

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국



(43) 국제공개일
2013년 5월 10일 (10.05.2013) WIPO | PCT

(10) 국제공개번호

WO 2013/066114 A1

(51) 국제특허분류:

H04W 8/30 (2009.01) H04W 12/08 (2009.01)
H04W 8/18 (2009.01)

(21) 국제출원번호:

PCT/KR2012/009201

(22) 국제출원일:

2012년 11월 2일 (02.11.2012)

(25) 출원언어:

한국어

(26) 공개언어:

한국어

(30) 우선권정보:

10-2011-0114552 2011년 11월 4일 (04.11.2011) KR
10-2012-0123718 2012년 11월 2일 (02.11.2012) 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 서
초구 우면동 17 KT 연구개발센터, Seoul (KR).

(74) 대리인: 김은구 (KIM, Eungu) 등; 135-908 서울시 강남
구 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,
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.

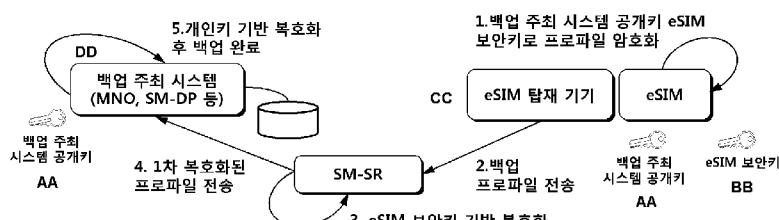
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의
역내 권리의 보호를 위하여): ARIPO (BW, GH, GM,
KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG,
ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ,
TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC,
MK, MT, NL, NO, PL, PT, RO, RS, SE, 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 접
수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

(54) Title: METHOD FOR BACKUP OF PROFILE EXISTING IN EMBEDDED UICC, EMBEDDED UICC, EXTERNAL EN-
TITY AND BACKUP DEVICE

(54) 발명의 명칭: 내장 UICC 내 프로파일 백업 방법, 내장 UICC, 외부 개체 및 백업 장치



AA ... Backup hosting system publication key
BB ... eSIM security key
CC ... Equipment with embedded eSIM
DD ... Backup hosting system (MNO, SM-DP, etc.)
1 ... Encode a profile using the backup hosting system publication key and eSIM security key
2 ... Transmit a backup profile
3 ... eSIM security key-based decoding
4 ... Transmit a primarily decoded profile
5 ... Personal key-based decoding and end the backup process

(57) Abstract: The present invention relates to a technology for managing a profile in an eUICC embedded in a terminal. More particularly, the present invention provides a method for backup of a profile existing in an eUICC to another device, a device for backup of the profile existing in the eUICC and a method for interlinking devices.

(57) 요약서: 본 발명은 단말에 내장된 eUICC 내 프로파일을 관리하는 기술에 관한 것으로서, 특히, eUICC 내 프로파일을 다른 장치에 백업할 수 있도록 해주는 방법과, 이러한 eUICC 내 프로파일 백업을 위한 장치 및 장치 간의 연동 방법을 제공한다.

명세서

발명의 명칭: 내장 UICC 내 프로파일 백업 방법, 내장 UICC, 외부 개체 및 백업 장치

기술분야

- [1] 본 발명은 내장 UICC(eUICC: Embedded Universal Integrated Circuit Card, 이하, "eUICC"라 함) 내 프로파일을 관리하는 기술에 관한 것이다.

배경기술

- [2] UICC(Universal Integrated Circuit Card, 이하 "UICC"라 함)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 내장 UICC(Embedded UICC) 구조가 제안되었다. 내장 UICC는 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 내장 UICC 내의 IMSI를 할당할 수 있다. 단말을 발주하는 이동 통신 사업자 및 단말 제조사는 모두 제품 재고에 신경을 쓸 수밖에 없고 제품 가격이 상승하는 문제가 발생하게 된다. 사용자는 단말에 대해 이동 통신 사업자를 바꿀 수 없는 불편이 있다. 그러므로, 내장 UICC의 경우에도 이동 통신 사업자에 구애받지 않고 사용자가 단말을 개통할 수 있는 방법이 요구된다.

- [6] 한편, 최근 내장 UICC의 도입으로 인하여 여러 이동통신 사업자의 가입자 정보를 원격에서 UICC로 업데이트 할 필요가 생기게 되었고, 그에 따라 가입자 정보 관리를 위한 가입 관리 장치(SM: Subscription Manager, 이하 "SM"이라 함) 또는 프로파일 관리장치(PM: Profile Manager, 이하 "PM"이라 함)가 논의되고

있다.

[7] 이와 같이, 기존의 착탈식 형태의 SIM과는 달리 단말에 일체형으로 탑재되는 Embedded SIM (이하 "eSIM" 라 함)은 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 Vendor 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, Profile)를 eSIM에 발급하고 Subscription 변경에 대한 프로세스를 처리하는 등 eSIM에 대한 전반적인 관리 역할을 수행하는 개체 또는 그 기능/역할을 의미한다. 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 구조를 제안하였다.

[8] eSIM은 프로파일이 소프트웨어적으로 eSIM 내에 발급됨으로써 통신과 부가 서비스를 제공하게 되며, 부가 서비스의 경우 eSIM 발급 이후에 서비스 제공자 (예, 신용카드사, 은행, 증권 등)로부터 후발급 (개인화 과정 - 실제 금융정보들을 발급하는 과정)이 일어나 초기 탑재된 프로파일에 수정이 일어나게 된다.

[9] 이 때, 사용자가 eSIM 지원 타 기기로 기기 변경을 할 경우, 현재 발급 및 부가 서비스 후발급이 완료된 프로파일을 eSIM 인프라(MNO, SM-DP, 서비스 제공자 서버, 제조사 서버, 금융사 서버 등)로 백업하고 이를 다시 신규 eSIM 지원 기기로 탑재(복원)하는 방안이 존재하지 않는다. 백업 기술이 존재하지 않을 경우, 사용자는 eSIM 탑재 기기에서 부가 서비스를 후발급 했을 경우, 신규 eSIM 탑재 기기로 변경했을 때 기존에 사용하던 부가 서비스를 모두 재발급 받아야 하는 상황이 발생하게 된다.

발명의 상세한 설명

기술적 과제

[10] 이러한 배경에서, 본 발명의 목적은, eUICC 내 프로파일을 백업하기 위한 방법을 제공하는 데 있다.

[11] 본 발명의 다른 목적은, eUICC 내 프로파일 백업을 위한 장치들과, 장치 간 연동 방식을 제공해주는 데 있다.

[12] 본 발명의 또 다른 목적은, eUICC 내 프로파일을 다른 장치에 백업함에 있어서, eUICC 내 프로파일 백업이 안전하게 이루어지도록 해주는 데 있다.

[13] 본 발명의 또 다른 목적은, 네트워크에 의해 eUICC 내 프로파일 백업이 트리거 되는 방식과 단말에 의해 의해 eUICC 내 프로파일 백업이 트리거 되는 방식을 제공해주는 데 있다.

과제 해결 수단

[14] 일 측면에서, 본 발명은, 내장 UICC(eUICC: embedded Universal Integrated

Circuit Card) 내 프로파일 백업 방법으로서, 상기 eUICC가 외부 개체와의 연동을 통해 관리되는 상기 eUICC 내 프로파일을 암호화하는 단계; 상기 eUICC가 상기 암호화된 프로파일을 백업 프로파일로서 전송하는 단계; 백업 장치 및 외부 개체 중 하나 이상을 포함하는 복호화 장치가 상기 백업 프로파일을 복호화하는 단계; 및 상기 백업 장치가 상기 복호화된 백업 프로파일을 백업하는 단계를 포함하는 eUICC 내 프로파일 백업 방법을 제공한다.

[15] 다른 측면에서, 본 발명은, 내부 프로파일 백업을 위한 내장 UICC(eUICC: embedded Universal Integrated Circuit Card)로서, 외부 개체와의 연동을 통해 관리되는 상기 eUICC 내 프로파일을 암호화하는 암호화 모듈; 및 상기 암호화 모듈에 의해 상기 암호화된 프로파일을 백업 장치에 백업시키기 위한 백업 프로파일로서 전송하는 통신 모듈을 포함하는 eUICC를 제공한다.

[16] 또 다른 측면에서, 본 발명은, 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 백업을 위한 외부 개체로서, 상기 외부 개체가 관리하는 상기 eUICC 내 프로파일이 암호화된 백업 프로파일을 수신하는 수신 모듈; 상기 암호화된 백업 프로파일을 복호화하는 복호화 모듈; 및 상기 복호화된 백업 프로파일을 상기 백업 장치로 전송하는 전송 모듈을 포함하는 외부 장치를 제공한다.

[17] 또 다른 측면에서, 본 발명은, 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 백업을 위한 백업 장치로서, 외부 개체와의 연동을 통해 관리되는 상기 eUICC 내 프로파일이 암호화된 백업 프로파일을 상기 외부 개체로부터 수신하는 수신 모듈; 상기 암호화된 백업 프로파일을 복호화하는 복호화 모듈; 및 상기 복호화된 백업 프로파일을 백업하는 백업 모듈을 포함하는 백업 장치를 제공한다.

[18] 또 다른 측면에서, 본 발명은, 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 백업 시스템으로서, 외부 개체와의 연동을 통해 관리되는 내부의 프로파일을 암호화하여 백업 프로파일로서 전송하는 eUICC를 내장한 기기; 상기 백업 프로파일을 복호화하는 복호화 장치; 및 상기 복호화된 백업 프로파일을 백업하는 백업 장치를 포함하는 eUICC 내 프로파일 백업 시스템을 제공한다.

도면의 간단한 설명

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

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

[21] 도 3은 본 발명이 적용되는 서비스 아키텍처에서 프로비저닝 과정의 전체 흐름도이다.

[22] 도 4는 본 발명이 적용되는 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.

[23] 도 5는 본 발명의 일 실시 예에 의한 eUICC 환경에서의 프로파일 백업을 위한

시스템 전체 구조를 도시한다.

- [24] 도 6은 본 발명의 일 실시예에 의한 eUICC 환경에서의 프로파일 백업방법의 흐름을 도시하는 것으로, 네트워크 트리거링(Network Triggered) 방식을 도시한다.
- [25] 도 7은 본 발명의 다른 실시예에 의한 eUICC 환경에서의 프로파일 백업방법의 흐름을 도시하는 것으로, 단말 트리거링(Device Triggered) 방식을 도시한다.
- [26] 도 8은 본 발명의 일 실시예에 따른 eUICC 내 프로파일 백업을 위한 시스템을 개략적으로 나타낸 도면이다.
- [27] 도 9는 본 발명의 일 실시예에 따른 eUICC 내 프로파일 백업 방법에 대한 흐름도이다.
- [28] 도 10는 본 발명의 일 실시예에 따른 eUICC 내 프로파일 백업 프로세스 트리거 단계의 상세 흐름도이다.
- [29] 도 11은 본 발명의 일 실시예에 따른 eUICC 내 프로파일 백업 프로세스 트리거 단계의 다른 상세 흐름도이다.
- [30] 도 12는 본 발명의 일 실시예에 따른 eUICC 내 프로파일 백업을 위한 eUICC에 대한 블록도이다.
- [31] 도 13은 본 발명의 일 실시예에 따른 eUICC 내 프로파일 백업을 위한 가입 관리 장치에 대한 블록도이다.
- [32] 도 14는 본 발명의 일 실시예에 따른 eUICC 내 프로파일 백업을 위한 백업 장치에 대한 블록도이다.
- 발명의 실시를 위한 형태**
- [33] 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.
- [34] 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 M2M단말을 제조하게 되면, M2M 단말의 소형화가 힘들게 된다.
- [35] 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.
- [36] 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.

- [37] 이와 같이, 기존의 착탈식 형태의 SIM과는 달리 단말에 일체형으로 탑재되는 내장 SIM(이하 "eSIM" 또는 "eUICC"이라 함)은, 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(Vendor) 등의 유관 회사들과 최상위 구조를 포함한 필요한 요소에 대해 표준화 활동을 전개하고 있다. eSIM이 표준화 단체들을 통해 논의되면서 이슈의 중심에 있는 것은 SM으로서, 중요한 프로파일(Operator Credential, MNO Credential, Profile, eUICC Profile, Profile Package 등으로 불릴 수 있음)를 eSIM에 발급하고 가입 변경에 대한 프로세스를 처리하는 등 eSIM에 대한 전반적인 관리 역할을 수행하는 개체 또는 그 기능/역할을 의미한다.
- [38] 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 구조를 제안하였으나, 세부적이며 기술적인 실제 발급 방식에 대해서는 언급하고 있지 않다.
- [39] 이에 본 발명에서는 GSMA의 SM 역할 분리 환경에서 동적 암호키 (공개 키 등) 생성을 활용하여 eSIM을 관리하는 방안을 제시한다.
- [40] 본 명세서에서는 eSIM과 eUICC를 동등한 개념으로 사용한다.
- [41] 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.
- [42] 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.
- [43] 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.

