



- (51) 국제특허분류:
H04W 12/08 (2009.01) H04W 8/18 (2009.01)
H04W 12/06 (2009.01)
- (21) 국제출원번호: PCT/KR2013/004536
- (22) 국제출원일: 2013년 5월 23일 (23.05.2013)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2012-0055412 2012년 5월 24일 (24.05.2012) KR
10-2013-0057509 2013년 5월 22일 (22.05.2013) KR
- (71) 출원인: 주식회사 케이티 (KT CORPORATION)
[KR/KR]; 463-711 경기도 성남시 분당구 불정로 90,
Gyeonggi-do (KR).
- (72) 발명자: 이형진 (LEE, Hyung Jin); 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR). 김관래 (KIM, Kwan Lae); 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR). 김주영 (KIM, Joo Young); 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR). 박철현 (PARK, Chul Hyun); 137-

140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR). 이진형 (LEE, Jin Hyoung); 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR). 정윤필 (JEUNG, Youn Pil); 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR).

(74) 대리인: 특허법인 이상 (E-SANG PATENT&TRADE-MARK LAW FIRM); 137-890 서울시 서초구 양재동 82-2 우도빌딩 3층, Seoul (KR).

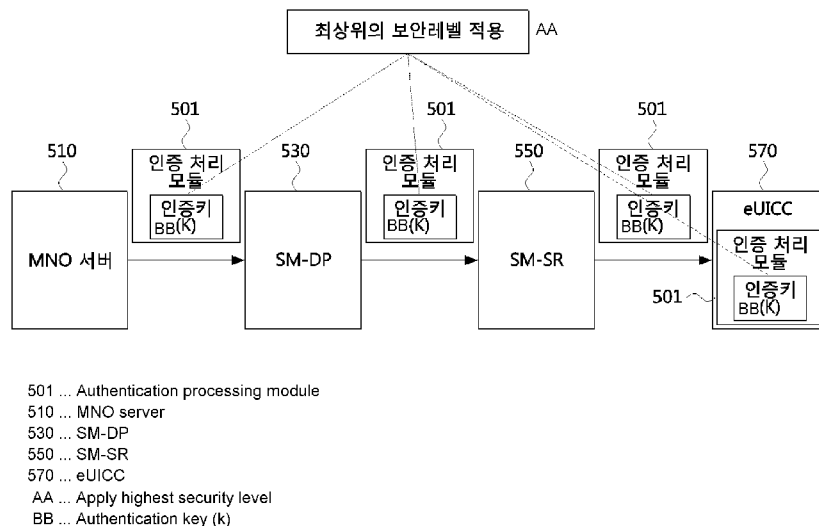
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, 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,

[다음 쪽 계속]

(54) Title: METHOD FOR PROVIDING MOBILE COMMUNICATION PROVIDER INFORMATION AND DEVICE FOR PERFORMING SAME

(54) 발명의 명칭: 이동통신사업자 정보 제공 방법 및 이를 수행하는 장치



(57) Abstract: A method for providing mobile communication provider information and a device for performing the same are disclosed. A terminal having an eUICC receives data, in which mobile communication provider information is capsulized and included, and stores the received data in the eUICC. Therefore, the mobile communication provider information can be transferred by applying the highest security scheme, and duplication of the eUICC due to the exposure of an authentication key by external hacking attacks can be prevented.

(57) 요약서: 이동통신사업자 정보 제공 방법 및 이를 수행하는 장치가 개시된다. eUICC를 구비한 단말은 이동통신사업자 정보가 캡슐화되어 포함된 데이터를 수신하고, 수신한 데이터를 eUICC에 저장한다. 따라서, 이동통신사업자 정보를 최상위 보안 기법을 적용하여 전달할 수 있고, 외부 해킹 공격에 의해 인증키가 노출되어 eUICC가 복제되는 것을 방지할 수 있다.





ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, **공개:**

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).

— 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

발명의 명칭: 이동통신사업자 정보 제공 방법 및 이를 수행하는 장치

기술분야

- [1] 본 발명은 내장 UICC를 구비한 단말에 이동통신사업자 정보를 제공하는 방법 및 이를 수행하는 장치에 관한 것이다.

배경기술

- [2] UICC(Universal Integrated Circuit Card)는 단말 내에 삽입되어 사용자가 가입한 이동 통신 네트워크와 사용자 인증을 위한 모듈로 사용될 수 있는 스마트 카드이다. UICC는 SMS(Short Message Service), 폰 북(phone book) 등과 같은 사용자의 개인 정보와, IMSI(International Mobile Subscriber Identity), HPLMN(Home Public Land Mobile Network) 등의 사용자가 가입한 이동 통신 사업자에 대한 사업자 정보를 저장할 수 있다.
- [3] UICC는 GSM(Global System for Mobile communications) 방식의 경우에는 SIM(Subscriber Identity Module) 카드로 불릴 수 있고, WCDMA(Wideband Code Division Multiple Access) 방식의 경우에는 USIM(Universal Subscriber Identity Module) 카드로 불릴 수 있다.
- [4] 사용자가 UICC를 단말에 장착하면, 단말은 UICC에 저장된 정보들을 이용하여 사용자 인증을 자동으로 수행함으로써 사용자가 편리하게 단말을 사용할 수 있도록 한다. 또한, 사용자가 단말을 교체하는 경우, 사용자는 기존의 단말에서 탈거한 UICC를 새로운 단말에 장착하는 것만으로 사용자가 가입한 이동통신 서비스 및 사용자 정보를 그대로 유지한 상태에서 단말을 용이하게 교체할 수 있다. 또는, 사용자는 현재 사용중인 단말에 삽입된 UICC를 다른 이동통신사업자의 UICC로 교체함으로써 간편하게 이동 통신 사업자를 변경할 수도 있다.
- [5] 그러나 단말에서 UICC를 착탈하기 어려운 경우, 예를 들면 기계 대 기계(Machine to Machine, M2M) 통신용 단말의 내부에 UICC가 실장되어 외부에서 교체하기 어려운 구조로 제조된 경우나, 기존 착탈식 플라스틱 구조의 UICC 보다 충격 및 열에 대한 내구성이 요구되는 경우를 위해 착탈식 구조가 아닌 칩 형태의 단말 일체형 구조로 제공되는 경우에도 착탈식 UICC와 동일한 서비스 제공이 가능하도록 내장 UICC(Embedded UICC, 이하 'eUICC'라 약칭함) 구조가 제안되었다.
- [6] eUICC는 기존 착탈식 형태의 UICC와 달리 eUICC가 단말의 제조 단계에서 단말에 실장되어 출시되어, 단말에 착탈될 수 없는 물리적 구조의 특성으로 인하여, eUICC 착탈을 통해 이동통신사업자를 변경할 수 없다.
- [7] 따라서, eUICC가 실장된 단말의 이동 통신 사업자를 변경하기 위해서는,

변경할 이동통신사업자의 정보를 원격에서 eUICC에 제공하기 위한 방법이 요구된다.

