등으로 표현될 수 있으나 그에 한정되는 것은 아니다. 이하 명세서에서는 키정보 프로파일로 대표해서 설명한다.
- [127] 도 5는 본 발명의 일 실시예에 의한 eUICC 내부 구조를 도시한다.
- [128] 본 발명의 일 실시예에 의한 eUICC(500)는 장치 또는 단말(device or Terminal) 내에 착탈 불가능하게 포함되며, eUICC 내부에는 가장 하위 레벨의 칩 OS(COS; 510)과, 그 상위 레벨의 SIM 플랫폼(520), 그 상위 레벨의 SIM 서비스 관리 플랫폼(530) 등을 포함하며, COS 상위에는 본 발명에 의한 PKI 키정보 프로파일(540)이 포함된다.
- [129] 도 5에서는 키정보 프로파일(540)이 예를 들면 EF_eSIMPKI 과 같이 EF 형태의 키 정보 프로파일 형태로 저장되는 것을 도시하고 있으나, 전술한 바와 같이 그러한 형식에 한정되는 것은 아니며, TLV(Tag, Length, Value)와 같은 파일 구조 형태이거나 애플릿 등과 같은 애플리케이션 형태일 수도 있다.
- [130] eUICC 내에 저장된 PKI 키정보 또는 키정보 프로파일은 예를 들면, ALG_RSA/ALG_RSA_CRT/ALG_DSA의 키생성 방식에 대한 정보와, 1024, 2048 등과 같은 키 길이에 대한 정보 등을 포함할 수 있으나 그에 한정되는 것은 아니다.

- [131] 또한, SIM 서비스 관리 플랫폼(530) 상에는 특정한 기능의 애플리케이션(550)이 설치될 수 있으며, 이러한 애플리케이션은 키 정보 프로파일을 추출하여 외부 엔터티(예를 들면, MNO 시스템)로 전송하는 기능을 수행할 수 있다. 또한, 이러한 애플리케이션 자체가 본 발명에 의한 키정보 프로파일을 저장/관리할 수도 있을 것이다.
- [132] 또한, 도시하지는 않았지만, 본 발명에 의한 eUICC(500) 내부에는 프로비저닝 프로파일과, 각 사업자별 사업자 정보 또는 오퍼레이션 프로파일과, 그에 대응되는 보안모듈이 포함될 수 있다. 오퍼레이션 프로파일 및 보안모듈은 각 사업자 또는 MNO별로 달리 포함될 수 있으나, 특정 시점에는 단지 1개의 오퍼레이션 프로파일만이 활성화(Active)되는 것이 바람직하다.
- [133] 또한, eUICC(500) 내부에는 프로비저닝 프로파일(Provisioning Profile; 524)이 존재하여, 발급 처리가 필요할 경우, 모든 MNO들은 해당 프로비저닝 프로파일을 토대로 eUICC 탑재 기기와 “eUICC 인프라(SM, MNO 등)” 간의 통신이 가능해야 한다. 또한, “eUICC” 내부에는 SM-SR에서 관리하는 eUICC 관리키 - 예를 들면, UICC OTA 키(Key), GP(global Platform) ISD(Issuer Security Domain) 키 등을 포함하지만 그에 한정되지는 않음-에 대한 정보가 저장될 수 있다.
- [134] 본 발명의 일 실시예에 의한 eUICC 동작은 상기 도 3 또는 도 4의 흐름을 근간으로 한다.
- [135] 도 3 및 도 4의 S320, S420 단계(eUICC status request & technical capabilities control)에서 MNO 시스템은 eUICC 내의 PKI 키 정보를 관리하는 키 정보 프로파일에 키 정보를 요청할 수 있다. 이 때, MNO 시스템은, 예를 들면, EF_eSIMPKI를 리드(READ)하거나, 특정 애플리케이션을 선택(SELECT)하여 구동한 후 데이터(즉, PKI 키정보)를 요청하는 방식을 통해서 본 발명에 의한 PKI 키정보를 획득할 수 있다.
- [136] 이렇게 획득된 정보를 토대로 (리시빙) MNO 시스템은 도 3 및 도 4의 S330 및 S430 단계에서 SM-SR 등을 통해서 획득한 특정 eUICC 공개키가 어떤 공개키 생성 알고리즘 또는 방식으로 생성된 것인지 확인할 수 있으며, 이 정보를 기초로 S340 및 S440 단계에서 SM-DP 등을 경유하여 필요한 프로파일을 해당 eUICC의 공개키로 암호화 할 수 있게 된다.
- [137] 도 6은 본 실시예에 적용되는 eUICC의 파일 구조(UICC Application Structure)의 일 예를 도시한다.
- [138] 도 6과 같이 본 발명의 일 실시예의 eUICC 또는 eSIM에 저장되는 파일 형태는 크게 마스터 파일(Master File; MF), 전용 파일(Dedicated File; DF) 및 기본 파일(Elementary File; EF)로 구분될 수 있다.
- [139] MF는 접근 조건(Access Condition)을 포함하고, 선택적으로 DF들과 EF들을 포함할 수 있는 고유한 필수 파일(Mandatory File)을 의미한다.
- [140] DF는 파일의 기능적 그룹핑(Grouping)을 가능하게 하는 파일로서, DF들

및/또는 EF 들의 모파일(parent file)이 될 수 있으며, 파일 식별자(File Identifier)로 참조될 수 있다.