- [44] 여기서, 관리키 또는 eSIM 관리키 또는 eUICC 관리키는 eSIM으로의 접근 인증키로서 사업자 정보를 안전하게 eSIM으로 전달하기 위한 것이며, 본 발명에서 주로 다루는 암호키(공개키 등)과는 구별되는 개념이며, 아래 설명할 바와 같이 eUICC 접근 크레덴셜(eUICC access credentials)로 표현될 수도 있을 것이다.
- [45] 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.
- [46] 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.
- [47] 본 발명을 설명하기 전에 우선 본 명세서에서 사용할 용어에 대하여 설명한다.
- [48] MNO(Mobile Network Operator)는 이동통신 사업자를 의미하며, 모바일 네트워크를 통해 고객에게 통신 서비스를 제공하는 엔터티를 의미한다.
- [49] SM(Subscription manager)는 가입 관리 장치로서, eUICC의 관리 기능을 수행한다.
- [50] eUICC 공급자(eUICC Supplier)는 eUICC 모듈과 내장 소프트웨어(펌웨어와 오퍼레이팅 시스템 등)를 공급하는 자를 의미한다.
- [51] 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.
- [52] 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.
- [53] 가입(Subscription)은 가입자와 무선통신 서비스 제공자 사이의 서비스 제공을 위한 상업적인 관계를 의미한다.
- [54] 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.

- [55] 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.
- [56] 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.
- [57] 오퍼레이션 프로파일(Operation Profile) 또는 사업자 정보는 사업자 가입(Operational Subscription)과 관련된 모든 종류의 프로파일을 의미한다.
- [58] 도 1은 본 발명이 적용되는 eSIM(eUICC)을 포함한 전체 서비스 아키텍처를 도시한다.
- [59] 전체 시스템에 대해서 설명하면 다음과 같다.
- [60] 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.
- [61] 도 1에서 점선은 신뢰 서클을 도시하고, 2개 실선은 안전한 링크를 의미한다.
- [62] 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.
- [63] 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.
- [64] 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.
- [65] MNO 크레덴셜 또는 프로파일은 K, 알고리즘, 알고리즘 파라미터, 부가 서비스 어플리케이션, 부가 서비스 데이터 등을 포함하는 가입 크레덴셜을 의미할 수 있다.
- [66] 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.

- [67] 오퍼레이터는 자신의 크레덴셜에 대해서 완전한 제어권을 가져야 하며, 오퍼레이터는 SM 오퍼레이션에 대해서 강한 감독권과 제어권한을 가져야 한다.
- [68] SM 기능은 MNO 또는 제3 기관에 의하여 제공되어야 하며, 만약 제3 기관에 의하여 제공된다면 SM과 MNO 사이에는 상업적인 관계가 설정되어 있는 경우 등일 것이다.
- [69] 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.
- [70] 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.
- [71] 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.
- [72] SM의 역할은 SM-SR, SM-DP와 같은 2개의 서브 기능으로 나뉘어 질 수 있다.
- [73] 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 경계지정 필요가 있고, 이들 엔티티들 사이의 인터페이스를 정의할 필요가 있다.
- [74] 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.
- [75] 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.

- [76] 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.
- [77] 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.
- [78] 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.
- [79] 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.
- [80] 도 2는 SM 분리 환경에서 SM-SR 및 SM-DP가 시스템에 위치하는 구성을 도시한다.
- [81] 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.
- [82] 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)
- [83] 도 3은 본 발명이 적용되는 시스템에서 제1차 가입에 해당되는 프로비저닝 과정의 전체 흐름도이다.
- [84] 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)
- [85] 또한, 도시하지는 않았지만, 상기 S320 단계에서는 아래에서 설명할 바와 같이,

eUICC가 자신의 공개키(PK) 또는 프로파일 접근 크레덴셜 정보인 PKI 키정보(키 생성 알고리즘, 키 길이, 키 생성 방식 등)를 해당 MNO 시스템 또는 SM-SR로 제공하는 과정이 포함될 수 있다.

- [86] S330 단계에서 MNO는 SM-SR과 사이에서 eUICC 아이덴티티 검증과, 장치(eUICC)에 대한 정보를 수집한다. S330 단계에서, MNO는 본 발명의 일 실시예에 의하여 해당 eUICC에 대한 암호화 키, 구체적으로는 eUICC에 대응되는 공개키를 SM-SR로부터 획득할 수 있다.
- [87] 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.
- [88] 동적인 암호키 획득방법은 아래에서 설명할 바와 같이, 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, 시큐어리티 정책(Security Policy) 모듈, 크레덴셜 매니저(Credential Manager), 프로파일 매니저(Profile Manager) 등 eUICC 내의 암호키 생성 및 암호키를 활용한 보안 연산을 수행하는 모듈)을 이용하여 공개키를 생성한 후 SM-SR로 전달하는 방식으로 수행될 수 있다. 이에 대해서는 아래에서 더 상세하게 설명한다.
- [89] 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.
- [90] 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) 이때, 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.
- [91] 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)

- [92] 그런 다음, MNO는 이중 암호화(Double Ciphered)된 eUICC 프로파일을 해당 eUICC로 전송한다.(S360 단계) 이때, 인증성을 제공하기 위해 SM-DP의 공개키 또는 인증서(Certification)를 함께 eUICC로 전송할 수 있다.
- [93] 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. 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.
- [94] S370 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.
이러한 각 단계에 대한 주요 구성을 추가로 설명하면 다음과 같다.
- [96] S310단계에서, eUICC 식별 정보(eICCid 등)는 공개된 데이터이며 eUICC 내부에 통합 보호되어야 한다.
- [97] S320, S330단계에서 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.
- [98] 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.
- [99] S370 단계에서, SM-SR 데이터베이스는 가입 설치(Subscription installation)의 마무리 단계에서 업데이트 될 수 있다.
도 4는 본 발명이 적용되는 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.
- [100] 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")
- [102] 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.
- [103] 도 4에 의한 MNO 변경 과정을 구체적으로 설명하면 다음과 같다.
- [104] 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)

- [105] 또한, 도시하지는 않았지만, 상기 S420 단계에서는 아래에서 설명할 바와 같이, eUICC가 자신의 공개키(PK) 또는 프로파일 접근 크레덴셜 정보인 PKI 키정보(키 생성 알고리즘, 키 길이, 키 생성 방식 등)를 해당 MNO 시스템 또는 SM-SR로 제공하는 과정이 포함될 수 있음은 프로비저닝 과정인 S320과 동일하다.
- [106] 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..
- [107] 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.
- [108] 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) 이 때, 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.
- [109] 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.
- [110] 즉, S440" 단계에서는 새로운 MNO(Receiving MNO)가 가입 스위칭에 대해서 도너 MNO의 인증을 요청하며, 이러한 인증은 정책 제어 기능(Policy Control Function)에 의해서 제공될 수 있다.
- [111] 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)
- [112] 그런 다음, MNO는 이중 암호화(Double CIPHERED)된 eUICC 프로파일을 해당 eUICC로 전송한다.(S460 단계) 이 때, 인증성을 제공하기 위해 SM-DP의 공개키 또는 인증서(Certification)를 함께 eUICC로 전송할 수 있다.
- [113] 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. 이 때, eUICC는 인증서 확인 (MNO로부터 획득한 공개키에 해당되는 SM-DP로부터 생성된 eUICC 프로파일인지 확인하기 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.

[114] S470 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.

[115] 이상 도 1 내지 도 4의 방식을 다시 설명하면 아래와 같다.

[116] 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.

[117] 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.

[118] eSIM 환경에서 중요한 요소 중의 하나인 SM은 eSIM은 원격으로 관리키를 통해 통신 및 부가 서비스 데이터를 발급하는 역할을 수행한다. GSMA에서는 SM의 역할을 SM-DP와 SM-SR로 분류하였다. SM-DP는 사업자 정보 (IMSI, K, OPc, 부가 서비스 데이터 등)를 안전하게 빌드하여 크레덴셜 패키지 (Credential Package) 형태로 만드는 역할을 수행하며, SM-SR은 SM-DP가 생성한 크레덴셜 패키지를 OTA 또는 GP SCP (Secure Communication Protocol)과 같은 SIM 원격 관리 기술을 통해 eSIM에 안전하게 다운로드하는 역할을 수행한다. 그리고 GSMA는 아래 그림의 "Circle of Trust"라는 구조를 제안하여 각 유사 개체들간 신뢰 관계의 중첩을 통해 MNO와 eSIM 간의 종단간 (End-to-End) 신뢰 관계를 구축한다는 개념을 제안하였다. 즉, MNO는 SM1과, SM1은 SM4, SM4는 eSIM과 신뢰관계를 형성하여, 이를 통해 MNO와 eSIM 간의 신뢰관계를 형성한다는 개념이다.

[119] 이렇게, eSIM은 프로파일이 소프트웨어적으로 eSIM 내에 발급됨으로써 통신과 부가 서비스를 제공하게 되며, 부가 서비스의 경우 eSIM 발급 이후에 서비스 제공자 (예, 신용카드사, 은행, 증권 등)로부터 후발급 (개인화 과정 - 실제

금융정보들을 발급하는 과정)이 일어나 초기 탑재된 프로파일에 수정이 일어나게 된다.

- [120] 이때, 사용자가 eSIM 지원 타 기기로 기기 변경을 할 경우, 현재 발급 및 부가 서비스 후발급이 완료된 프로파일을 eSIM 인프라 (MNO, SM-DP, 서비스 제공자 서버, 제조사 서버, 금융사 서버 등)로 백업하고 이를 다시 신규 eSIM 지원 기기로 탑재(복원)하는 방안이 존재하지 않는다. 백업 기술이 존재하지 않을 경우, 사용자는 eSIM 탑재 기기에서 부가 서비스를 후발급 했을 경우, 신규 eSIM 탑재 기기로 변경했을 때 기존에 사용하던 부가 서비스를 모두 재발급 받아야 하는 상황이 발생하게 된다.
- [121] 이에 본 발명에서는 GSMA에서 제안한 SM 역할 분리 환경을 기반으로 eSIM 내의 발급 및 후발급된 프로파일을 백업하는 방안을 제시한다.
- [122] 그러나, 본 발명은 전술한 도 3 및 4에 의한 프로비저닝 또는 MNO 변경 과정에 한정하여 적용되는 것은 아니며, 본 발명에서 정의하는 신뢰정보를 이용하여 eUICC와 관련된 개체사이에 신뢰관계를 구축할 수 있는 한, 여하한 다른 환경 또는 시스템에도 적용될 수 있을 것이다.
- [123] 도 5는 본 발명의 일 실시예에 의한 eUICC 환경에서의 프로파일 백업을 위한 시스템 전체 구조를 도시한다.
- [124] 본 발명의 기본적인 상위 구조는 도 1과 같이 GSMA 제안 eSIM 구조를 근간으로 한다.
- [125] 본 발명은 eSIM 내의 모든 프로파일 (발급 이후 부가 서비스 후발급 등으로 인해 변경된 정보 포함)들을 PK(Public Key Cryptography)를 활용하여 안전하게 백업 주체 시스템(예: MNO, SM-DP, 제조사, 서비스 제공자, 금융사 등)로 백업하는 방안을 제시한다.
- [126] 본 발명의 백업 및 복원 대상 정보는 통신 및 부가 서비스의 데이터 및 어플리케이션을 포함하는 프로파일이며, 부가 서비스의 경우, 서비스 제공자(예, 신용카드사, 은행, 증권 등)로부터 후 발급이 완료된 상태의 데이터와 어플리케이션을 의미한다.
- [127] 세부적으로 보면, 통신 영역과 관련해서는 폰북 정보, 개통된 사업자 프로파일 (전화번호 등의 정보가 가입자 정보에 맞게 업데이트된 상태) 등이 될 수 있으며, 부가 서비스 영역은 금융 정보 (예, 사용자의 계좌정보, 신용카드 정보 등)가 발급이 완료된 상태의 부가 서비스 프로파일이 될 수 있다. 이 이외에도 eSIM에 프로파일을 발급할 수 있는 개체의 필요에 의해 생성된 각종 프로파일들이 백업의 대상이 될 수 있다.
- [128] 본 발명의 기본 구조는 도 5와 같으며, 기본적인 동작은 eSIM 내의 프로파일을 백업 주체 시스템의 공개키(예: Profile Backup Credential, Profile Protection Credential, Profile Access Credential 등)를 활용하여 암호화한 후, eSIM 보안키(예: eUICC Access Credential, ISD Key, GP Key, UICC OTA Key 등)로 암호화하여 SM-SR로 전달하면, SM-SR은 이를 복호화한 후 백업 주체 시스템으로 전달하고,

해당 백업 주최 시스템은 자신의 개인키로 최종적인 복호화를 수행함으로써 백업을 수행하게 된다.