- [8] 그러나, 현재까지는 eUICC에 이동통신사업자의 정보를 제공하는 기능이나 이를 위한 인터페이스 등이 구체적으로 정의되지 않았고, 이에 따라 기존의 UICC를 구비한 단말에 이동통신사업자 정보를 제공하는 방법을 eUICC를 구비한 단말에 그대로 적용하는 경우에는 보안에 취약해지는 단점이 있다.

발명의 상세한 설명

기술적 과제

- [9] 상술한 문제점을 해결하기 위한 본 발명의 목적은 높은 보안을 유지하면서 eUICC에 이동통신사업자의 정보를 제공할 수 있고, 이동통신사업자 정보가 eUICC에 저장된 이후에도 높은 보안을 유지할 수 있는 이동통신사업자 정보 제공 방법을 제공하는 것이다.
- [10] 또한, 본 발명의 다른 목적은 높은 보안을 유지하면서 eUICC에 이동통신사업자 정보를 제공할 수 있고, 이동통신사업자 정보가 eUICC에 저장된 이후에도 높은 보안을 유지할 수 있는 이동통신사업자 정보를 제공 장치를 제공하는 것이다.
- [11]
- [12] 본 발명의 목적들은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 이해될 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

과제 해결 수단

- [13] 상술한 본 발명의 목적을 달성하기 위한 본 발명의 일 측면에 따른 이동통신사업자 정보 제공 방법에 따르면, eUICC를 구비한 단말에서 수행되는 이동통신사업자 정보 제공 방법으로, 이동통신사업자 정보가 캡슐화되어 포함된 데이터를 수신하는 단계 및 상기 수신한 데이터를 상기 eUICC에 저장하는 단계를 포함한다.
- [14] 여기서, 상기 이동통신사업자 정보가 캡슐화되어 포함된 데이터를 수신하는 단계는, 상기 단말의 인증을 위한 인증키 정보가 캡슐화되어 포함된 데이터를 수신할 수 있다. 또한, 상기 인증키 정보가 캡슐화되어 포함된 데이터는 상기 단말의 인증을 처리하는 인증 처리 모듈의 데이터로 구성될 수 있다.
- [15] 여기서, 상기 이동통신사업자 정보가 캡슐화되어 포함된 데이터를 수신하는 단계는, 상기 단말의 인증을 위한 인증키 정보의 형식을 이전과 다른 형식으로 생성하는 암호화 모듈 데이터를 수신할 수 있다.
- [16] 여기서, 상기 수신한 데이터를 상기 eUICC에 저장하는 단계는, 상기 단말의 인증을 처리하는 인증 처리 모듈을 상기 eUICC에 저장하고, 상기

이동통신사업자 정보는 인증키를 포함하되, 상기 인증키는 상기 인증 처리 모듈에 캡슐화된 상태로 상기 eUICC에 저장될 수 있다.

- [17] 여기서, 상기 인증 처리 모듈은 상기 eUICC에 저장된 후, 상기 단말로부터 제공된 인증 요청에 상응하여 인증 처리를 수행한 후, 인증 처리 결과에 대한 응답으로 인증 성공 응답, 인증 실패 응답 및 동기화 실패 응답 중 어느 하나의 응답을 상기 단말에 제공할 수 있다.
- [18] 여기서, 상기 이동통신사업자 정보 제공 방법은, 상기 인증 처리 모듈이 상기 eUICC에 저장된 후, 상기 인증키가 사용되는 경우 상기 인증키의 노출을 방지하기 위한 처리를 수행하는 단계를 더 포함할 수 있다.
- [19] 또한, 본 발명의 목적을 달성하기 위한 본 발명의 다른 측면에 따른 이동통신사업자 정보 제공 방법에 따르면, 이동통신사업자 서버에서 수행되는 이동통신사업자 정보 제공 방법으로, 이동통신사업자 정보를 캡슐화한 모듈을 생성하는 단계 및 상기 캡슐화한 모듈을 특정 단말로 전송하는 단계를 포함한다.
- [20] 여기서, 상기 이동통신사업자 정보를 캡슐화한 모듈을 생성하는 단계는, 인증 처리를 수행하는 인증 처리 모듈에 상기 이동통신사업자 정보로 인증키를 캡슐화하여 포함시켜 상기 캡슐화한 모듈을 생성할 수 있다.
- [21] 여기서, 상기 이동통신사업자 정보를 캡슐화한 모듈을 생성하는 단계는, 상기 캡슐화한 모듈을 애플릿 파일과 동일한 형태의 파일로 생성할 수 있다.
- [22] 여기서, 상기 캡슐화한 모듈을 특정 단말로 전송하는 단계는, 상기 캡슐화한 모듈을 SM-DP(Subscription Manager - Data Preparation)에 전송하는 단계와, 상기 SM-DP가 상기 캡슐화한 모듈을 SM-SR(Subscription Manager Secure Routing)에 전송하는 단계 및 상기 SM-SR이 상기 캡슐화한 모듈을 OTA(Over The Air) 통신 방식을 통해 상기 특정 단말로 전송하는 단계를 포함할 수 있다.
- [23] 또한, 본 발명의 다른 목적을 달성하기 위한 본 발명의 일 측면에 따른 이동통신사업자 정보 제공 장치는, 이동통신사업자 정보가 캡슐화된 모듈 및 상기 이동통신사업자 정보가 캡슐화된 모듈을 다운로드 하기 위한 처리를 수행하는 처리부를 구비하는 eUICC를 포함한다.
- [24] 여기서, 상기 이동통신사업자 정보가 캡슐화된 모듈은 상기 장치의 인증을 위한 인증키가 캡슐화되어 포함되고, 인증을 위한 처리를 수행하는 인증 처리 모듈로 구성될 수 있다.
- [25] 여기서, 상기 처리부는 상기 장치로부터 인증 요청 메시지를 수신하여 상기 인증 처리 모듈에 제공하고, 상기 인증 처리 모듈로부터 인증 결과로 제공된 응답을 수신하여 상기 장치에 제공할 수 있다.
- [26] 여기서, 상기 인증 처리 모듈은 상기 처리부로부터 제공된 인증 요청에 상응하여 인증 처리를 수행한 후, 인증 성공을 지시하는 인증 성공 응답, 인증 실패를 지시하는 인증 실패 응답 및 동기화 실패를 지시하는 동기화 실패 응답 중 어느 하나의 응답을 상기 처리부를 통해 상기 장치에 제공할 수 있다.