- [141] 일부 파일 식별자는 특정 사용을 위하여 예약(Reservation)되어 있으며, 예를 들면 DF 중에서 DF_{TELECOM}은 ‘7F10’으로, DF_{GSM}은 ‘7F20’으로 설정되어 있는 것과 같다. 이 중에서 DF_{TELECOM}은 선택적으로 사용(Optional)될 수 있으며, 애플리케이션 독립 정보(Application Independent Information)을 포함한다.
- [142] 또한, DF 중에서 DF_{TELECOM}인 ‘7F10’의 하위에 있는 DF_{PHONEBOOK}은 ‘5F3A’, DF_{MULTIMEDIA}는 ‘5F3B’, DF_{GRAPHIC}은 ‘5F50’으로 설정되어 있다.
- [143] 한편, EF_{DIR}은 MF 아래에 있는 선형 고정 파일(Linear Fixed File)로서, 일종의 애플리케이션 독립 파일이다.
- [144] 도 6에서 각 DF의 파일 식별자도 상기와 같은 예약 자원에 따라 표시된 것이다.
- [145] 이러한 파일 구조에서 본 실시예에 의한 PKI 키정보는 기본 파일 형태인 EF_eSIMPKI 형태로 저장되어 eUICC의 파일 구조에 포함될 수 있다.
- [146] 더 구체적으로는, 예를 들면, EF_eSIMPKI는 DF_{TELECOM}(파일 식별자 7F10) 하부에 위치할 수 있으며, 파일 식별자로서 ‘6F1X’를 가질 수 있고, EF_eSIMPKI의 파일 식별자인 6F1X에서 ‘X’는 0 내지 F 중 하나의 값을 의미할 수 있다.
- [147] 그러나 본 실시예에 의한 eUICC 또는 eSIM의 파일 구조는 도 6에 한정되는 것은 아니며, 필요한 PKI 키정보를 저장하기 위한 다른 형태(예를 들면, TLV와 같은 파일 구조나, 애플릿과 같은 애플리케이션 형태)도 가능할 것이다.
- [148] 이상과 같은 본 발명을 이용하면, 본 발명을 통해 GSMA에서 제안한 SM 역할 분리 환경에서 eUICC 제조 단계에서 정적으로 생성되거나 동작으로 생성된 PKI 및 그에 대한 키정보를 eUICC 발급 과정 등에서 활용함으로써 eUICC의 효율적이고 안전한 관리를 할 수 있게 된다.
- [149] 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.

청구범위

[청구항 1]

통신사업자(MNO) 시스템, 가입 관리시스템(SM)을 포함하는 외부 엔티티와 연동되어 있는 내장 UICC(eUICC)에서, 상기 eUICC는 상기 외부 엔티티 중 하나 이상과 상태 및 능력 확인 과정을 수행하며, 상기 상태 및 능력 확인과정에서 상기 eUICC는 자신의 상태 및 능력에 대한 정보를 제공하며, 상기 상태 및 능력에 대한 정보는 키생성 알고리즘, 키 길이, 키 생성방식 중 하나 이상을 포함하는 키정보인 것을 특징으로 하는 eUICC의 키정보 관리방법.

[청구항 2]

제1항에 있어서, 상기 eUICC는 상기 외부 엔티티로부터 수신한 암호화된 프로파일을 복호화하기 위한 프로파일 접근 크레덴셜을 추가로 포함하며, 상기 프로파일 접근 크레덴셜은 상기 eUICC의 공개키(또는 그에 대응되는 비밀키)인 것을 특징으로 하는 eUICC의 키정보 관리방법.

[청구항 3]

상기 eUICC 공개키는 상기 eUICC의 제조단계에서 생성되어 상기 eUICC 내에 저장되는 것을 특징으로 하는 eUICC의 키정보 관리방법.

[청구항 4]

상기 eUICC 공개키는 상기 MNO 시스템 또는 SM의 요청에 따라 상기 eUICC가 동적으로 생성되는 것을 특징으로 하는 eUICC의 키정보 관리방법.

[청구항 5]

제2항에 있어서, 상기 SM은 SM-DP(Data Preparation) 및 SM-SR(Secure Routing) 장치를 포함하며, 상기 SM-DP는 상기 eUICC 공개키를 이용하여 상기 프로파일을 암호화하고, 상기 SM-SR은 eUICC 공개키로 1차 암호화된 프로파일을 별도의 관리키로 2차 암호화함으로써, 상기 MNO 시스템 또는 SM으로부터 전송되는 프로파일은 이중 암호화(Double Ciphered)된 프로파일 인 것을 특징으로 하는 eUICC의 키정보 관리방법.