- [129] 백업 된 정보는 기본적인 발급 과정에 따라 eSIM 내로 복원되게 된다.
- [130] 본 발명의 백업 동작은 망에서 시작하는 경우와 eSIM 탑재 기기에서 시작하는 경우로 분류할 수 있으며, 이는 도 6 및 도 7과 같으며, 세부적인 내용은 다음과 같다.
 - [131] 도 6은 본 발명의 일 실시 예에 의한 eUICC 환경에서의 프로파일 백업방법의 흐름을 도시하는 것으로, 네트워크 트리거링(Network Triggered) 방식을 도시한다.
 - 네트워크 트리거드 백업 프로세스(Network-Triggered Backup Process)
 - [133] S600 단계: 백업 주최 시스템은 특정 기기의 eSIM 프로파일 백업이 필요할 경우, SM-SR과 연동하여 eSIM 보안키 기반 보안이 적용된 백업 명령을 생성하여 eSIM 탑재 기기로 전송한다. (이때, 백업 주최 시스템의 공개키 또는 공인인증서가 함께 전송될 수 있다.)
 - [134] S602 단계: eSIM은 eSIM 보안키로 해당 명령의 인증 및 복호화를 수행한 후, 백업 주최 시스템의 공개키로 eSIM 내의 프로파일을 암호화 한 후, eSIM 보안키로 재암호화를 수행한다. (이때, 백업 주최 시스템의 공개키는 제3의 기관으로부터 획득할 수 있으며, eSIM은 자신이 암호화한 데이터에 대해서 자신의 개인키로 서명을 하여 서명 정보를 추가할 수 있다.)
 - [135] S604 단계: eSIM에 의해 이중 암호화된 백업 프로파일은 SM-SR에 전송된다.
 - [136] S606 단계: SM-SR이 이중 암호화된 백업 프로파일을 eSIM 보안키로 복호화한다.
 - [137] S608 단계: SM-SR에 의해 복호화된 백업 프로파일(백업 사업자 정보)는 백업 주최 시스템으로 전송된다.
 - [138] S610 단계: 백업 주최 시스템은 SM-SR로부터 전달 받은 백업 사업자 정보를 자신의 개인키로 복호화하여 백업 과정을 수행한다. (이때, 전자서명이 포함될 경우, eSIM의 공개키로 서명 검증을 수행할 수 있다.)
 - [139] 도 7은 본 발명의 다른 실시 예에 의한 eUICC 환경에서의 프로파일 백업방법의 흐름을 도시하는 것으로, 단말 트리거링(Device Triggered) 방식을 도시한다.
 - eSIM 탑재 기기 트리거드 백업 프로세스(Terminal Triggered Backup Process)
 - [141] S700 단계: eSIM 탑재 기기는 백업 주최 시스템에 eSIM 보안키로 암호화된 백업 명령(백업 요청)을 전송한다.
 - [142] S702 단계: 백업 주최 시스템은 전송받은 암호화된 백업 명령을 SM-SR에 전달하여 복호화를 요청한 후, SM-SR로부터 응답을 받는다.
 - [143] S704 단계: 백업 주최 시스템은 SM-SR과 연동하여 eSIM 보안키 기반 보안이 적용된 백업 승인 명령(백업 명령에 대한 응답)을 생성한다.
 - [144] S706 단계: 백업 주최 시스템은 백업 승인 명령을 eSIM 탑재 기기로 전송한다. (이때, 백업 주최 시스템의 공개키 또는 공인인증서가 함께 전송될 수 있다.)

- [145] S708 단계: eSIM은 eSIM 보안키로 해당 명령의 인증 및 복호화를 수행한 후, 백업 주최 시스템의 공개키로 eSIM 내의 사업자 정보를 암호화한 후, eSIM 보안키로 재암호화를 수행한다. (이때, 백업 주최 시스템의 공개키는 제3의 기관으로부터 획득할 수 있으며, eSIM은 자신이 암호화한 데이터에 대해서 자신의 개인키로 서명을 하여 서명 정보를 추가할 수 있다.)
- [146] S710 단계: eSIM에 의해 이중 암호화된 백업 프로파일은 SM-SR에 전송된다.
- [147] S712 단계: SM-SR은 eSIM 보안키로 이중 암호화된 백업 프로파일을 복호화한다.
- [148] S714 단계: SM-SR은 복호화된 백업 프로파일을 백업 주최 시스템으로 전송한다.
- [149] S716 단계: 백업 주최 시스템은 SM-SR로부터 전달받은 백업 프로파일을 자신의 개인키로 복호화하여 백업 과정을 수행한다. (이때, 전자서명이 포함될 경우, eSIM의 공개키로 서명 검증을 수행할 수 있다.)
- [150] 이상의 본 발명의 일 실시예를 이용하면, GSMA에서 제안한 SM 역할 분리 환경에서 프로파일(개통, 후발급, 사용자 정보 입력 등을 통한 변경내역 포함)을 안전하게 eSIM 인프라로 백업하고 신규 eSIM 탑재 기기로 복원하는 것이 가능하게 된다. 이를 통해 eSIM 탑재 기기에서도 기존 USIM이 갖고 있던 서비스 연속성(단말 변경 시에도 USIM 내에 저장된 서비스는 USIM과 함께 지속적으로 유지됨)을 제공할 수 있다. 또한, eSIM 탑재 기기 간에 필요 시 프로파일 교환이 가능하게 된다.
- [151] 이하에서는, 이상에서 설명한 eUICC 내 프로파일을 백업하기 위한 방법을 다시 한번 정리하여 설명한다. 단, 아래에서는 위에서 언급된 백업 주최 시스템을 백업 장치로 기재한다. 또한, 전술한 바와 같이, 본 명세서에서는 eSIM과 eUICC은 동등한 개념으로 사용되고 있으나, 아래에서는, 설명의 편의를 위해, eUICC로 통일하여 기재한다.
- [152] 도 8은 본 발명의 일 실시예에 따른 eUICC(810) 내 프로파일 백업을 위한 시스템(eUICC 내 프로파일 백업 시스템)을 개략적으로 나타낸 도면이다.
- [153] 도 8을 참조하면, 본 발명의 일 실시예에 따른 eUICC(810) 내 프로파일 백업을 위한 시스템은, 외부 개체와의 연동을 통해 관리되는 내부의 프로파일을 암호화하여 백업 프로파일로서 전송하는 eUICC(810)를 내장한 기기(800, '단말'이라고도 함)와, eUICC(810)에서 암호화된 프로파일인 백업 프로파일을 복호화하는 복호화 장치와, 복호화 장치에 의해 복호화된 백업 프로파일을 백업하는 백업 장치(830) 등을 포함한다.
- [154] 전술한 복호화 장치는, 외부 개체 및 백업 장치(830) 중 하나 이상을 포함할 수 있다.
- [155] 위에서 언급된 바와 같이, eUICC(810) 내 프로파일을 관리하고 복호화 기능도 가질 수 있는 외부 개체(External Entity)는, 외부 장치(External Apparatus)라고도 하는데, 일 예로, 도 8에 도시된 가입 관리 장치(SM: Subscription Manager, 820)

- 또는 프로파일 관리장치(PM: Profile Manager) 등일 수 있다.
- [156] 이하 설명에서는, 설명의 편의상, 외부 개체를 가입 관리 장치(820)로 기재하여 설명한다.
- [157] 그리고, 가입 관리 장치(820)는, 사업자 정보 (Operator Credential Profile)를 eUICC(810)에 발급하고 가입 변경에 대한 프로세스를 처리하는 등 eUICC(810)에 대한 전반적인 관리 역할을 수행하는 개체 또는 그 기능/역할을 의미할 수 있다. 이러한 가입 매니저는, 역할 측면에서, 사업자 정보를 생성하는 역할을 수행하는 SM-DP(Data Preparation)와 eUICC(810)에 사업자 정보의 직접적 운반을 수행하는 SM-SR(Secure Routing)로 분류할 수 있으며, 도 8 내지 도 14를 참조하여 설명하는 가입 관리 장치(820)는 SM-SR(Secure Routing)일 수 있다.
- [158] 도 9는 본 발명의 일 실시 예에 따른 eUICC(810) 내 프로파일 백업 방법에 대한 흐름도이다.
- [159] 도 9를 참조하면, 본 발명의 일 실시 예에 따른 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 백업 방법은, eUICC가 가입 관리 장치(820)와의 연동을 통해 관리되는 eUICC 내 프로파일을 암호화하는 단계(S902)와, eUICC가 암호화된 프로파일을 백업 프로파일로서 전송하는 단계(S904)와, 백업 장치(830) 및 가입 관리 장치(820) 등 중 하나 이상을 포함하는 복호화 장치가 백업 프로파일을 복호화하는 단계(S906)와, 백업 장치(830)가 복호화 장치에 의해 복호화된 백업 프로파일을 백업하는 단계(S908) 등을 포함한다.
- [160] 전술한 S902 단계에서, eUICC는, 1개의 암호화 키 또는 2개 이상의 암호화 키를 이용하여 eUICC 내 프로파일을 암호화할 수 있다.
- [161] 이에 따라, 전술한 S906 단계에서, 백업 장치(830) 및 가입 관리 장치(820) 등 중 하나 이상을 포함하는 복호화 장치는, 1개의 복호화 키 또는 2개 이상의 복호화 키를 이용하여 eUICC에서 전송된 백업 프로파일을 복호화한다.
- [162] 여기서, 암호화 키는, 암호화 방식에 따라 달라질 수 있는데, 일 예로, 백업 장치 공개키 및 eUICC 보안키 등 중 하나 이상을 포함하고, 복호화 키는 암호화 방식과 대응되는 복호화 방식에 따라 달라질 수 있는데, 일 예로, 백업 장치 개인키 및 eUICC 보안키 등 중 하나 이상을 포함할 수 있다.
- [163] 위에서 언급한 백업 장치 공개키는, 일 예로, 프로파일 백업 크레덴셜(Profile Backup Credential), 프로파일 프로텍션 크레덴셜(Profile Protection Credential) 및 프로파일 액세스 크레덴셜(Profile Access Credential) 등 중 하나일 수 있다.
- [164] 또한, eUICC 보안키는, 일 예로, eUICC 액세스 크레덴셜(eUICC Access Credential), ISD(Issuer Security Domain) 키, GP Key, UICC OTA 키 등 중 하나일 수 있다.
- [165] 만약, S902 단계에서, eUICC가 2개의 암호화 키(1차 암호화 키, 2차 암호화 키)를 이용하여 eUICC 내 프로파일을 암호화하는 경우, S902 단계에서, eUICC는, 1차 암호화 키를 이용하여 eUICC 내 프로파일을 1차 암호화하고, 2차

암호화 키를 이용하여 1차 암호화된 프로파일을 2차 암호화할 수 있다. 여기서, 일 예로, 1차 암호화 키는 백업 장치 공개키이고, 2차 암호화 키는 eUICC 보안키일 수 있다. 아래에서는, 설명의 편의를 위해, 1차 암호화 키는 백업 장치 공개키로, 2차 암호화 키는 eUICC 보안키로 기재한다.