발명의 효과

- [27] 상술한 바와 같은 상술한 바와 같은 본 발명의 실시예에 따른 이동통신사업자의 정보 제공 방법 및 장치에 따르면, eUICC에 제공하기 위해 전달하는 이동통신사업자의 정보를 인증 처리 모듈과 같은 임의의 데이터에 캡슐화하여 전달함으로써 인증키를 최상위 보안 기법을 적용하여 전달할 수 있다.
- [28] 따라서, 보안이 이루어지지 않은 공개된 무선 네트워크를 통해 이동통신사업자의 정보를 전달하는 경우에도 최상위 레벨의 보안을 적용하여 이동통신사업자의 정보를 eUICC에 전달할 수 있다.
- [29] 또한, 본 발명에서는 eUICC 내부에 인증키를 캡슐화하여 저장하여 인증키에 접근할 수 인터페이스가 존재하지 않도록 구성함으로써 인터페이스를 이용한 외부 해킹 공격에 의해 인증키가 노출되지 않게 되고, 이에 따라 eUICC의 복제를 방지할 수 있다.

도면의 간단한 설명

- [30] 도 1은 본 발명의 일 실시예에 따른 이동통신사업자 정보 제공 방법이 실행되는 환경을 나타내는 개념도이다.
- [31] 도 2는 본 발명의 일 실시예에 따른 이동통신사업자 정보 제공 방법을 설명하기 위한 개념도이다.
- [32] 도 3은 단말과 이동통신사업자 네트워크 사이의 인증 과정을 나타내는 순서도이다.
- [33] 도 4는 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법 이 적용되는 eUICC의 구성을 나타내는 블록도이다.
- [34] 도 5는 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법을 나타내는 개념도이다.
- [35] 도 6은 본 발명의 다른 실시예에 따라 eUICC에 인증키가 저장된 이후의 인증 처리의 수행 과정을 설명하기 위한 개념도이다.
- [36] 도 7은 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법에서 사용되는 인증 인터페이스의 일 예를 나타낸 것이다.
- [37] 도 8은 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법에서 사용되는 인증 성공 응답 인터페이스의 일 예를 나타내는 것이다.
- [38] 도 9는 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법에서 사용되는 동기화 실패 응답 인터페이스의 일 예를 나타내는 것이다.
- [39] 도 10은 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법을 나타내는 흐름도이다.

발명의 실시를 위한 형태

- [40] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다.

- [41] 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.
- [42] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [43] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [44] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.
- [45]
- [46] 도 1은 본 발명의 일 실시예에 따른 이동통신사업자 정보 제공 방법이 실행되는 환경을 나타내는 개념도이다.
- [47] 도 1을 참조하면, 본 발명의 일 실시예에 따른 이동통신사업자 정보 제공 방법은 이동통신사업자(MNO: Mobile Network Operator) 서버(이하, 'MNO 서버'라 지칭함)(110), 가입자정보관리 서버(130) 및 eUICC(150)가 네트워크를 통해 서로 연결된 환경에서 수행될 수 있다.
- [48] MNO 서버(110)는 WCDMA(Wideband Code Division Multiple Access), LTE(Long Term Evolution) 등과 같은 이동 통신 시스템에서 제공하는 이동 통신 서비스에 가입한 가입자에게 이동 통신 서비스를 제공하기 위해 eUICC(150)가 구비해야 하는 이동통신사업자 정보를 생성한다. 여기서, 이동통신사업자 정보는 오퍼레이터 크레덴셜(Operator Credential), MNO 크레덴셜, 프로파일(Profile), eUICC 프로파일 또는 프로파일 패키지(Profile Package) 등의 다른 용어로 지칭될 수 있다.
- [49] 가입자정보관리 서버(130)는 eUICC(150)에 대한 정보 관리, 여러 이동통신 사업자에 대한 정보 관리, 가입자의 이동통신 사업자 변경에 따른 인증 및 원격 정보 변경 등의 기능을 처리한다.
- [50] 즉, 가입자정보관리 서버(130)는 이동통신사업자 정보를 eUICC(150)에

발급하고 가입(Subscription) 변경이나 이동통신사업자 변경에 대한 절차를 처리하는 등의 eUICC(150)에 대한 전반적인 관리를 수행한다.

[51] 가입자정보관리 서버(130)는 가입 관리자(SM: Subscription Manager, 이하 'SM'이라 약칭함) 또는 프로파일 관리자(PM: Profile Manager, 이하 'PM'이라 약칭함)를 포함할 수 있다.

[52] SM은 이동통신사업자 정보를 생성하는 역할을 수행하는 주체인 SM-DP(Subscription Manager - Data Preparation)와 eUICC(150)에 사업자 정보를 직접적으로 전달하는 주체인 SM-SR(Subscription Manager Secure Routing)을 포함할 수 있다.

[53] SM-DP는 이동통신 사업자(MNO)가 eUICC(150)에 제공할 데이터에 대해 암호화 등의 처리를 수행하여 보안이 적용된 패키지(Package)를 구성한 후, 이를 SM-SR에 전달한다. 여기서, 보안이 적용된 패키지는 MNO 서버(110)에서 생성한 이동통신사업자 정보로 구성될 수 있다.

[54] SM-SR은 SM-DP로부터 전달받은 보안이 적용된 패키지가 목적 eUICC(150)에 정상적으로 전달될 수 있도록 다른 SM-SR로 라우팅하거나 또는 해당 eUICC(150)로 전달하는 역할을 수행한다. 여기서, 보안이 적용된 패키지가 해당 eUICC(150)로 전달되는 과정에서는 보안이 적용된 OTA(Over The Air) 통신 방식이 사용될 수 있다.