[청구항 6]

제1항에 있어서, 상기 프로파일은 프로비저닝을 위한 프로비저닝 프로파일, 오퍼레이션 프로파일, MNO 크레덴셜 정보 또는 MNO 크레덴셜 정보를 포함하는 패키지 정보, IMSI(International Mobile Subscriber Identity), 관리키(UICC OTA Key, GP ISD Key 등), 부가 서비스

어플리케이션, 부가 서비스 데이터 중 하나 이상의 정보를 포함하는 것을 특징으로 하는 eUICC의 키정보 관리방법.

[청구항 7]

상기 MNO 시스템 또는 SM으로부터 전송된 프로파일은 이중 암호화(Double Ciphered)된 프로파일이며, eUICC는 별도의 관리키로 상기 프로파일을 1차 복호화하는 단계와, 상기 eUICC 공개키로 2차 복호화하는 단계를 추가로 포함하는 것을 특징으로 하는 eUICC의 키정보 관리방법.

[청구항 8]

상기 키정보는 하나의 프로파일 형태로 상기 eUICC 내에 저장되는 것을 특징으로 하는 eUICC의 키정보 관리방법.

[청구항 9]

상기 키정보는 EF(Elementary File) 형태, TLV(Tag, Length, Value)의 파일 구조 형태 및 애플릿의 형태 중 하나로서 상기 eUICC 내에 저장되는 것을 특징으로 하는 eUICC의 키정보 관리방법.

[청구항 10]

통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 그와 연동된 내장 UICC(eUICC)를 포함하는 eUICC 시스템에서의 프로비저닝 방법으로서,

상기 MNO 시스템이 상기 eUICC로부터 프로파일을 암호화할 수 있는 eUICC 공개키에 대한 PKI 키정보를 수신하는 단계;

상기 MNO 시스템 또는 상기 SM이 상기 프로파일을 상기 eUICC 공개키로 1차 암호화하는 단계;

상기 MNO 시스템이 암호화된 상기 프로파일을 상기 eUICC로 전송하는 단계;를 포함하는 것을 특징으로 하는 프로비저닝 방법.

[청구항 11]

상기 PKI 키정보는 공개키 생성 방식, 키 길이, 암호화 알고리즘 중 하나 이상에 대한 정보를 포함하는 것을 특징으로 하는 프로비저닝 방법.

[청구항 12]

통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 그와 연동된 내장 UICC(eUICC)를 포함하는 eUICC 시스템에서의 MNO 변경 방법으로서,

리시빙 MNO 시스템이 상기 eUICC로부터 프로파일을 암호화할 수 있는 eUICC 공개키에 대한 PKI 키정보를 수신하는 단계;

상기 리시빙 MNO 시스템 또는 상기 SM이 상기 프로파일을 상기 eUICC 공개키로 1차 암호화하는 단계;

상기 리시빙 MNO 시스템이 도너 MNO 시스템으로 MNO 변경 통지를 한 후 인증을 받는 단계;

상기 리시빙 MNO 시스템이 상기 SM에게 1차 암호화된
프로파일을 전송하여 2차 암호화를 요청하며, 그에 대한 응답으로
2차 암호화된 프로파일을 수신하는 단계;
상기 리시빙 MNO 시스템이 상기 2차 암호화된 프로파일을 상기
eUICC로 전송하는 단계;를 포함하는 것을 특징으로 하는 MNO
변경방법.

[청구항 13]

제12항에 있어서,
상기 PKI 키정보는 공개키 생성 방식, 키 길이, 암호화 알고리즘 중
하나 이상에 대한 정보를 포함하는 것을 특징으로 하는 MNO
변경방법.

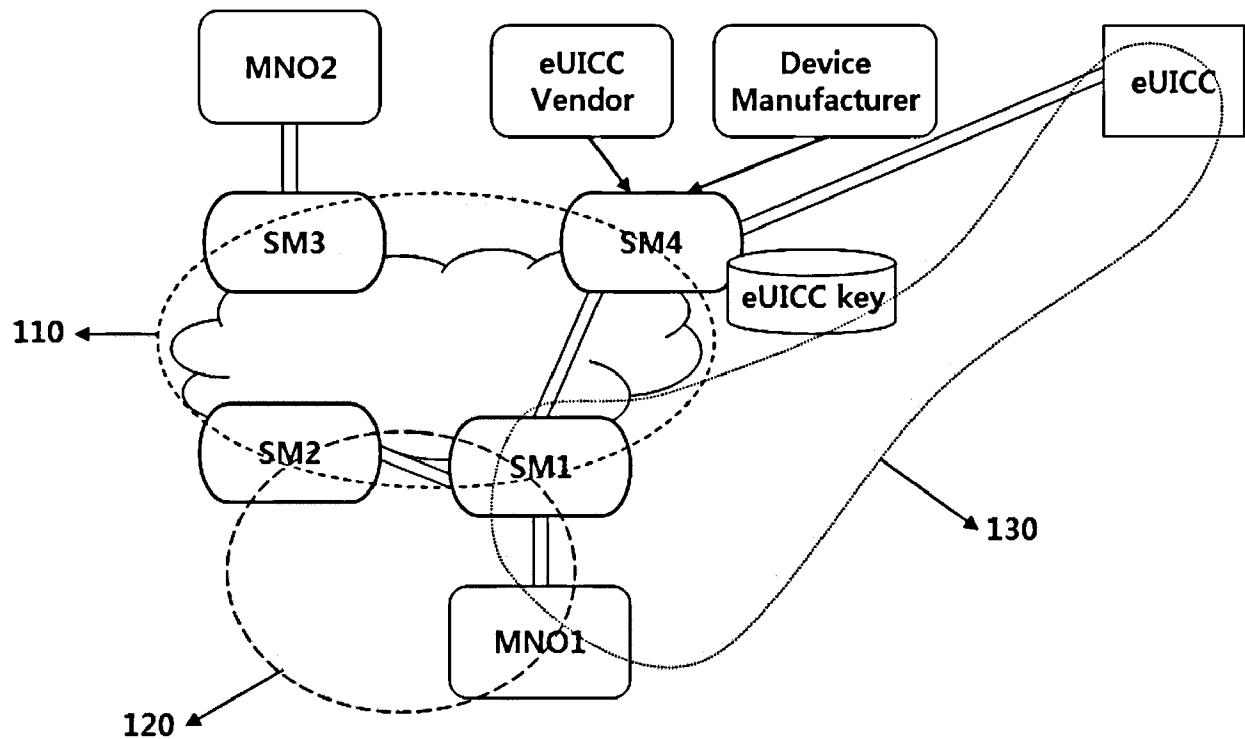
[청구항 14]