- [166] 이에 따라, 전술한 S906 단계에서, 백업 장치(830) 및 가입 관리 장치(820)를 포함하는 복호화 장치는, 2개의 암호화 키를 이용하여, eUICC에서 이중으로 암호화된 프로파일인 백업 프로파일을 2차례 복호화할 수 있다.
- [167] 즉, S906 단계에서, 가입 관리 장치(820)는 eUICC 보안키를 이용하여 eUICC에서 전송된 백업 프로파일(이중으로 암호화된 프로파일)을 1차 복호화 키로 1차 복호화하고, 이후, 백업 장치(830)가 가입 관리 장치(820)에 의해 1차 복호화된 백업 프로파일을 2차 복호화 키로 2차 복호화할 수 있다. 여기서, 일 예로, 1차 복호화 키는 eUICC 보안키이고, 2차 복호화 키는 백업 장치 개인키일 수 있다. 아래에서는, 설명의 편의를 위해, 1차 복호화 키는 eUICC 보안키로, 2차 복호화 키는 백업 장치 개인키로 기재한다.
- [168] 본 명세서에서 기재된 eUICC 내 프로파일(들)은, 통신 서비스 및 부가 서비스 중 하나 이상과 관련된 데이터 및 애플리케이션 중 하나 이상을 포함할 수 있다.
- [169] 여기서, eUICC 내 프로파일(들)은, 통신 서비스와 관련하여, 일 예로, 폰북(Phonebook) 정보 및 개통된 사업자 프로파일 중 하나 이상을 포함할 수 있다. eUICC 내 프로파일(들)은, 부가 서비스와 관련하여, 일 예로, 서비스 제공자(예: 신용카드사, 은행, 증권 등)으로부터 발급이 완료된 상태의 데이터 및 애플리케이션 중 하나 이상을 포함할 수 있다.
- [170] 또한, 본 명세서에서 기재된 eUICC 내 프로파일(들)은, 통신 서비스 및 부가 서비스 중 하나 이상과 관련된 데이터 및 애플리케이션 중 하나 이상뿐만 아니라, eUICC에 프로파일을 발급할 수 있는 개체(Entity)의 필요에 의해 생성된 각종 프로파일을 포함할 수도 있다.
- [171] 한편, S902 단계부터 진행되는 eUICC 내 프로파일 백업 프로세스는, 네트워크에서 트리거되는 방식일 수도 있고(네트워크 트리거드 백업 프로세스(Network-Triggered Backup Process)), eUICC 또는 eUICC를 내장하는 기기(단말)에서 트리거되는 방식일 수도 있다(단말 트리거드 백업 프로세스(Terminal-Triggered Backup Process)).
- [172] 즉, eUICC 내 프로파일 백업 프로세스의 시작 단계인 S902 단계 이전에, 백업 장치(830)가 백업 명령을 전송하거나(네트워크 트리거드 백업 프로세스), 상기 eUICC 또는 상기 eUICC를 내장한 기기가 백업 명령을 전송(단말 트리거드 백업 프로세스)함으로써, eUICC 내 프로파일 백업 프로세스를 트리거하는 단계(S900)를 더 포함할 수 있다.
- [173] 아래에서는, 도 10 및 도 11을 참조하여, 네트워크 트리거드 백업 프로세스(도 6 참조)를 위한 S900 단계와, 단말 트리거드 백업 프로세스(도 7 참조)를 위한 S900 단계에 대하여 더욱 상세하게 설명한다.

- [174] 면자, 도 10을 참조하여, 네트워크 트리거드 백업 프로세스(도 6 참조)를 위한 S900 단계에 대하여 더욱 상세하게 설명한다.
- [175] 도 10을 참조하면, S900 단계는, 백업 장치(830)가 eUICC 내 프로파일의 백업이 필요한 경우 가입 관리 장치(820)와 백업 명령 암호화 요청 응답 절차를 통해 eUICC 보안키 기반의 암호화된 백업 명령을 생성하는 단계(S1000)와, 백업 장치(830)가 eUICC 보안키 기반의 암호화된 백업 명령을 eUICC 또는 eUICC를 내장한 기기로 전송하는 단계(S1002) 등을 포함한다.
- [176] 전술한 S1000 단계 및 S1002 단계는, 네트워크 트리거드 백업 프로세스를 도시한 도 6의 S600 단계이다.
- [177] 전술한 S1000 단계에서, 백업 장치(830)는, eUICC 보안키 기반의 암호화된 백업 명령과 함께, 백업 장치 공개키 또는 공인 인증서를 eUICC를 내장한 기기로 전송할 수 있다.
- [178] 전술한 S1000 및 S1002 단계를 포함하는 S900 단계 이후에 수행되는 S902 단계에서, eUICC는, S10S10S10계에서 백업 장치(830)로부터 전송받은 백업 명령(eUICC 보안키 기반의 암호화된 백업 명령)을 eUICC 보안키로 인증 및 복호화한 이후, eUICC 내 프로파일을 암호화한다.
- [179] 다음으로, 도 11을 참조하여, 단말 트리거드 백업 프로세스(도 7 참조)를 위한 S900 단계에 대하여 더욱 상세하게 설명한다.
- [180] 도 11을 참조하면, 단말 트리거드 백업 프로세스를 위한 S900 단계에서, eUICC 또는 eUICC를 내장한 기기는, eUICC 내 프로파일의 백업이 필요한 경우, 백업 명령(백업 요청)을 백업 장치(830)로 전송하고, 백업 장치(830)로부터 백업 명령에 대한 응답으로서 백업 승인 명령을 수신한다. 이에 따라, S902 단계가 진행됨으로써 단말 트리거드 백업 프로세스가 시작된다.
- [181] 도 11을 참조하여 더욱 상세하게 설명하면, 단말 트리거드 백업 프로세스를 위한 S900 단계는, eUICC 또는 eUICC를 내장한 기기가, eUICC 보안키 기반의 암호화된 백업 명령을 백업 장치(830)로 전송하는 단계(S1100)와, 백업 장치(830)가, 가입 관리 장치(820)와 백업 명령 복호화 요청 응답 절차를 통해 eUICC 보안키 기반의 암호화된 백업 명령을 복호화하는 단계(S1102)와, 백업 장치(830)가 가입 관리 장치(820)와 백업 승인 명령 암호화 요청 응답 절차를 통해 eUICC 보안키 기반의 암호화된 백업 승인 명령을 생성하는 단계(S1104)와, 백업 장치(830)가 eUICC 또는 eUICC를 내장한 기기로 eUICC 보안키 기반의 암호화된 백업 승인 명령을 전송하는 단계(S1106) 등을 포함한다.
- [182] 도 11의 각 단계를 도 7의 단계와 대응시켜보면, S1100 단계는 S700 단계와 대응되고, S1102 단계는 S702 단계와 대응되고, S1104 단계 및 S1106 단계는 S704 단계와 대응된다.
- [183] 전술한 S1106 단계에서, 백업 장치(830)는, eUICC 보안키 기반의 암호화된 백업 승인 명령과 함께, 백업 장치 공개키 또는 공인 인증서를 eUICC를 내장한 기기로 전송할 수 있다.

- [184] 전술한 S1106 단계 이후, 즉, S900 단계 이후 수행되는 S902 단계에서 eUICC는, eUICC 보안키 기반의 암호화된 백업 승인 명령을 eUICC 보안키로 인증 및 복호화한 이후, eUICC 내 프로파일을 암호화할 수 있다.
- [185] 아래에서는, 이상에서 설명한 eUICC 내 프로파일 백업에 관여하는 eUICC, 가입 관리 장치(820) 및 백업 장치(830) 각각에 대하여 다시 설명한다.
- [186] 도 12는 본 발명의 일 실시예에 따른 eUICC 내 프로파일 백업을 위한 기기(800)에 내장된 eUICC(810)에 대한 블록도이다.
- [187] 도 12를 참조하면, 본 발명의 일 실시예에 따른 eUICC(810) 내 프로파일 백업을 위한 eUICC(810)는, 가입 관리 장치(820)와의 연동을 통해 관리되는 eUICC(810) 내 프로파일을 암호화하는 암호화 모듈(1220)과, 암호화 모듈(1220)에 의해 암호화된 프로파일을 백업 장치(830)에 백업시키기 위한 백업 프로파일로서 전송하는 통신 모듈(1230) 등을 포함한다.
- [188] 전술한 암호화 모듈(1220)은, eUICC(810) 내 프로파일을 1차례만 암호화할 수도 있고, 더 높은 보안성을 위해 여러 차례 암호화할 수 있다.
- [189] 만약, 이중으로 암호화하는 경우, 암호화 모듈(1220)은, 일 예로, eUICC(810) 내 프로파일을 백업 장치 공개키로 1차 암호화하고, 1차 암호화된 프로파일을 eUICC 보안키로 2차 암호화할 수 있다.
- [190] 한편, eUICC(810) 내 프로파일을 백업하기 위해, eUICC(810)가 eUICC(810) 내 프로파일을 암호화하고 이를 백업 프로파일로서 전송함으로써 시작되는 eUICC(810) 내 프로파일 백업 프로세스는, 네트워크(즉, 백업 장치(830))에 의해 트리거될 수도 있고, 단말(800, 즉, eUICC(810))에 의해 트리거될 수도 있다.
- [191] 만약, eUICC(810) 내 프로파일 백업 프로세스가 네트워크(즉, 백업 장치(830))에 의해 트리거되는 경우, 암호화 모듈(1220)은, 백업 장치(830)로부터 백업 명령의 수신에 따라 eUICC(810) 내 프로파일을 암호화할 수 있다.
- [192] 이때, 백업 장치(830)로부터 수신한 백업 명령은 eUICC 보안키 기반의 암호화된 명령이고, 암호화 모듈(1220)은 eUICC 보안키 기반의 암호화된 백업 명령을 복호화한 이후, 1개 또는 2개 이상의 암호화 키를 이용하여 eUICC(810) 내 프로파일을 암호화할 수 있다.
- [193] 만약, eUICC(810) 내 프로파일 백업 프로세스가 단말(즉, eUICC(810))에 의해 트리거되는 경우, eUICC(810)는, eUICC(810) 내 프로파일의 백업이 필요한 경우, 백업 명령을 백업 장치(830)로 전송하고 백업 승인 명령을 백업 장치(830)로부터 수신하는 백업 트리거 모듈(1210)을 더 포함할 수 있다.
- [194] 이러한 백업 트리거 모듈(1210)을 더 포함하는 경우, 즉, 백업 장치(830)로 백업 명령(백업 요청)을 전송한 이후 백업 장치(830)로부터 백업 승인 명령을 수신하는 경우, 암호화 모듈(1220)은, 백업 장치(830)로부터의 백업 승인 명령의 수신에 따라 eUICC(810) 내 프로파일을 암호화할 수 있다.
- [195] 이때, 백업 장치(830)로 전송한 백업 명령은 eUICC 보안키 기반의 암호화된 명령이고, 백업 장치(830)로부터 수신한 백업 승인 명령은 eUICC 보안키 기반의

암호화된 명령일 수 있다.

- [196] 도 13은 본 발명의 일 실시예에 따른 eUICC(810) 내 프로파일 백업을 위한 가입 관리 장치(820)에 대한 블록도이다.
- [197] 도 13을 참조하면, 본 발명의 일 실시예에 따른 eUICC(810) 내 프로파일 백업을 위한 가입 관리 장치(820)는, 가입 관리 장치(820)가 관리하는 eUICC(810) 내 프로파일이 암호화된 백업 프로파일을 수신하는 수신 모듈(1310)과, 암호화된 백업 프로파일을 복호화하는 복호화 모듈(1320)과, 복호화된 백업 프로파일을 백업 장치(830)로 전송하는 전송 모듈(1330) 등을 포함한다.
- [198] 수신 모듈(1310)이 수신한 백업 프로파일은, eUICC(810) 내 프로파일이 이중으로 암호화된 것일 수 있다. 일 예로, 백업 프로파일은 eUICC(810) 내 프로파일이 백업 장치 공개키로 1차 암호화되고 eUICC 보안키로 2차 암호화되어 있을 수 있다.
- [199] 이 경우, 복호화 모듈(1320)은, 백업 장치 공개키로 1차 암호화되고 eUICC 보안키로 2차 암호화된 프로파일인 백업 프로파일을 eUICC 보안키로 1차 복호화하할 수 있다. 이때, 1차 복호화된 백업 프로파일은 백업 장치(830)에서 2차 복호화될 수 있다.
- [200] 한편, eUICC(810) 내 프로파일 백업 프로세스는, 네트워크(즉, 백업 장치(830))에 의해 트리거될 수도 있고, 단말(800, 즉, eUICC(810))에 의해 트리거될 수도 있다.
- [201] 이와 관련하여, 가입 관리 장치(820)는, 도 13에 도시된 바와 같이, 백업 장치(830) 및/또는 단말)에 의한 eUICC(810) 내 프로파일 백업 프로세스를 트리거하는 것을 지원해주는 백업 트리거 지원 모듈(1340)을 더 포함할 수 있다.
- [202] 만약, eUICC(810) 내 프로파일 백업 프로세스가 백업 장치(830))에 의해 트리거되는 경우, 백업 트리거 지원 모듈(1340)은, 백업 장치(830)가 eUICC(810) 내 프로파일 백업 프로세스를 트리거 하기 위한 백업 명령을 암호화하여 eUICC(810) 또는 eUICC(810)를 내장한 기기(800)로 전송할 수 있도록, 백업 장치(830)와 연동하여 백업 명령이 암호화되도록 지원할 수 있다.
- [203] 즉, 백업 트리거 지원 모듈(1340)은, 도 6의 S600 단계 및 도 10의 S1000 단계에서와 같이, 백업 장치(820)의 백업 명령 암호화 요청에 대하여, 백업 명령을 암호화하여 암호화된 백업 명령을 백업 명령 암호화 요청에 대한 응답으로서 백업 장치(820)에 전송할 수 있다.
- [204] 여기서, 백업 명령에 대한 암호화는, 일 예로, eUICC 보안키 기반의 암호화일 수 있다.
- [205] 만약, eUICC(810) 내 프로파일 백업 프로세스가 eUICC(810) 또는 eUICC(810)를 내장한 기기(800)에 의해 트리거되는 경우, 백업 트리거 지원 모듈(1340)은, eUICC(810) 또는 eUICC(810)를 내장한 기기(800)가 eUICC(810) 내 프로파일 백업 프로세스를 트리거 하기 위해 백업 장치(830)로 전송한 암호화된 백업 명령이 복호화되도록 지원하고, 백업 장치(830)가 백업 승인 명령을 암호화하여

eUICC(810) 또는 eUICC(810)를 내장한 기기(800)로 전송할 수 있도록 백업 승인 명령이 암호화되도록 지원할 수 있다.