[55] eUICC(150)는 SM-SR로부터 OTA 통신 방식을 통해 전달받은 OTA 패키지를 복호화하여 SM-DP가 암호화한 패키지를 추출한 후, 추출된 패키지를 복호화하여 실제 이동통신사업자 정보를 획득한 후, 획득한 이동통신사업자 정보를 eUICC(150) 내에 저장한다.

[56]

[57] 도 2는 본 발명의 일 실시예에 따른 이동통신사업자 정보 제공 방법을 설명하기 위한 개념도이다. 이하에서는 eUICC에 제공되는 이동통신사업자 정보의 예로 인증키 K를 예를 들어 설명한다.

[58] 도 2를 참조하면, 먼저 MNO 서버(210)는 가입자의 인증키(K), UICC 데이터 파일(예를 들면, IMSI, HPLMN 등의 네트워크 접속 파일), 사용자 정보 파일(예를 들면, SMS 파일, 폰북 등) 및 애플릿 등과 관련된 파일을 생성하고, 생성한 파일을 SM-DP(230)에 전달한다.

[59] SM-DP(230)는 MNO 서버(210)로부터 제공받은 파일을 암호화한 후, 암호화된 파일을 SM-SR(250)에 전달한다. 여기서, SM-DP(230)는 SM-SR(250)을 통해 eUICC(270)에 전달될 파일을 포함하는 OTA 패키지를 생성하고, OTA 패키지에는 가입자의 인증키(K), UICC 데이터 파일(예를 들면, IMSI, HPLMN) 등과 같은 이동통신 사업자(MNO)의 크레덴셜(credential)이 포함될 수 있다.

[60] SM-SR(250)은 SM-DP(230)로부터 제공된 암호화된 OTA 패키지를 해당 목적 eUICC(270)에 전달한다. 여기서, SM-SR(250)은 암호화된 OTA 통신 방식을 이용하여 eUICC(270)에 OTA 패키지를 전달할 수 있다.

- [61] eUICC(270)는 SM-SR(250)로부터 전달받은 암호화된 OTA 패키지를 복호화하여 인증키(K), UICC 데이터 파일 등을 획득한 후, 이를 저장한다.
- [62] SM-DP(230)에서 암호화하여 eUICC(270)에 제공되는 인증키 K는 전술한 바와 같이 이동통신사업자 정보의 하나이다. 즉, 인증키 K는 eUICC(270)와 이동통신 사업자의 인증 센터(AuC: Authentication Center)간에 공유하는 가입자 키(subscriber key)로써 해당 이동통신 사업자의 네트워크와 가입자(또는 eUICC(270))간에 인증을 위해 사용된다.
- [63] 인증키는 이동통신 사업자 네트워크를 인증하기 위한 것으로 보안상 최상위 레벨의 중요도를 가진다. 만약, 인증키 K 값이 노출되는 경우 해당 eUICC(270)는 복제가 가능하게 되며, 복제를 통해 해당 가입자의 음성 통화, SMS/MMS(Multimedia message service), 데이터 서비스 등이 해킹당할 수 있다.
- [64] 도 2에 도시한 실시예에서는 보안상 최상위 레벨의 중요한 정보인 K를 다른 정보(예를 들면, IMSI, HPLMN, SMS, 폰북 등)와 동일한 레벨의 보안(예를 들면, 단순한 암호화 정도)을 적용하여 무선 네트워크를 통해 전달하는 것으로 예시하였다.
- [65] 인증키 K와 같은 가입자 인증키 정보는 단말의 개통 과정 중에 eUICC(270)에 제공되어 저장하게 되므로, eUICC(270)와 이동통신 사업자 네트워크와의 인증이 이루어지기 전에 eUICC(270)에 제공되고, 이와 같은 과정에서 보안이 이루어지지 않은 공개된 무선 네트워크를 사용하게 된다.
- [66] 따라서, 인증키 K와 같은 이동통신사업자 정보의 전달을 위해서는 더욱 더 높은 수준의 보안이 요구된다.
- [67] 한편, 원격지에서 인증키 K를 제공하기 위해서, eUICC(270)에 인증키 K의 제공을 위한 별도의 인터페이스를 이용할 수도 있다. 그러나, 보안상 최상위 레벨의 중요도를 가지는 인증키 K를 어떤 형식(암호화 또는 비암호화)으로든 그대로 주고 받을 수 있는 인터페이스가 존재한다는 것은 보안 공격에 매우 취약하게 된다는 것을 의미하고, 취약한 보안으로 인하여 인증키 K의 원격 전송 과정에서 해킹될 수 있는 확률이 높아짐을 의미한다.
- [68] 즉, 인증키 K는 노출되었을 때 eUICC(270)의 복제가 가능하므로, 보안상 최상위 레벨의 중요도를 가지는 정보이다. 따라서, 인증키 K를 전달하기 위해서는 인증키 K에 최상위의 보안을 적용하여 전달할 필요가 있으며, eUICC(270) 내부에서도 인증키 K에 대해 최상위 보안레벨이 유지될 수 있어야 한다.
- [69] 상기한 바와 같은 요구를 충족시키기 위해 본 발명의 다른 실시예에서는 인증키 K에 최상위 레벨의 보안을 적용하고, 인증키가 eUICC(270)의 내부에 다운로드된 이후에도 최상위의 보안을 유지할 수 있는 방법을 제공한다.
- [70] 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법에서는 인증키 K에 최상위 레벨의 보안을 적용하는 방법으로, eUICC(270)가 원격으로부터 인증키 K를 전달받고, 인증키 K가 eUICC(270)의 내부에서 이동통신 사업자의

네트워크와 인증을 위해 사용되는 과정에서도 인증키 정보 K가 단독적으로 사용되지 않도록 하는 방법을 적용한다.