통신사업자(MNO) 시스템, 가입 관리시스템(SM)을 포함하는 외부
엔터티와 연동되어 있는 내장 UICC(eUICC)로서,
상기 eUICC는 상기 외부 엔터티 중 하나로부터 전송된
프로파일을 복호화할 수 있는 프로파일 접근 크레덴셜을
포함하며,
상기 eUICC는 상기 외부 엔터티 중 하나에게 자신의 상태 및
능력에 대한 정보인 키정보를 제공하며, 상기 키정보는 키생성
알고리즘, 키 길이 정보, 키 생성 방식 정보 중 하나 이상을
포함하는 것을 특징으로 하는 eUICC.

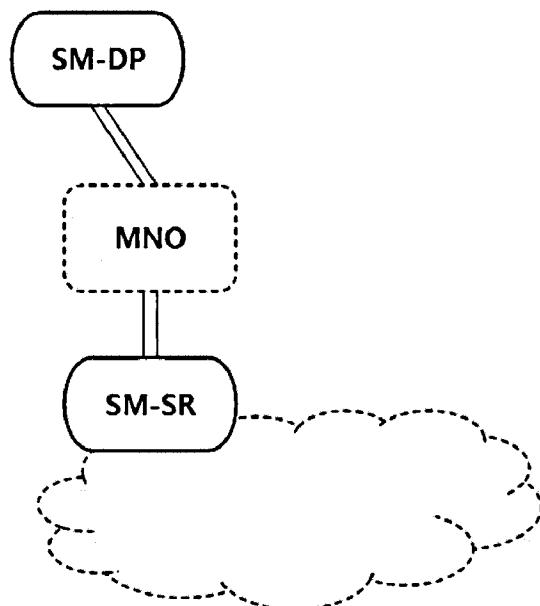
[청구항 15]

제14항에 있어서,
상기 프로파일 접근 크레덴셜은 상기 eUICC의 공개키(또는 그에
대응되는 비밀키)인 것을 특징으로 하는 eUICC.