- [206] 더욱 상세하게, 백업 트리거 지원 모듈(1340)은, eUICC(810)가 백업 장치(830)로 전송한 암호화된 백업 명령이 복호화되도록 지원하기 위하여, 도 7의 S702 단계 및 도 11의 S1102 단계에서와 같이, 백업 장치(820)의 백업 명령 복호화 요청에 대하여, 암호화된 백업 명령을 복호화하여 복호화된 백업 명령을 백업 명령 복호화 요청에 대한 응답으로서 백업 장치(820)에 전송할 수 있다.
- [207] 또한, 백업 트리거 지원 모듈(1340)은, 백업 승인 명령을 암호화하는 것을 지원해주기 위하여, 도 7의 S704 단계 및 도 11의 S1104 단계에서와 같이, 백업 장치(820)의 백업 승인 명령 암호화 요청에 대하여, 백업 승인 명령을 암호화하여 암호화된 백업 승인 명령을 백업 승인 명령 암호화 요청에 대한 응답으로서 백업 장치(820)에 전송할 수 있다.
- [208] 이 때, eUICC(810)에서 백업 장치(820)로 전송된 백업 명령에 대한 복호화는 eUICC 보안키 기반의 복호화이고, 백업 승인 명령에 대한 암호화는, eUICC 보안키 기반의 암호화일 수 있다.
- [209] 도 13에 도시된 가입 관리 장치(820)는, 일 예로, 가입 매니저(SM: Subscription Manager)일 수 있으며, 이에 제한되지 않고, 그 기능 및 역할 등만 유사하다면 그 어떠한 장치로도 구현이 가능할 것이다.
- [210] 여기서, 가입 관리 장치(820)가 가입 매니저(SM: Subscription Manager)로 구현된 경우, 가입 매니저는, 사업자 정보 (Operator Credential Profile)를 eUICC(810)에 발급하고 가입 변경에 대한 프로세스를 처리하는 등 eUICC(810)에 대한 전반적인 관리 역할을 수행하는 개체 또는 그 기능/역할을 의미한다. 이러한 가입 매니저는, 역할 측면에서, 사업자 정보를 생성하는 역할을 수행하는 SM-DP(Data Preparation)와 eUICC(810)에 사업자 정보의 직접적 운반을 수행하는 SM-SR(Secure Routing)로 분류할 수 있으며, 도 8 내지 도 14를 참조하여 설명하는 가입 관리 장치(820)는 SM-SR(Secure Routing)일 수 있다.
- [211] 도 14는 본 발명의 일 실시예에 따른 eUICC(810) 내 프로파일 백업을 위한 백업 장치(830)에 대한 블록도이다.
- [212] 도 14를 참조하면, 본 발명의 일 실시예에 따른 eUICC(810) 내 프로파일 백업을 위한 백업 장치(830)는, 가입 관리 장치(820)와의 연동을 통해 관리되는 eUICC(810) 내 프로파일이 암호화된 백업 프로파일을 가입 관리 장치(820)로부터 수신하는 수신 모듈(1410)과, 암호화된 백업 프로파일을 복호화하는 복호화 모듈(1420)과, 복호화된 백업 프로파일을 백업하는 백업 모듈(1430) 등을 포함한다.
- [213] 전술한 수신 모듈(1410)이 가입 관리 장치(820)로부터 수신한 백업 프로파일은, eUICC(810) 내 프로파일이 백업 장치 공개키로 1차 암호화되고 eUICC 보안키로 2차 암호화된 백업 프로파일이 가입 관리 장치(820)에서 1차 복호화된 백업 프로파일이다.

- [214] 즉, eUICC(810) 내 프로파일은, eUICC(810)에서 1차, 2차 암호화되고, 이렇게 이중으로 암호화된 프로파일(즉, 백업 프로파일)은 가입 관리 장치(820)에서 1차 복호화가 되고, 백업 장치(830)에서 2차 복호화가 된다.
- [215] 전술한 복호화 모듈(1420)은, 가입 관리 장치(820)에서 1차 복호화된 백업 프로파일을 백업 장치 개인키로 2차 복호화할 수 있다.
- [216] 한편, eUICC(810) 내 프로파일 백업 프로세스는, 네트워크(즉, 백업 장치(830))에 의해 트리거될 수도 있고, 단말(800, 즉, eUICC(810))에 의해 트리거될 수도 있다.
- [217] 만약, eUICC(810) 내 프로파일 백업 프로세스가 백업 장치(830)에 의해 트리거되는 경우, 백업 장치(830)는 eUICC(810) 내 프로파일 백업 프로세스를 트리거하기 위한 백업 트리거 모듈(1440)를 포함할 수 있다.
- [218] 이러한 백업 트리거 모듈(1440)은, 백업 장치(830)가 eUICC(810) 내 프로파일 백업 프로세스를 트리거 하기 위한 백업 명령을 eUICC(810) 또는 eUICC(810)를 내장한 기기(800)로 전송할 수 있다.
- [219] 또한, 백업 트리거 모듈(1440)은, 백업 명령을 전송함에 있어서, 가입 관리 장치(820)와 연동을 통해, 즉, 가입 관리 장치(820)의 백업 트리거 지원 모듈(1340)과 연동하여, 백업 명령을 암호화하여 전송할 수 있다.
- [220] 이 때, 백업 명령에 대한 암호화는, eUICC 보안키 기반의 암호화일 수 있다.
- [221] 만약, eUICC(810) 내 프로파일 백업 프로세스가 eUICC(810) 또는 eUICC(810)를 내장한 기기(800)에 의해 트리거 되는 경우, 백업 장치(830)는, eUICC(810) 또는 eUICC(810)를 내장한 기기(800)가 프로파일 백업 프로세스를 트리거 하는 것과 관련된 기능을 수행하기 위한 백업 트리거 지원 모듈(1450)을 더 포함할 수 있다.
- [222] 이러한 백업 트리거 지원 모듈(1450)은, eUICC(810) 또는 eUICC(810)를 내장한 기기(800)가 eUICC(810) 내 프로파일 백업 프로세스를 트리거 하기 위해 전송한 백업 명령을 수신하여 백업 승인 명령을 eUICC(810) 또는 eUICC(810)를 내장한 기기(800)로 전송할 수 있다.
- [223] 더욱 상세하게는, 백업 트리거 지원 모듈(1450)은, eUICC(810) 또는 eUICC(810)를 내장한 기기(800)가 eUICC(810) 내 프로파일 백업 프로세스를 트리거 하기 위해 전송한 암호화된 백업 명령을 수신하여, 암호화된 백업 명령을 가입 관리 장치(820)와 연동하여 복호화하고, 이후, 가입 관리 장치가 입 관리 장치가 입 관리 장치인 명령을 암호화하여 eUICC(810) 또는 eUICC(810)를 내장한 기기(800)로 전송할 수 있다.
- [224] 이 때, 일 예로, 암호화된 백업 명령에 대한 복호화는 eUICC 보안키 기반의 복호화이고, 백업 승인 명령에 대한 암호화는, eUICC 보안키 기반의 암호화일 수 있다.
- [225] 이상에서 설명한 본 발명에 의하면, eUICC 내 프로파일을 백업하기 위한 방법을 제공할 수 있다.
- [226] 또한, 본 발명에 의하면, eUICC 내 프로파일 백업을 위한 장치들과, 장치 간

연동 방식을 제공해줄 수 있다.

- [227] 또한, 본 발명에 의하면, eUICC 내 프로파일을 다른 장치에 백업함에 있어서, eUICC 내 프로파일 백업이 안전하게 이루어지도록 해주는 데 있다.
- [228] 또한, 본 발명에 의하면, 네트워크에 의해 eUICC 내 프로파일 백업이 트리거 되는 방식과 단말에 의해 의해 eUICC 내 프로파일 백업이 트리거 되는 방식을 제공해줄 수 있다. 따라서, 필요에 따라 두 방식 중 하나를 선택적으로 이용할 수 있다.
- [229] 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.

CROSS-REFERENCE TO RELATED APPLICATION

- [230] 본 특허출원은 2011년 11월 4일 한국에 출원한 특허출원번호 제 10-2011-0114552 호 및 2012년 11월 2일 한국에 출원한 특허출원번호 제 10-2012-0123718 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]

내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내
프로파일 백업 방법으로서,
상기 eUICC가 외부 개체와의 연동을 통해 관리되는 상기 eUICC
내 프로파일을 암호화하는 단계;
상기 eUICC가 상기 암호화된 프로파일을 백업 프로파일로서
전송하는 단계;
백업 장치 및 외부 개체 중 하나 이상을 포함하는 복호화 장치가
상기 백업 프로파일을 복호화하는 단계; 및
상기 백업 장치가 상기 복호화된 백업 프로파일을 백업하는
단계를 포함하는 eUICC 내 프로파일 백업 방법.

[청구항 2]

제1항에 있어서,
상기 암호화하는 단계에서, 상기 eUICC는, 1개의 암호화 키 또는
2개 이상의 암호화 키를 이용하여 상기 eUICC 내 프로파일을
암호화하고,
상기 복호화하는 단계에서, 상기 복호화 장치는, 1개의 복호화 키
또는 2개 이상의 복호화 키를 이용하여 상기 eUICC에서 전송된
상기 백업 프로파일을 복호화하는 것을 특징으로 하는 eUICC 내
프로파일 백업 방법.

[청구항 3]

제1항에 있어서,
상기 암호화하는 단계에서,
상기 eUICC는, 1차 암호화 키를 이용하여 상기 eUICC 내
프로파일을 1차 암호화하고, 2차 암호화 키를 이용하여 상기 1차
암호화된 프로파일을 2차 암호화하며,
상기 복호화하는 단계에서,
상기 외부 개체는 1차 복호화 키를 이용하여 상기 eUICC에서
전송된 상기 백업 프로파일을 1차 복호화하고, 상기 백업 장치는
2차 복호화 키를 이용하여 상기 1차 복호화된 백업 프로파일을 2차
복호화하는 것을 특징으로 하는 eUICC 내 프로파일 백업 방법.

[청구항 4]

제3항에 있어서,
상기 1차 암호화 키는 백업 장치 공개키이고, 상기 2차 암호화 키는
eUICC 보안키이며, 상기 1차 복호화 키는 eUICC 보안키이고, 상기
2차 복호화 키는 백업 장치 개인키인 것을 특징으로 하는 eUICC
내 프로파일 백업 방법.

[청구항 5]

제1항에 있어서,
상기 eUICC 내 프로파일은,
통신 서비스 및 부가 서비스 중 하나 이상과 관련된 데이터 및

애플리케이션 중 하나 이상을 포함하는 것을 특징으로 하는 eUICC 내 프로파일 백업 방법.