- [71] 일반적으로, 단말의 인증 과정은 네트워크로부터 입력값(예를 들면, 난수 값 등)을 전달받아 내부적으로 저장된 인증키와 함께 약속된 계산을 수행하고, 계산 결과를 네트워크로 전달하는 방법으로 처리된다.
- [72] 즉, 인증키는 eUICC(270)가 이동통신사업자 네트워크와 인증 처리를 문제없이 수행할 수 있는 형태로만 eUICC(270) 내에 존재하면 되며, 도 2에 도시한 바와 같이 인증키 정보 K를 단독적으로 전달하거나 출력할 필요가 없다.
- [73]
- [74] 도 3은 단말과 이동통신사업자 네트워크 사이의 인증 과정을 나타내는 순서도이다.
- [75] 도 3은 단말(310)에 장착된 USIM과 이동통신사업자의 인증 센터(AuC: Authentication Center)(350)간에 서로 공유하고 있는 인증키(K)를 이용하여 단말(310)과 네트워크간에 양방향으로 유효성을 확인하는 절차를 나타낸 것으로, 도 3에 도시한 절차의 수행을 통해 데이터의 기밀성 및 무결성을 보장하기 위해 사용되는 파라미터(Ciphering Key, Integrity Key)가 생성된다.
- [76] 도 3을 참조하면, 먼저 MSC(Mobile Switching Centre) 또는 SGSN(Serving GPRS Support Node)(330)은 인증 절차를 수행하기 위해 인증 데이터 요청(AUTHENTICATION DATA REQUEST) 메시지를 인증 센터(350)로 전송함으로써, 가입자 인증 데이터를 요구한다(S301). 여기서, 인증 데이터 요청 메시지에는 이동통신 서비스의 가입자 식별정보인 IMSI(International Mobile Subscriber Identity) 정보가 포함될 수 있다.
- [77] 인증 센터(350)는 MSC 또는 SGSN(330)으로부터 수신한 인증 데이터 요청 메시지에 포함된 IMSI 정보를 이용하여 가입자를 구별하고, RAND(Random number), K, AMF(Authentication Management Field) 및 SQN(Sequence Number) 값에 기초하여 XRES(Expected response), AUTN(Authentication Token), CK(Ciphering Key), IK(Integrity Key) 및 MAC(Message Authentication Code) 값을 생성한다(S303).
- [78] 여기서, RAND는 임의의 숫자(random number)를 의미하며, 소정의 이동통신사업자가 운용하는 홈 네트워크(home network)에서 생성되어 단말(310)로 전송된다. K는 비밀키를 의미하고 인증키(authentication key)라 불리며, 홈 네트워크(home network)의 인증 센터(350)와 단말(310)에 장착된 USIM에 각각 저장되어 있다. AMF는 인증시 사용한 알고리즘의 유형과, 인증 벡터(authentication vector) 생성 시 어떤 키 값을 사용했는지 알려주는 용도로 사용된다. SQN은 시퀀스(Sequence) 번호로, 이동통신 사업자별로 SQN을 생성하는 규칙이 다를 수 있으며, USIM에서 수신된 인증 벡터가 새로운 값이라는 것을 확인하는데 사용된다.
- [79] XRES는 USIM 카드에 대한 유효성을 판단할 때 사용된다.

AUTN(Authentication Token)은 SQN+AK, MAC, AMF로 구성된다. AK(Anonymity Key)는 인증을 시도 할 때마다 증가하는 SQN 값을 매스킹하여 SQN 값의 규칙성이 외부에 노출되지 않도록 하는 용도로 사용된다. CK는 암호화(ciphering) 알고리즘에 사용되는 값으로, 단말(310)과 MSC 또는 SGSN(330)간에 전송되는 데이터를 암호화 하는 용도로 사용된다. IK는 무결성(integrity) 알고리즘에 사용되는 값으로, 무선 구간을 통해 송수신 되는 시그널링(signaling) 메시지에 대한 무결성을 확인하는 용도로 사용된다. MAC은 단말(310)에서 네트워크의 유효성을 판단하는데 사용된다.

- [80] 한편, 인증 센터(350)는 RAND, XRES, CK, IK, ATUN을 포함하는 인증 벡터(AV: Authentication Vector)를 구성하고, 인증 데이터 응답(AUTHENTICATION DATA RESPONSE) 메시지를 통하여 n개의 인증 벡터(AV(1...n))를 MSC 또는 SGSN(330)으로 전송한다(S305). 여기서, 하나의 인증 벡터는 RAND, AUTN, CK, IK, XRES로 구성되며, AUTN은 SQN+AK, MAC, AMF로 구성된다. 또한, n개의 인증 벡터(AV(1...n))는 RAND, AUTN, XRES, CK, IK를 기본 구성으로 하는 n개의 인증 벡터들의 배열을 의미한다. 즉 AV(i)는 RAND(i), AUTN(i), XRES(i), CK(i), IK(i)로 구성된 인증 벡터를 의미한다.
- [81] MSC 또는 SGSN(330)은 인증 센터(350)로부터 제공된 n개의 인증 벡터들 중 인증에 사용할 인증 벡터(AV(i))를 선택하고 선택한 인증 벡터(AV(i))를 인증 요청(AUTHENTICATION REQUEST) 메시지에 포함시켜 단말(310)로 전송함으로써, 선택한 인증 벡터(AV(i))의 구성 요소 중 RAND(i) 및 AUTN(i)를 단말(310)로 전송한다(S307).
- [82] 단말(310)은 MSC 또는 SGSN(330)로부터 수신한 인증 요청(AUTHENTICATION REQUEST) 메시지에 포함된 RAND(i) 및 AUTN(i)를 USIM에 전달한다.
- [83] USIM은 단말(310)로부터 전달받은 RAND(i), AUTN(i) 값 및 USIM 카드 내부에 저장된 인증키인 K 값을 입력으로 RES(Response), XMAC(Expected Message Authentication Code), CK(Ciphering Key), IK(Integrity Key) 및 SQN(Sequence Number) 값을 생성한다(S309).
- [84] 이후, USIM은 RNC(Radio Network Controller)로부터 제공받은 MAC 값과 생성된 XMAC 값을 비교한다(S311).
- [85] USIM은 MAC 값과 XMAC 값이 서로 다른 것으로 판단되면, 인증 거절(AUTHENTICATION REJECT) 메시지를 MSC 또는 SGSN(330)에 전송한다(S313). 여기서, 인증 거절 메시지에는 인증 실패의 원인(cause)을 나타내는 정보로 MAC 실패(MAC failure)가 포함될 수 있다.
- [86] 또는, USIM은 MAC 값과 XMAC 값이 서로 동일한 것으로 판단되면, AUTN으로부터 추출한 SQN 값이 미리 지정된 SQN 범위 내에 포함되는가를 판단한다(S315).
- [87] 여기서, SQN이 미리 지정된 범위를 벗어나는 경우, USIM은 AUTS를 생성하고

인증 거절(AUTHENTICATION REJECT) 메시지에 인증 실패 원인을 나타내는 동기 실패(Sync failure) 정보와 생성된 AUTS(Authentication re-Synchronization token)를 포함시켜 MSC 또는 SGSN(330)으로 전송한다(S317). 여기서, 상기 AUTS는 MAC-S와 SQNms+AK로 구성된다.