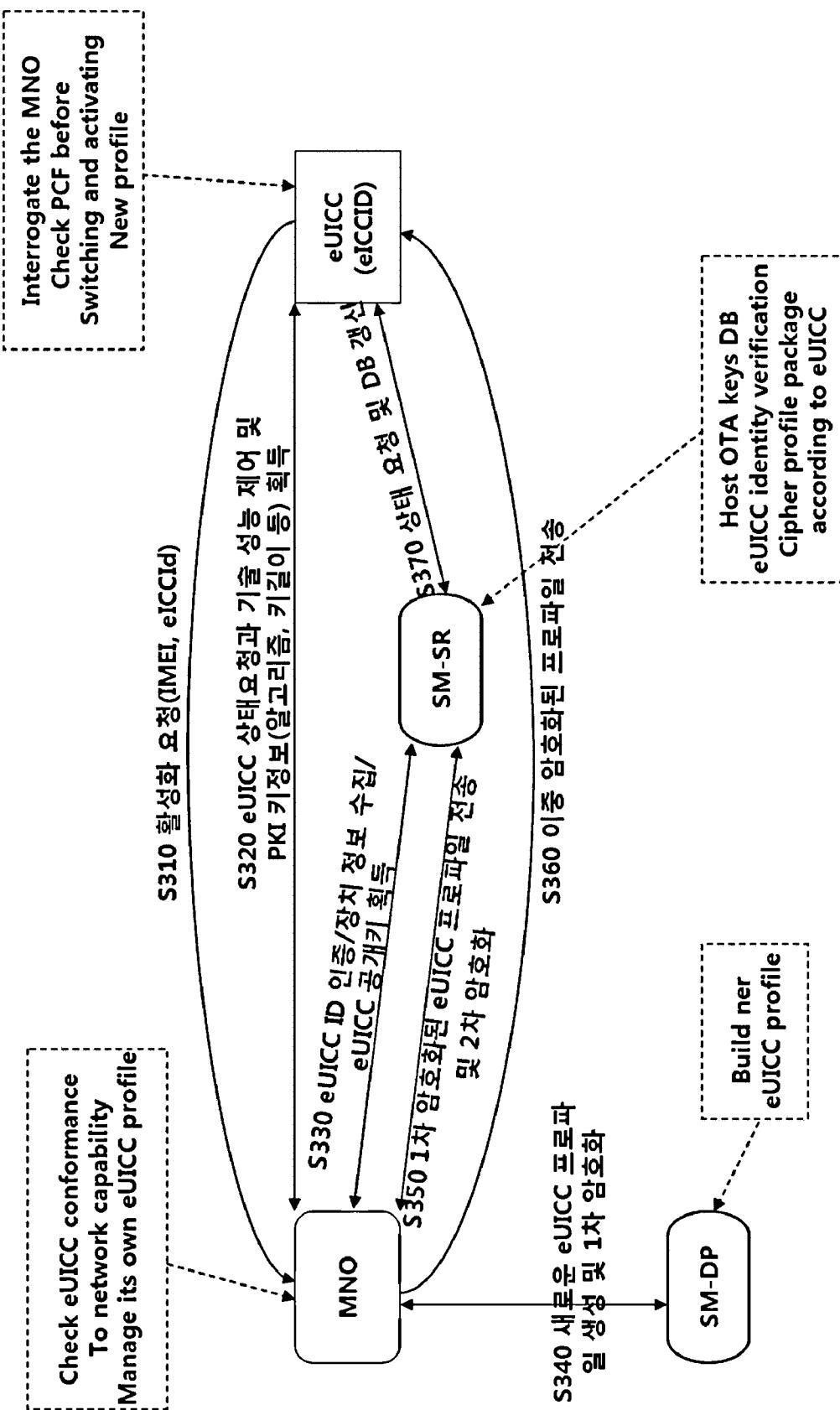
[Fig. 1]



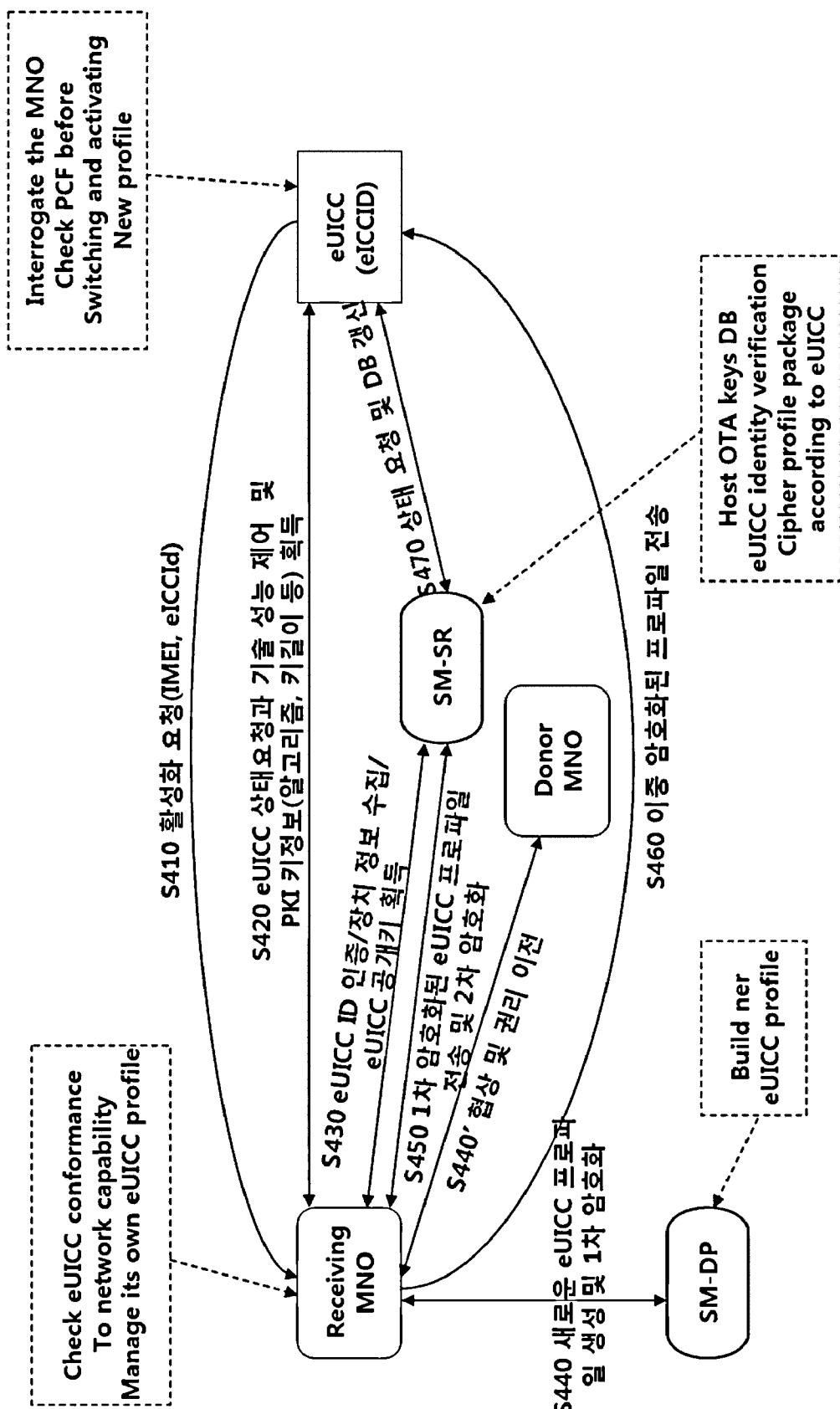
[Fig. 2]