[청구항 6]

제5항에 있어서,

상기 eUICC 내 프로파일은,

상기 통신 서비스와 관련하여, 폰북(Phonebook) 정보 및 개통된 사업자 프로파일 중 하나 이상을 포함하는 것을 특징으로 하는 eUICC 내 프로파일 백업 방법.

[청구항 7]

제5항에 있어서,

상기 eUICC 내 프로파일은,

상기 부가 서비스와 관련하여, 발급이 완료된 상태의 데이터 및 애플리케이션 중 하나 이상을 포함하는 것을 특징으로 하는 eUICC 내 프로파일 백업 방법.

[청구항 8]

제1항에 있어서,

상기 암호화하는 단계 이전에,

상기 백업 장치가 백업 명령을 전송하거나, 상기 eUICC 또는 상기 eUICC를 내장한 기기가 백업 명령을 전송함으로써, 상기 eUICC 내 프로파일 백업 프로세스를 트리거하는 단계를 더 포함하는 eUICC 내 프로파일 백업 방법.

[청구항 9]

제8항에 있어서,

상기 트리거하는 단계에서, 상기 백업 장치는,

상기 eUICC 내 프로파일의 백업이 필요한 경우 외부 개체와 백업 명령 암호화 요청 응답 절차를 통해 암호화된 상기 백업 명령을 생성하고, 상기 암호화된 상기 백업 명령을 상기 eUICC 또는 상기 eUICC를 내장한 기기로 전송하는 것을 특징으로 하는 eUICC 내 프로파일 백업 방법.

[청구항 10]

제8항에 있어서,

상기 트리거하는 단계에서,

상기 eUICC 또는 상기 eUICC를 내장한 상기 기기는,

상기 eUICC 내 프로파일의 백업이 필요한 경우, 상기 백업 명령을 상기 백업 장치로 전송하고, 상기 백업 장치로부터 백업 승인 명령을 수신하는 것을 특징으로 하는 eUICC 내 프로파일 백업 방법.

[청구항 11]

내부 프로파일 백업을 위한 내장 UICC(eUICC: embedded Universal Integrated Circuit Card)로서,

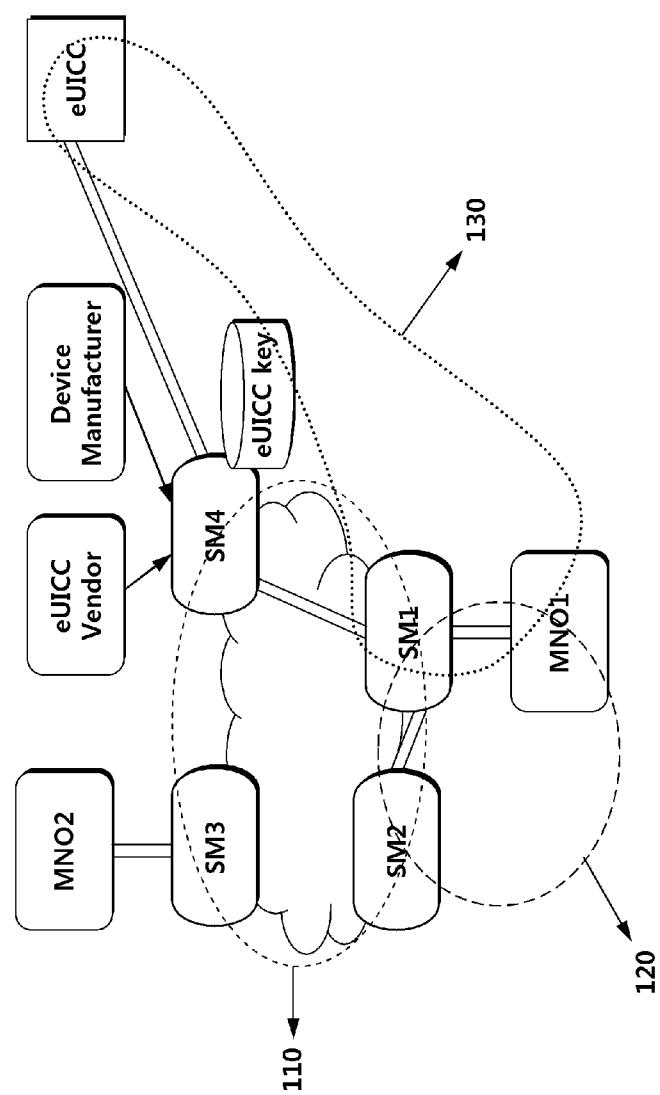
외부 개체와의 연동을 통해 관리되는 상기 eUICC 내 프로파일을 암호화하는 암호화 모듈; 및

상기 암호화 모듈에 의해 상기 암호화된 프로파일을 백업 장치에 백업시키기 위한 백업 프로파일로서 전송하는 통신 모듈을

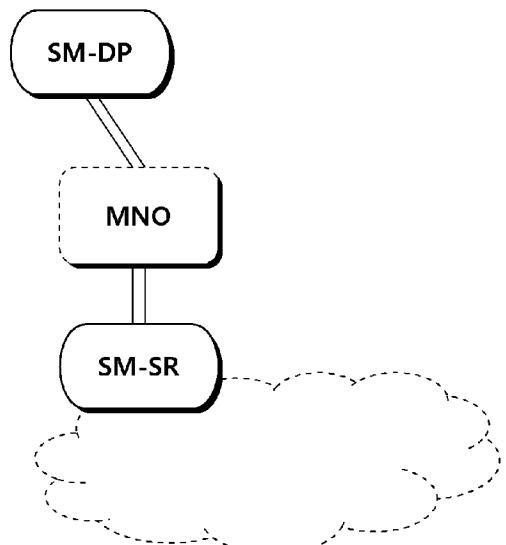
- 포함하는 eUICC.
- [청구항 12] 제11항에 있어서,
상기 암호화 모듈은,
상기 eUICC 내 프로파일을 이중으로 암호화하는 것을 특징으로 하는 eUICC.
- [청구항 13] 제11항에 있어서,
상기 eUICC 내 프로파일의 백업이 필요한 경우, 백업 명령을 상기 백업 장치로 전송하고 백업 승인 명령을 상기 백업 장치로부터 수신하는 백업 트리거 모듈을 더 포함하되,
상기 암호화 모듈은, 상기 백업 승인 명령의 수신에 따라 상기 eUICC 내 프로파일을 암호화하는 것을 특징으로 하는 eUICC.
- [청구항 14] 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 백업을 위한 외부 장치로서,
상기 외부 장치가 관리하는 상기 eUICC 내 프로파일이 암호화된 백업 프로파일을 수신하는 수신 모듈;
상기 암호화된 백업 프로파일을 복호화하는 복호화 모듈; 및
상기 복호화된 백업 프로파일을 상기 백업 장치로 전송하는 전송 모듈을 포함하는 외부 장치.
- [청구항 15] 제14항에 있어서,
상기 복호화 모듈은,
상기 eUICC에서 이중으로 암호화된 백업 프로파일을 1차 복호화 키로 1차 복호화하는 것을 특징으로 하는 외부 장치.
- [청구항 16] 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 백업을 위한 백업 장치로서,
외부 개체와의 연동을 통해 관리되는 상기 eUICC 내 프로파일이 암호화된 백업 프로파일을 상기 외부 개체로부터 수신하는 수신 모듈;
상기 암호화된 백업 프로파일을 복호화하는 복호화 모듈; 및
상기 복호화된 백업 프로파일을 백업하는 백업 모듈을 포함하는 백업 장치.
- [청구항 17] 제16항에 있어서,
상기 백업 장치가 상기 eUICC 내 프로파일 백업 프로세스를 트리거 하기 위한 백업 명령을 상기 eUICC 또는 상기 eUICC를 내장한 기기로 전송하는 백업 트리거 모듈을 더 포함하는 백업 장치.
- [청구항 18] 제16항에 있어서,
상기 eUICC 또는 상기 eUICC를 내장한 기기가 상기 eUICC 내 프로파일 백업 프로세스를 트리거 하기 위해 전송한 백업 명령을

수신하여 백업 승인 명령을 상기 eUICC 또는 상기 eUICC를
내장한 기기로 전송하는 백업 트리거 지원 모듈을 더 포함하는
백업 장치.

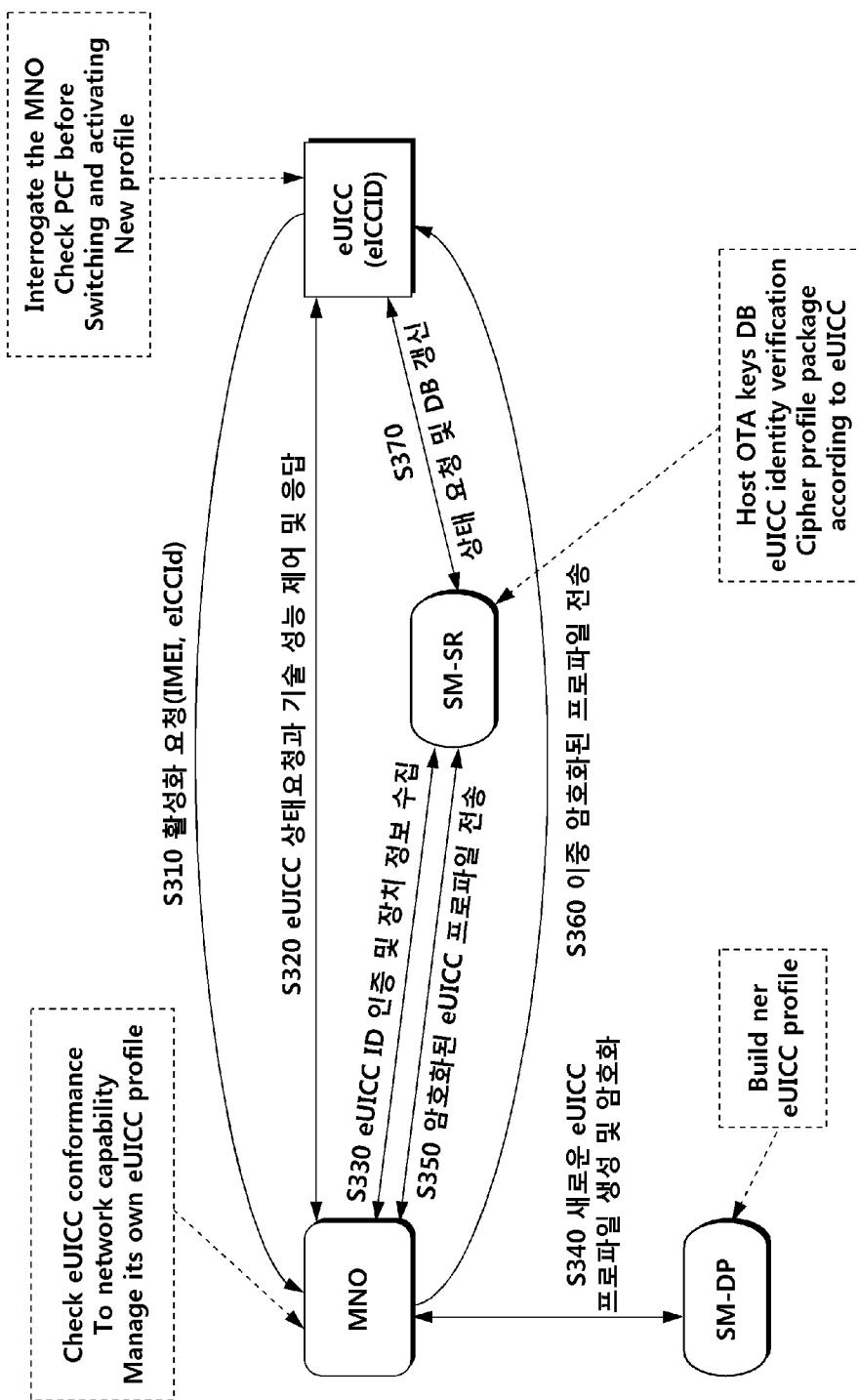
[Fig. 1]