[88] 또는, 단계 S315에서 SQN이 미리 지정된 범위내에 포함되는 경우 USIM은 생성한 RES 값을 인증 응답(AUTHENTICATION RESPONSE) 메시지에 포함시켜 MSC 또는 SGSN(330)으로 전송한다(S319).

[89] MSC 또는 SGSN(330)은 인증 응답(AUTHENTICATION RESPONSE) 메시지를 통해 단말(310)(또는 USIM)로부터 수신한 RES 값과 VLR(Visitor Location Register)/SGSN에 저장된 XRES 값을 비교한다(S321).

[90] 여기서, RES 값과 XRES 값이 같은 경우 MSC 또는 SGSN(330)은 인증 백터 배열에서 IK 및 CK를 선택하고(S323), 이로써 전체 인증 절차가 종료된다.

[91] 한편, MSC 또는 SGSN(330)은 단계 S313을 통해 단말(310)로부터 인증 거절(AUTHENTICATION REJECT) 메시지를 수신하거나, RES 값과 XRES 값이 서로 다른 경우 인증 실패 보고(AUTHENTICATION FAILURE REPORT) 메시지를 인증 센터(350)에 전송한다(S325). 여기서, 인증 실패 보고 메시지에는 IMSI, 인증 실패 원인(cause), 접속 유형(access type), 인증 재시도(authentication re-attempt) 정보, VLR/SGSN 주소, RAND 값 등의 정보를 포함할 수 있다.

[92] 또한, MSC 또는 SGSN(330)은 단계 S317을 통해 단말(310)로부터 인증 거절(AUTHENTICATION REJECT) 메시지를 수신하는 경우, 인증을 재시도 하기 위한 인증 데이터 요청 (AUTHENTICATION DATA REQUEST) 메시지를 인증 센터(350)에 전송할 수 있다(S327). 여기서, 인증 데이터 요청 메시지에는 동기 실패 지시(Synchronization failure indication) 정보, RAND 또는 AUTS 정보가 포함될 수 있다.

[93] 도 3에 도시한 인증 절차를 참조하면, eUICC를 구비하는 단말이 이동통신사업자 네트워크와 인증 기능을 수행하기 위해서 eUICC는 1개의 인증 요청(AUTHENTICATION REQUEST) 메시지와 3개의 응답 메시지 즉, 인증 응답(AUTHENTICATION RESPONSE(RES)), 인증 거절(AUTHENTICATION REJECT(MAC failure)), 인증 거절(AUTHENTICATION REJECT(Sync failure))을 처리해야 함을 알 수 있다.

[94] 이는 단말이 인증 요청에 대하여 상기한 3가지 형태의 응답으로 처리할 수 있는 경우, 인증키 K가 eUICC 내부에 단독적인 형태로 존재하지 않아도, 단말은 이동통신사업자 네트워크와의 인증 기능을 수행할 수 있음을 의미한다.

[95] 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법에서는 도 3에 도시한 바와 같은 인증 처리 과정을 고려하여 원격지에 위치한 장치에서 eUICC에 인증키를 전달할 때, 인증키를 단독적인 형태가 아닌 임의의 모듈(예를 들면, 인증 처리 모듈) 내에 캡슐화시켜 전달하는 방법을 사용한다.

[96]

- [97] 도 4는 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법 이 적용되는 eUICC의 구성을 나타내는 블록도이다.
- [98] 도 4를 참조하면, eUICC(400)는 처리부(410) 및 인증 처리 모듈(430)을 포함할 수 있다.
- [99] 처리부(410)는 인증 처리 모듈(430)을 다운로드 하기 위해 필요한 처리를 수행할 수 있다. 또한, 처리부는 eUICC(400)와 관련된 다양한 어플리케이션들을 실행할 수 있다.
- [100] 인증 처리 모듈(430)은 인증과 관련된 처리를 수행하는 모듈로, 내부에 인증키 K(431)가 캡슐화되어 포함된다.
- [101] 본 발명의 다른 실시예에서는 전술한 본 발명의 일 실시예와는 달리 eUICC(400)가 이동통신사업자 서버로부터 다운로드하는 인증키 K(431)가 단독적인 형태로 전달되지 않으며 미리 지정된 형식의 모듈을 통해 캡슐화(encapsulated)되어 전달된다. 여기서 인증키 K(431)를 캡슐화하여 전달한다는 것은 인증키 K(431)를 단독적인 형태로 전달하지 않는 것을 의미한다.
- [102] 인증키 K(431)의 캡슐화에 사용되는 모듈은 다양한 형식의 모듈이 사용될 수 있다. 예를 들어, 인증키 K(431)의 캡슐화에 사용되는 모듈은 인증키 K(431)를 임의의 다른 정보들과 함께 가공하여 인증키 K(431)의 형식을 원래 형식과 다른 새로운 형식으로 생성할 수 있는 임의의 암호화 모듈이 될 수 있다.
- [103] 바람직하게는, 상기 캡슐화 모듈은 단말이 네트워크로부터 받는 특정 값을 입력 값(예를 들어, 난수 값)으로 하여 상기한 3가지의 응답(즉, 인증 응답, 인증 거절(MAC 실패), 및 인증 거절(동기화 실패))중의 하나를 출력할 수 있는 인증 처리 모듈(430)로 구성될 수 있다.
- [104] 본 발명의 다른 실시예에서는 인증키 K(431)가 단독적인 형태로 전달되거나, 인증키 K(431)의 전달을 위한 특정 인터페이스를 사용하지 않기 때문에 eUICC(400)가 인증되지 않은 네트워크를 이용하여 인증키 K(431)를 다운로드하는 경우에도 해킹에 의해서 인증키 K(431)가 유출될 가능성이 없다.
- [105] 또한, 인증키 K(431)를 eUICC(400)의 인증 처리 모듈(430) 내부에 저장함에 따라 다음과 같이 최상위 보안 레벨을 적용하는 효과를 얻을 수 있다.
- [106] 인증키 K(431)를 생성 또는 변경하기 위한 단말과의 인터페이스가 존재하지 않는다. 전술한 바와 같이 인증키 K(431)를 단독적인 형태 그대로 주고 받을 수 있는 인터페이스가 존재한다는 것은 보안 공격에 매우 취약해지는 문제가 발생할 수 있고, 해킹될 수 있는 확률이 높아지게 된다. 예를 들어, 해킹 프로그램이 인증 알고리즘과 인증키 K와의 인터페이스 정보를 알아내는 경우 해킹 프로그램은 인증 알고리즘처럼 동작하여 인증키 K를 추출해 낼 수 있다. 그러나, 본 발명의 다른 실시예에서는 상기한 바와 같은 인터페이스를 사용하지 않기 때문에 인증키가 해킹될 가능성이 없다.
- [107] 또한, 본 발명의 다른 실시예에서는 인증 처리 모듈(430) 내에 다양한 보안

기법을 적용하여 인증키 K(431)가 노출되는 것을 방지한다.