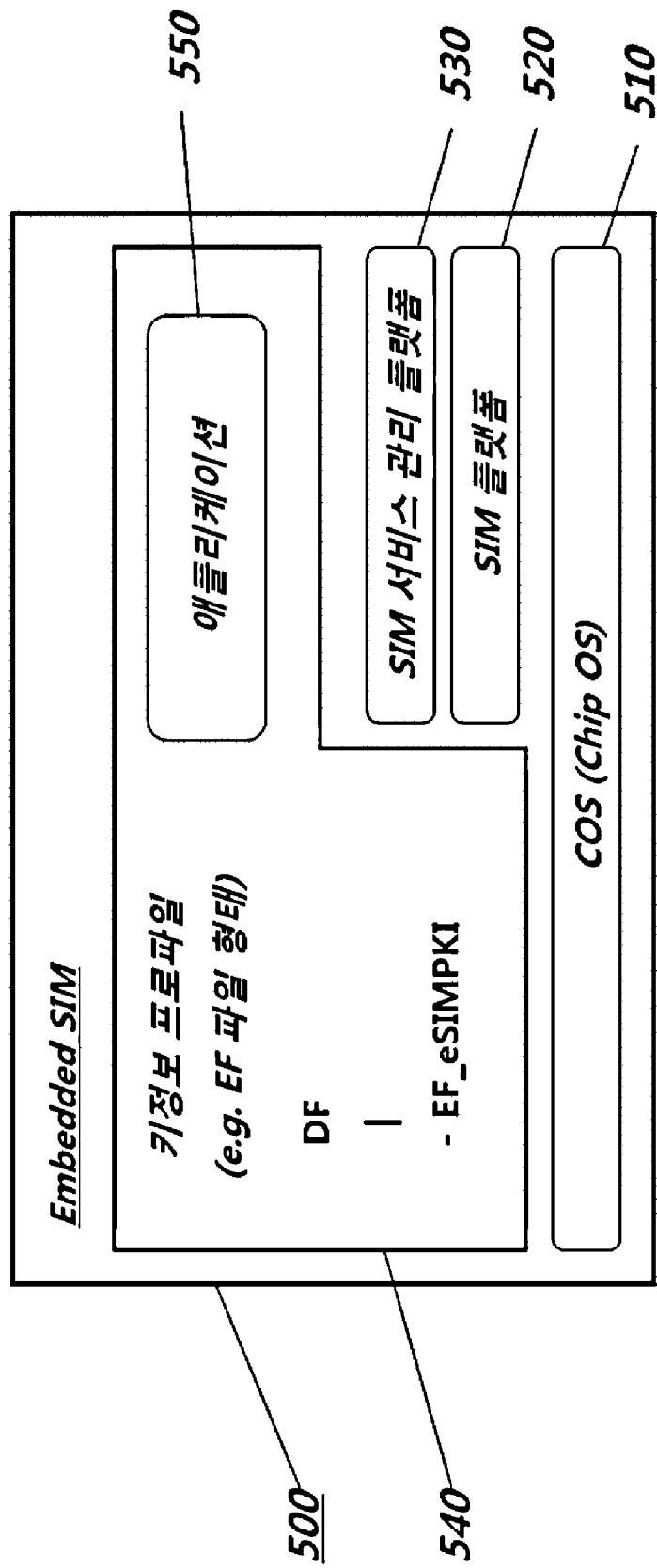
[Fig. 3]