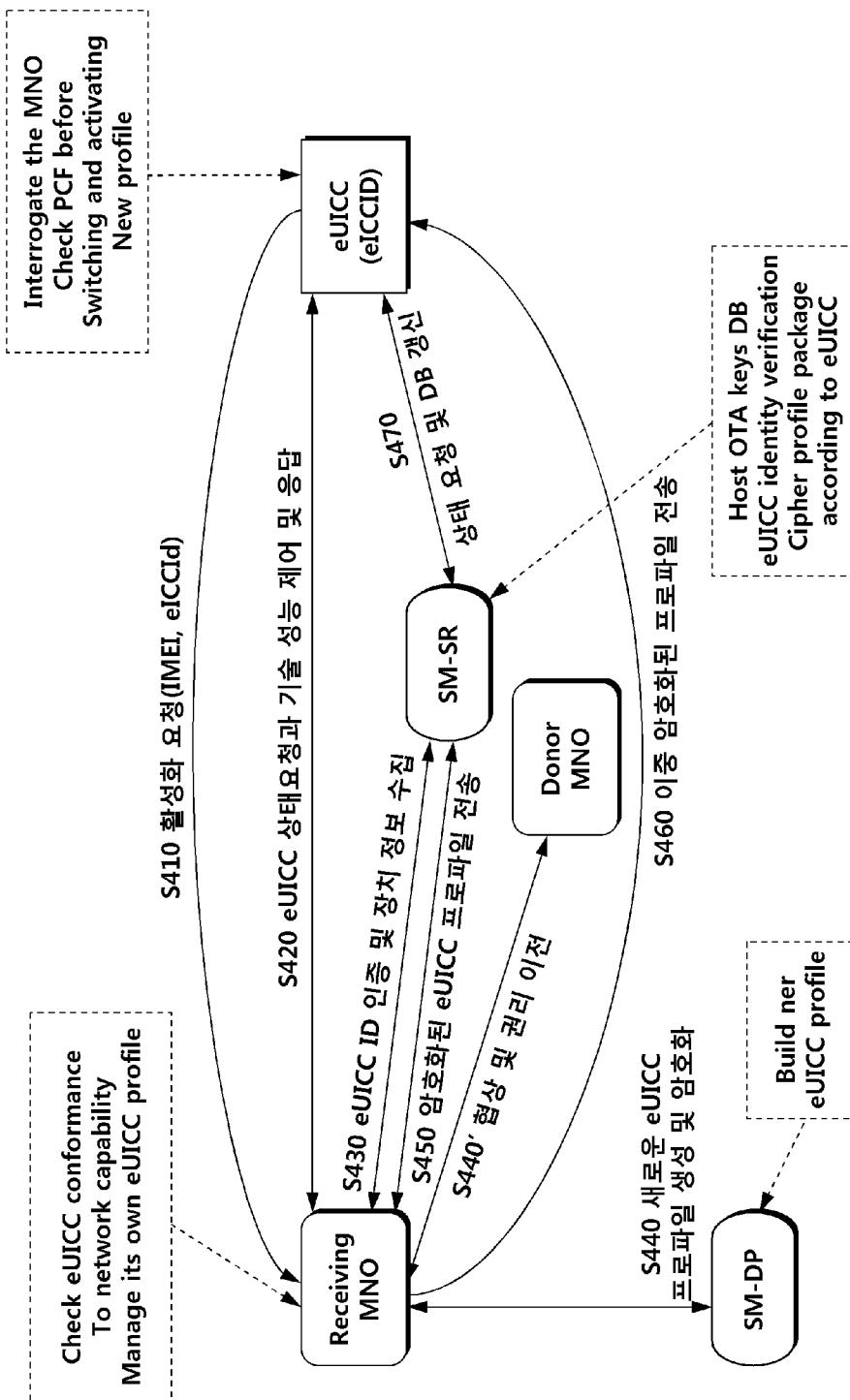
[Fig. 2]



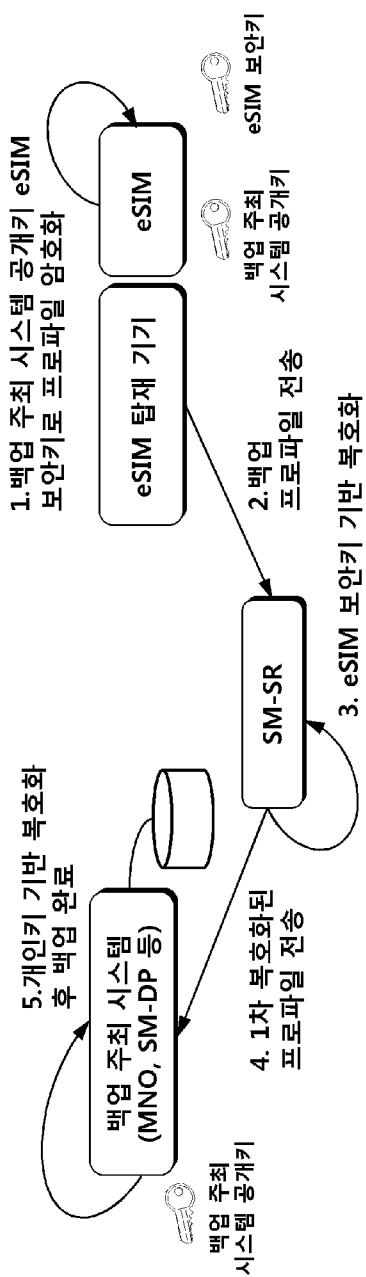
[Fig. 3]



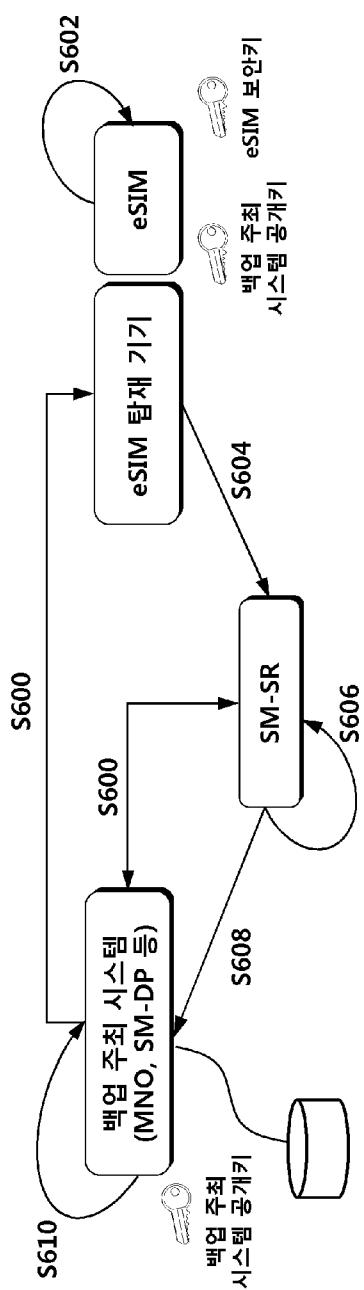
[Fig. 4]



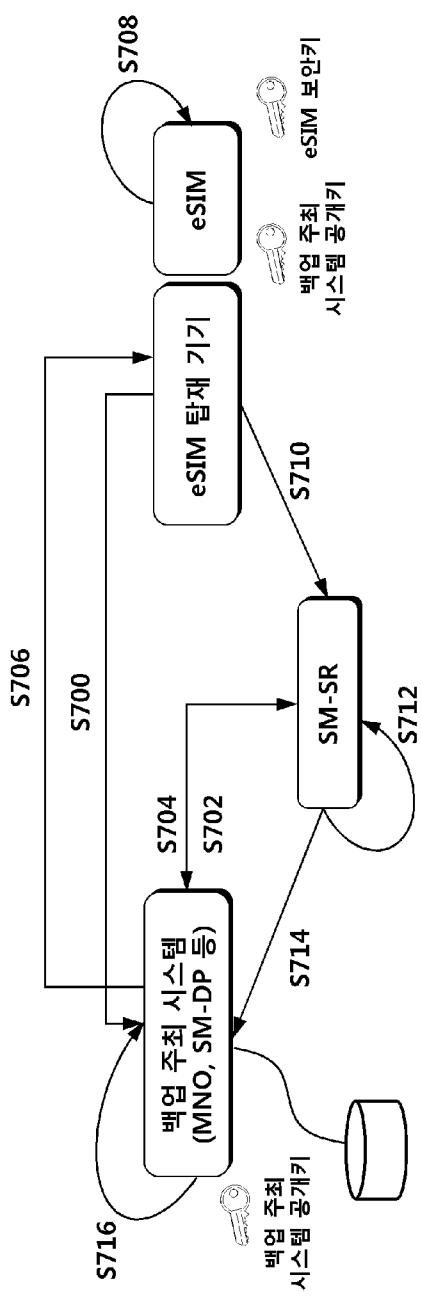
[Fig. 5]



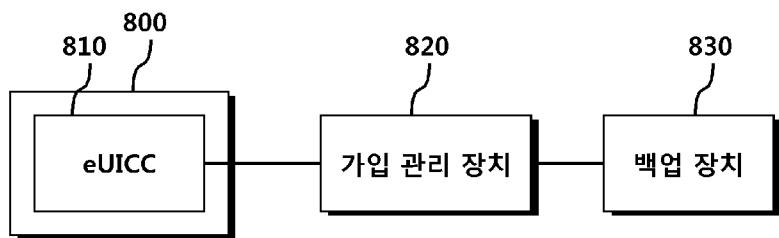
[Fig. 6]



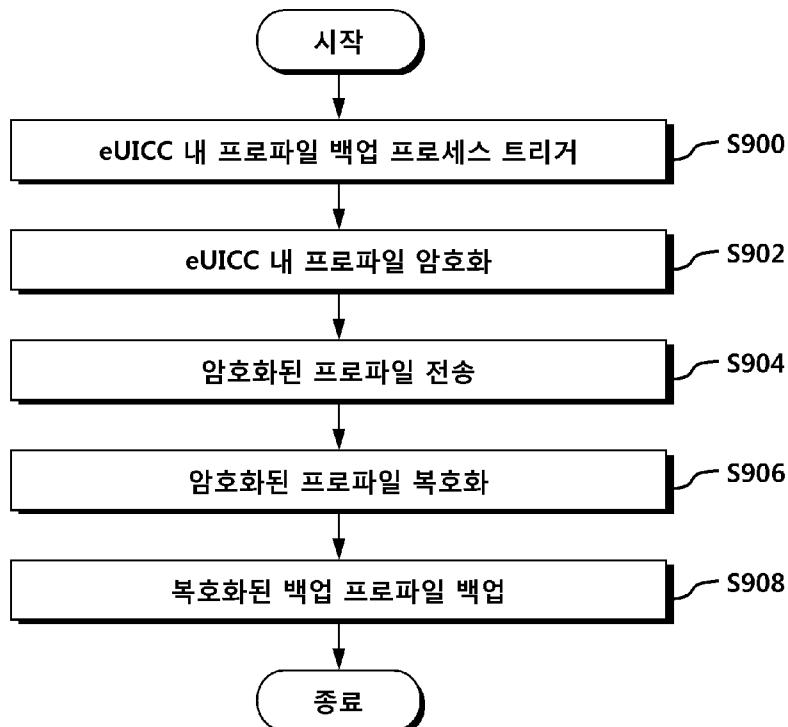
[Fig. 7]



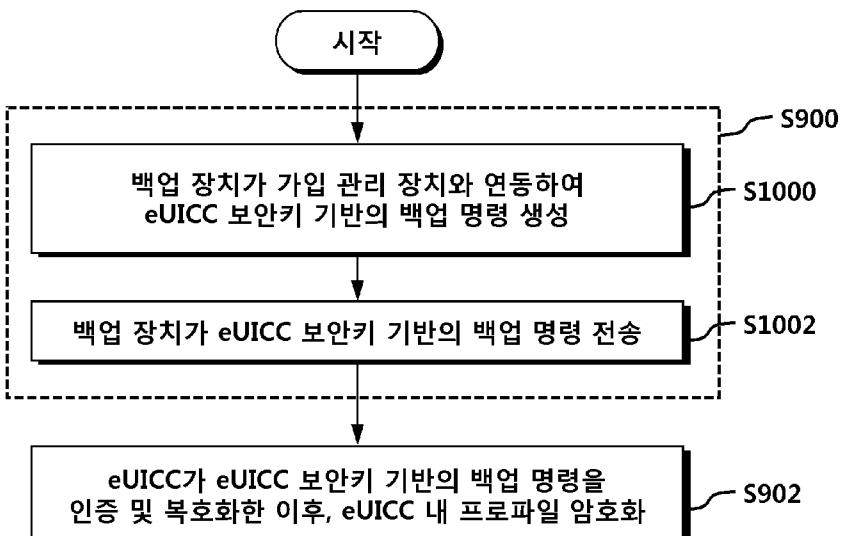
[Fig. 8]