- [108] 예를 들어, 인증 처리 모듈(430)은 슈도(Pseudo) 암호화 연산을 통해 메모리 상에서 인증키 K(431)가 연산에 사용된 위치를 숨길 수 있다. 또한, 인증키를 이용한 암호/복호화시 사용된 버퍼를 모두 초기화하여 연산된 값을 추정할 수 없도록 한다. 또한, 인증키를 이용한 암호/복호화 연산시 역탐지(counter measure) 기능을 제공하여 불법 접근을 방지한다. 여기서, 암호/복호화에 필요한 인증키는 인증 처리 모듈(430) 내에 가지고 있으면 되므로 상기한 바와 같은 보안 기법을 적용하는 경우에도 신규로 암호화키를 할당받을 필요가 없다.
- [109] 또한, 인증 처리 모듈(430)내에 내부적으로 인증키 K(431)를 가지고 있음에 따라 상술한 바와 같은 보안 기법들 뿐만 아니라 외부의 공격으로부터 방어할 수 있는 수많은 기법들을 적용할 수 있다.
- [110]
- [111] 도 5는 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법을 나타내는 개념도로서, eUICC가 인증키 K를 캡슐화한 모듈을 MNO 서버로부터 다운로드 하는 과정을 예시한 것이다.
- [112] 도 5를 참조하면, 먼저 MNO 서버(510)는 가입자의 인증키(K)를 캡슐화한 모듈을 생성하고, 생성한 캡슐화 모듈 SM-DP(530)에 전달한다. 여기서, MNO 서버(510)는 인증 처리 모듈(501)을 이용하여 인증키 K를 캡슐화할 수 있다. 또한, MNO 서버(510)는 인증키가 캡슐화된 인증 처리 모듈(501)을 일반 애플릿과 동일한 형태(예를 들면, .cap)의 파일(또는 라이브러리)로 생성할 수 있다.
- [113] SM-DP(530)는 MNO 서버(510)로부터 제공받은 인증 처리 모듈(501)을 SM-SR(550)에 전달한다. 여기서, SM-DP(530)는 SM-SR(550)을 통해 eUICC(570)에 전달될 인증 처리 모듈(501)을 암호화하여 OTA 패키지를 생성하고, 암호화된 OTA 패키지를 SM-SR(550)에 전달할 수 있다.
- [114] SM-SR(550)은 SM-DP(530)로부터 제공된 OTA 패키지를 해당 목적 eUICC(570)에 전달한다. 여기서, SM-SR(550)은 암호화된 OTA 통신 방식을 이용하여 eUICC(570)에 OTA 패키지를 전달할 수 있고, 암호화된 OTA 패키지에는 인증키가 캡슐화되어 포함된 인증 처리 모듈(501)이 포함될 수 있다.
- [115] eUICC(570)는 SM-SR(550)로부터 전달받은 암호화된 OTA 패키지를 복호화하여 인증키가 캡슐화된 인증 처리 모듈(501)을 추출한 후, 추출한 인증 처리 모듈(501)을 내부에 저장할 수 있다.
- [116] 도 5에 도시한 바와 같이 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법에서는, MNO 서버(510)로부터 eUICC(570)로 전달되는 인증키를 다른 형식의 파일(예를 들면, 인증 처리 모듈(501))에 캡슐화한 후, 캡슐화된 파일을 암호화하여 eUICC(570)에 전달함으로써, 인증키의 전달에 대한 보안 레벨을 최상위 레벨로 강화시킬 수 있다.

[117]

- [118] 한편, 인증키가 캡슐화된 인증 처리 모듈이 eUICC의 내부에 저장된 이후, eUICC는 인증키 K가 외부에 노출되지 않으면서 이동통신사업자 네트워크와 인증 기능을 수행할 수 있어야 한다.
- [119] 도 6은 본 발명의 다른 실시예에 따라 eUICC에 인증키가 저장된 이후의 인증 처리의 수행 과정을 설명하기 위한 개념도이다.
- [120] 도 6에서는 단말(610)과 eUICC(630)를 각각 독립적인 블록으로 도시하였으나, 이는 설명의 편의를 위한 것일 뿐이며, 실제로 eUICC(630)는 단말(610)의 내부에 칩 형태로 실장되는 방식으로 구성될 수 있다.
- [121] 도 6을 참조하면, eUICC(630)는 하나 내지 네 개의 인증 처리를 위한 인터페이스를 통해 단말(610)과 메시지를 송수신하여 이동통신사업자 네트워크와의 인증 기능을 제공하기만 하면, 단말(610)은 인증키 K를 단독적인 형태로 다운로드하지 않아도 인증키 K가 요구되는 인증 처리를 수행할 수 있다.
- [122] 즉, 단말(610)은 이동통신사업자 네트워크와 인증을 처리하는 과정에서 인증(Authenticate) 인터페이스(601)를 통해 eUICC의 처리부에 인증을 요청하면, eUICC의 처리부(631)는 인증 요청을 인증 처리 모듈(633)에 제공한다.
- [123] 인증 처리 모듈(633)은 처리부(631)로부터 제공된 인증 요청에 상응하여 전송한 바와 같은 처리를 수행한 후, 인증 요청에 대한 응답을 처리부(631)에 제공하고, 처리부(631)는 인증 성공 응답 인터페이스(602), 인증 실패 응답 인터페이스(603) 및 동기화 실패 응답 인터페이스(604) 중 해당 인터페이스를 통해 인증 처리 모듈로부터 제공된 응답 메시지를 단말에 제공한다.
- [124] 도 6에서 인증(Authenticate) 인터페이스(601), 인증 성공 응답 인터페이스(602), 인증 실패 응답 인터페이스(603) 및 동기화 실패 응답 인터페이스(604)는 각각 메시지 형태로 구성될 수 있다.
- [125]
- [126] 이하에서는 도 7 내지 도 9를 참조하여 도 6에 도시한 네 개의 인증 처리를 위한 인터페이스 각각에 대해 보다 구체적으로 설명한다.
- [127] 도 7은 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법에서 사용되는 인증 인터페이스의 일 예를 나타낸 것이다. 도 8은 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법에서 사용되는 인증 성공 응답 인터페이스의 일 예를 나타내는 것이다. 또한, 도 9는 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법에서 사용되는 동기화 실패 응답 인터페이스의 일 예를 나타내는 것이다.
- [128] 먼저 도 7을 참조하면, 인증(AUTHENTICATE) 인터페이스(또는 인증 메시지)는 명령어(instruction)의 클래스를 지시하는 CLA 필드, 명령어(instruction)를 나타내는 INS 필드, 제1 파라미터를 지시하는 P1 필드, 제2 파라미터를 지시하는 P2 필드, 명령어(command) 데이터의 길이를 지시하는 Lc 필드 및 인증 관련 데이터를 포함하는 DATA 필드를 포함할 수 있다. 여기서, 상기 DATA 필드에는 네트워크로부터 제공된 RAND(Random number)와