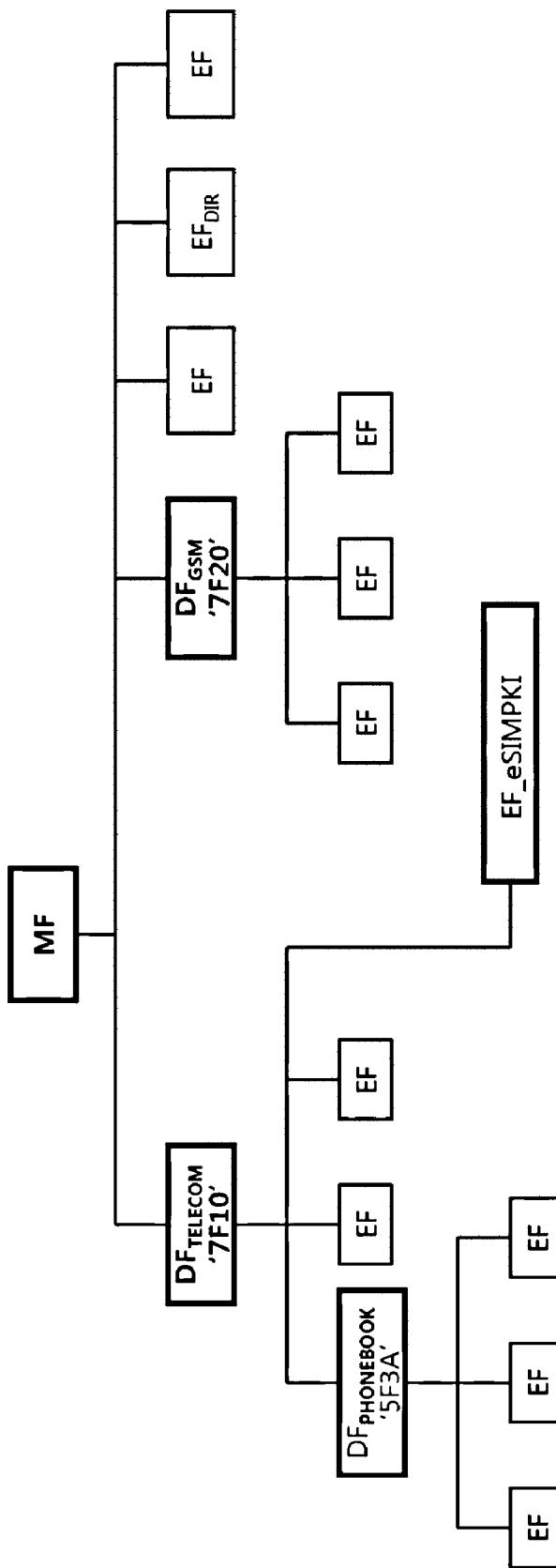
[Fig. 4]



[Fig. 5]



[Fig. 6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2012/007062**A. CLASSIFICATION OF SUBJECT MATTER*****H04W 12/04(2009.01)i, H04W 12/08(2009.01)i, H04W 8/18(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 12/04; G06F 15/00; H04K 1/00; H04L 9/32; H04W 12/06; H04L 9/00

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: embedded UICC, key generation algorithms, key length

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2175674 A1 (VODAFONE HOLDING GMBH) 14 April 2010 See abstract; paragraphs [0025]-[0027],[0047],[0048]; figure 1; claims 1,10,11.	1-15
A	KR 10-2008-0077786 A (KTFREETEL CO., LTD.) 26 August 2008 See abstract; paragraphs [0039]-[0051]; claims 1,2.	1-15
A	JP 2003-530012 A (NOKIA CO., LTD.) 07 October 2003 See abstract; paragraphs [0112]-[0122]; figure 10; claim 1.	1-15
A	US 7382882 B1 (IMMONEN OLLI) 03 June 2008 See abstract; figure 4; claims 1,4,28.	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	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"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
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search	Date of mailing of the international search report
30 JANUARY 2013 (30.01.2013)	30 JANUARY 2013 (30.01.2013)

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 SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2012/007062

Patent document cited in search report	Publication date	Patent family member	Publication date
EP 2175674 A1	14.04.2010	NONE	
KR 10-2008-0077786 A	26.08.2008	NONE	
JP 2003-530012 A	07.10.2003	AT 309656 T AU 2001-26838 A1 AU 2683801 A BR 0109651 A CA 2403521 A1 CA 2403521 C CN 1275418 C CN 1430835 A DE 60114789 D1 DE 60114789 T2 EP 1273128 A1 EP 1273128 B1 ES 2251459 T3 FI 20000760 D0 JP 04723158 B2 KR 10-0754458 B1 US 07107620 B2 US 07512796 B2 US 2002-0012433 A1 US 2007-0060106 A1 WO 2001-076134 A1 ZA 200207299 A	15.11.2005 15.10.2001 15.10.2001 22.04.2003 11.10.2001 26.05.2009 13.09.2006 16.07.2003 15.12.2005 20.07.2006 08.01.2003 09.11.2005 01.05.2006 31.03.2000 15.04.2011 31.08.2007 12.09.2006 31.03.2009 31.01.2002 15.03.2007 11.10.2001 02.05.2003
US 7382882 B1	03.06.2008	AT 264033 T AU 1999-47818 A1 AU 4781899 A BR 9911814 A CA 2336479 A1 CA 2336479 C CA 2466390 A1 CA 2466390 C CN 100452700 C CN 1126345 C0 CN 1316152 A0 CN 1516387 A DE 69916277 D1 DE 69916277 T2 EP 1095492 A1 EP 1095492 B1 EP 1408669 A1 ES 2219032 T3 JP 2002-520911 A JP 2010-259074 A KR 10-0451557 B1 WO 00-02358 A1	15.04.2004 24.01.2000 24.01.2000 16.10.2001 13.01.2000 27.11.2007 13.01.2000 06.10.2009 14.01.2009 29.10.2003 03.10.2001 28.07.2004 13.05.2004 10.03.2005 02.05.2001 07.04.2004 14.04.2004 16.11.2004 09.07.2002 11.11.2010 06.10.2004 13.01.2000