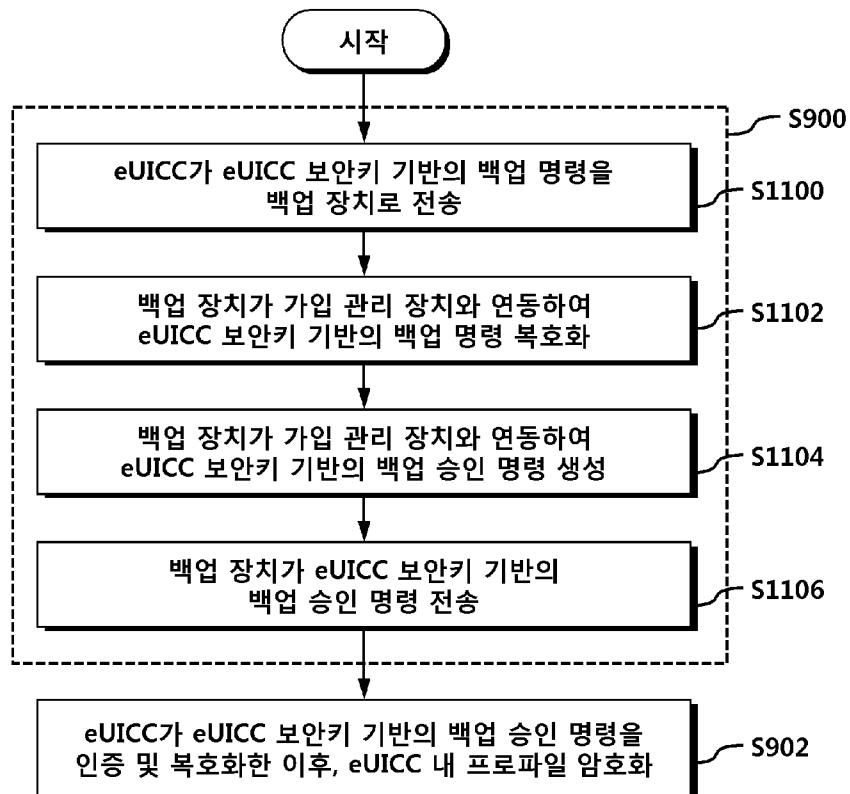
[Fig. 9]



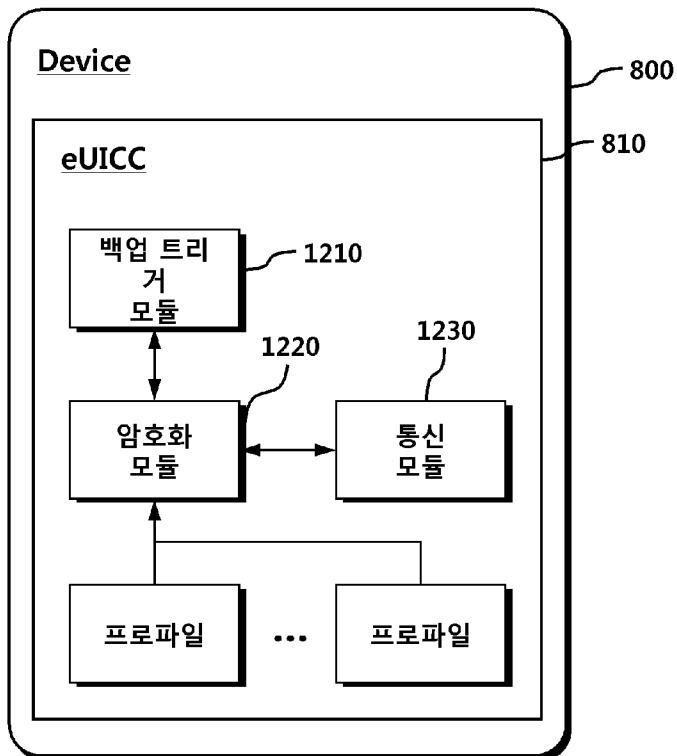
[Fig. 10]



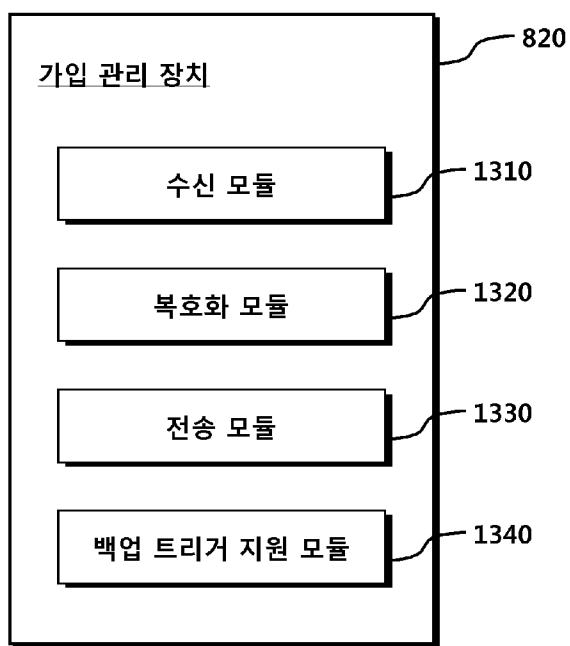
[Fig. 11]



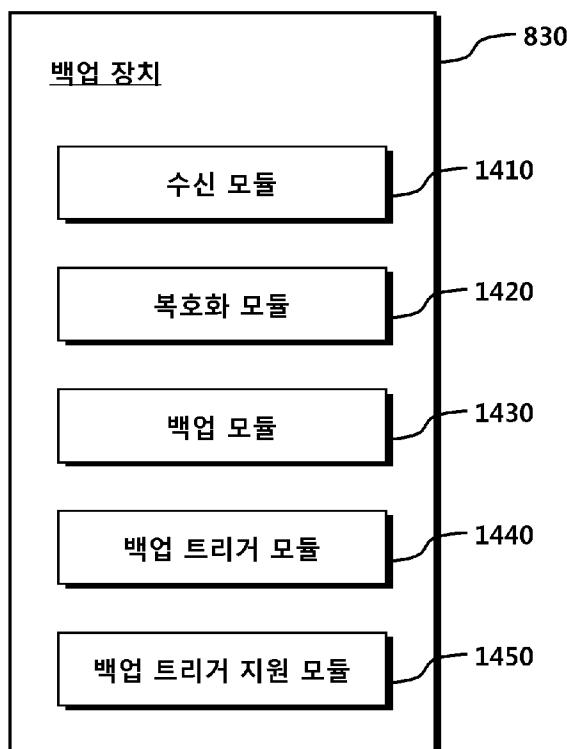
[Fig. 12]



[Fig. 13]



[Fig. 14]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2012/009201**A. CLASSIFICATION OF SUBJECT MATTER****H04W 8/30(2009.01)i, H04W 8/18(2009.01)i, H04W 12/08(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 8/30; H04W 8/18; H04W 92/08; H04W 88/02; G06F 15/16; H04W 12/06; H04W 12/08; H04B 1/38; H04W 8/24; G06F 11/00

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: UICC, backup, encoding, decoding, profile

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2009-0046607 A (SAMSUNG ELECTRONICS CO., LTD.) 11 May 2009	1,5-11,13,14,16-18
Y	See paragraphs [2],[3],[28]-[48] and figures 1-3.	2-4,12,15
Y	KR 10-0764658 B1 (SAMSUNG ELECTRONICS CO., LTD.) 08 October 2007 See paragraphs [24],[25].	2-4,12,15
A	US 2010-0311468 A1 (GUANGMING SHI et al.) 09 December 2010 See paragraphs [81]-[90] and figure 11.	1-18
A	KR 10-0898055 B1 (SMARTCARD LABORATORY) 19 May 2009 See abstract, paragraphs [45]-[55] and figure 5.	1-18
A	KR 10-2007-0097026 A (VERISIGN, INC.) 02 October 2007 See paragraphs [17]-[28].	1-18



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

27 FEBRUARY 2013 (27.02.2013)

Date of mailing of the international search report

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 SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2012/009201

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0046607 A	11.05.2009	NONE	
KR 10-0764658 B1	08.10.2007	CN 101075871 A EP 1858280 A1 US 2008-0020798 A1 US 8036705 B2	21.11.2007 21.11.2007 24.01.2008 11.10.2011
US 2010-0311468 A1	09.12.2010	CN 102461228 A EP 2441286 A2 KR 10-2012-0028368 A WO 2010-144479 A2 WO 2010-144479 A3	16.05.2012 18.04.2012 22.03.2012 16.12.2010 03.02.2011
KR 10-0898055 B1	19.05.2009	US 2010-0159878 A1	24.06.2010
KR 10-2007-0097026 A	02.10.2007	AU 2005-299577 A1 CA 2583758 A1 CN 101129057 A0 EP 1805977 A2 JP 2008-518364 A US 2006-0156052 A1 WO 2006-047764 A2 WO 2006-047764 A3	04.05.2006 04.05.2006 20.02.2008 11.07.2007 29.05.2008 13.07.2006 04.05.2006 18.05.2007

A. 발명이 속하는 기술분류(국제특허분류(IPC))**H04W 8/30(2009.01)i, H04W 8/18(2009.01)i, H04W 12/08(2009.01)i****B. 조사된 분야**

조사된 최소문현(국제특허분류를 기재)

H04W 8/30; H04W 8/18; H04W 92/08; H04W 88/02; G06F 15/16; H04W 12/06; H04W 12/08; H04B 1/38; H04W 8/24; G06F 11/00

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: UICC, 백업, 암호화, 복호화, 프로파일**C. 관련 문현**

카테고리*	인용문현명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X Y	KR 10-2009-0046607 A (삼성전자주식회사) 2009.05.11 단락 [2],[3],[28]-[48] 및 도면 1-3 참조.	1,5-11,13,14,16-18 2-4,12,15
Y	KR 10-0764658 B1 (삼성전자주식회사) 2007.10.08 단락 [24],[25] 참조.	2-4,12,15
A	US 2010-0311468 A1 (GUANGMING SHI 외 4명) 2010.12.09 단락 [81]-[90] 및 도면 11 참조.	1-18
A	KR 10-0898055 B1 (주식회사 스마트카드연구소) 2009.05.19 요약, 단락 [45]-[55] 및 도면 5 참조.	1-18
A	KR 10-2007-0097026 A (베리사인 인코포레이티드) 2007.10.02 단락 [17]-[28] 참조.	1-18

 추가 문현이 C(계속)에 기재되어 있습니다. 대응특허에 관한 별지를 참조하십시오.

* 인용된 문현의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문현

“T” 국제출원일 또는 우선일 후에 공개된 문현으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문현

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문현

“X” 특별한 관련이 있는 문현. 해당 문현 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문현 또는 다른 인용문현의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문현

“Y” 특별한 관련이 있는 문현. 해당 문현이 하나 이상의 다른 문현과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

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

“&” 동일한 대응특허문현에 속하는 문현

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문현

국제조사의 실제 완료일

국제조사보고서 발송일

2013년 02월 27일 (27.02.2013)

2013년 02월 28일 (28.02.2013)

ISA/KR의 명칭 및 우편주소

심사관



팩스 번호 82-42-472-7140

김병성



전화번호 82-42-481-8403

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2012/009201

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0046607 A	2009. 05. 11	없음	
KR 10-0764658 B1	2007. 10. 08	CN 101075871 A EP 1858280 A1 US 2008-0020798 A1 US 8036705 B2	2007. 11. 21 2007. 11. 21 2008. 01. 24 2011. 10. 11
US 2010-0311468 A1	2010. 12. 09	CN 102461228 A EP 2441286 A2 KR 10-2012-0028368 A WO 2010-144479 A2 WO 2010-144479 A3	2012. 05. 16 2012. 04. 18 2012. 03. 22 2010. 12. 16 2011. 02. 03
KR 10-0898055 B1	2009. 05. 19	US 2010-0159878 A1	2010. 06. 24
KR 10-2007-0097026 A	2007. 10. 02	AU 2005-299577 A1 CA 2583758 A1 CN 101129057 A0 EP 1805977 A2 JP 2008-518364 A US 2006-0156052 A1 WO 2006-047764 A2 WO 2006-047764 A3	2006. 05. 04 2006. 05. 04 2008. 02. 20 2007. 07. 11 2008. 05. 29 2006. 07. 13 2006. 05. 04 2007. 05. 18