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 12/04(2009.01)i, H04W 12/08(2009.01)i, H04W 8/18(2009.01)i

B. 조사된 분야

조사된 최소문현(국제특허분류를 기재)

H04W 12/04; G06F 15/00; H04K 1/00; H04L 9/32; H04W 12/06; H04L 9/00

조사된 기술분야에 속하는 최소문현 이외의 문현

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문현란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문현란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 내장UICC, 키 생성 알고리즘, 키 길이

C. 관련 문헌

카테고리*	인용문현명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	EP 2175674 A1 (VODAFONE HOLDING GMBH) 2010.04.14 요약; 문단번호[0025]-[0027],[0047],[0048]; 도면1; 청구항 1,10,11 참조.	1-15
A	KR 10-2008-0077786 A (주식회사 케이티프리텔) 2008.08.26 요약; 문단번호 [0039]-[0051]; 청구항 1,2 참조.	1-15
A	JP 2003-530012 A (NOKIA Co., LTD.) 2003.10.07 요약; 문단번호 [0112]-[0122]; 도면 10; 청구항 1 참조.	1-15
A	US 7382882 B1 (IMMONEN OLLI) 2008.06.03 요약; 도면4; 청구항 1,4,28 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 문현

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후
에 공개된 선출원 또는 특허 문현“L” 우선권 주장에 의문을 제기하는 문현 또는 다른 인용문현의 공개일
또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문현

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문현

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문현

“T” 국제출원일 또는 우선일 후에 공개된 문현으로, 출원과 상충하지
않으면 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된
문현“X” 특별한 관련이 있는 문현. 해당 문현 하나만으로 청구된 발명의 신
규성 또는 진보성이 없는 것으로 본다.“Y” 특별한 관련이 있는 문현. 해당 문현이 하나 이상의 다른 문현과
조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명
은 진보성이 없는 것으로 본다.

“&” 동일한 대응특허문현에 속하는 문현

국제조사의 실제 완료일

2013년 01월 30일 (30.01.2013)

국제조사보고서 발송일

2013년 01월 30일 (30.01.2013)

ISA/KR의 명칭 및 우편주소

대한민국 특허청

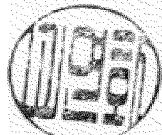
(302-701) 대전광역시 서구 청사로 189,
4동(둔산동, 정부대전청사)

팩스 번호 82-42-472-7140

심사관

고연화

전화번호 82-42-481-8569



국제조사보고서에서
인용된 특허문현

공개일

대응특허문현

공개일

EP 2175674 A1

2010.04.14

없음

KR 10-2008-0077786 A

2008.08.26

없음

JP 2003-530012 A

2003.10.07

AT 309656 T	2005.11.15
AU 2001-26838 A1	2001.10.15
AU 2683801 A	2001.10.15
BR 0109651 A	2003.04.22
CA 2403521 A1	2001.10.11
CA 2403521 C	2009.05.26
CN 1275418 C	2006.09.13
CN 1430835 A	2003.07.16
DE 60114789 D1	2005.12.15
DE 60114789 T2	2006.07.20
EP 1273128 A1	2003.01.08
EP 1273128 B1	2005.11.09
ES 2251459 T3	2006.05.01
FI 20000760 D0	2000.03.31
JP 04723158 B2	2011.04.15
KR 10-0754458 B1	2007.08.31
US 07107620 B2	2006.09.12
US 07512796 B2	2009.03.31
US 2002-0012433 A1	2002.01.31
US 2007-0060106 A1	2007.03.15
WO 2001-076134 A1	2001.10.11
ZA 200207299 A	2003.05.02

US 7382882 B1

2008.06.03

AT 264033 T	2004.04.15
AU 1999-47818 A1	2000.01.24
AU 4781899 A	2000.01.24
BR 9911814 A	2001.10.16
CA 2336479 A1	2000.01.13
CA 2336479 C	2007.11.27
CA 2466390 A1	2000.01.13
CA 2466390 C	2009.10.06
CN 100452700 C	2009.01.14
CN 1126345 C0	2003.10.29
CN 1316152 A0	2001.10.03
CN 1516387 A	2004.07.28
DE 69916277 D1	2004.05.13
DE 69916277 T2	2005.03.10
EP 1095492 A1	2001.05.02
EP 1095492 B1	2004.04.07
EP 1408669 A1	2004.04.14
ES 2219032 T3	2004.11.16
JP 2002-520911 A	2002.07.09
JP 2010-259074 A	2010.11.11
KR 10-0451557 B1	2004.10.06
WO 00-02358 A1	2000.01.13