AUTN(Authentication Token)이 포함될 수 있다.

- [129] 인증 처리 모듈은 단말로부터 인증 메시지를 수신하면, RAND와 비밀키(K)를 이용하여 XMAC(Expected Message Authentication Code)을 계산한다. 이후, 인증 처리 모듈은 AUTN에 포함되어 전달된 MAC(Message Authentication Code)과 계산된 XMAC을 비교하여 두 값이 서로 동일한가를 판단한다. 또한, 인증 처리 모듈은 SQN(Sequence Number)이 미리 정의된 유효한 영역안에 있는지 확인한다.
- [130] 만약, MAC과 XMAC이 서로 동일하고, SQN이 유효한 영역안에 있는 경우, 인증 처리 모듈은 인증 응답인 RES(Response)를 계산하고, 도 8에 도시한 바와 같은 인증 성공 응답 인터페이스(또는 인증 성공 응답 메시지)를 이용하여 단말에 인증이 성공하였음을 통보한다. 여기서, 인증 처리 모듈은 RES와 함께 계산된 암호화 키(CK)와 무결성 키(IK)도 단말에 전달한다.
- [131] 인증 성공 응답 인터페이스(또는 인증 성공 응답 메시지)는 도 8에 예시한 바와 같이 구성될 수 있다. 즉, 인증 성공 응답 인터페이스는 인증 성공 여부를 지시하는 'DB' 필드, 인증 값을 지시하는 RES, 암호화 키 CK, 무결성 키 IK 및 2G(2세대 이동통신방식)의 암호화 키 Kc 정보를 포함할 수 있다.
- [132] 한편, 단말은 eUICC로부터 인증 성공 응답 메시지를 수신하면, 인증 응답(AUTHENTICATION RESPONSE) 메시지 내에 수신한 해당 응답(RES)을 포함하여 네트워크로 전달한다.
- [133] 단말로부터 인증 응답을 수신한 네트워크(MSC 또는 SGSN)는, 단말에서 인증 응답 메시지에 포함시켜 전송한 인증 응답 RES와 미리 저장되어 있는 XRES(Expected Response)를 비교한다. 여기서, RES와 XRES가 동일한 경우, 네트워크측에서 단말은 인증된다.
- [134] 상기한 바와 같이 단말이 네트워크에 인증된 후, 단말과 네트워크는 상호간에 생성된 암호화 키(CK)와 무결성 키(IK)를 이용하여 보안 채널을 구성하고, 이후 보안 채널을 이용하여 통신을 수행함으로써 신뢰성을 보장받는다.
- [135] 또는, eUICC의 인증 처리 모듈은 계산한 XMAC과 MAC을 비교한 결과, 두 값이 서로 다른 경우, SW(Status Word)=9082로 설정한 인증 실패 응답 메시지(또는 인증 실패 응답 인터페이스)를 단말로 전송한다. 이 경우, 네트워크에 단말의 인증 및 등록은 실패하게 된다.
- [136] 단말은 eUICC로부터 제공된 인증 실패 응답 메시지에 상응하여 인증 거절(AUTHENTICATION REJECT) 메시지 내에 실패 원인을 지시하는 정보를 포함시켜 네트워크로 전달한다.
- [137]
- [138] 한편, 동기화 관리는 무선구간에서 암호화 없이 그대로 전송되는 인증 벡터를 허가받지 않은 사용자가 획득하고 획득한 인증 벡터를 이용하여 공격하는 상황을 방지하기 위해 수행된다. 즉, 동기화 관리는 한번 사용된 인증 벡터가 재사용될 수 없도록 처리하는 것을 의미한다.

- [139] 인증 처리 모듈은 네트워크로부터 전달된 AUTN내에 포함된 MAC과 SQN을 확인하고, 계산한 XMAC과 네트워크로부터 전달된 MAC이 동일하나 SQN이 유효한 범위내에 있지 않을 경우, 동기화가 실패한 것으로 판단하고 동기화 실패 응답 메시지(또는 동기화 실패 응답 인터페이스)를 이용하여 단말에 응답한다.
- [140] 일반적으로 네트워크(인증센터)는 SQN을 인증 처리 모듈에 저장된 값보다 큰 값으로 생성하고, 인증 처리 모듈은 인증 성공시 저장된 SQN 값을 네트워크에서 생성한 SQN 값으로 갱신한다.
- [141] 인증 처리 모듈은 동기화 실패시 도 9에 도시한 바와 같은 포맷을 가지는 동기화 실패 응답 메시지(또는 동기화 실패 응답 인터페이스)를 단말에 전송한다.
- [142] 동기화 실패 응답 메시지는 도 9에 도시한 바와 같이 동기화 실패 태그를 지시하는 'DC', AUTS의 길이를 지시하는 'OE' 및 AUTS 정보를 포함할 수 있다.
- [143] 네트워크(인증 센터)는 인증 처리 모듈로부터 전달된 AUTS(Authentication re-Synchronization token)와 기저장된 RAND를 포함하는 새로운 인증 벡터를 생성한다.
- [144] 즉, 네트워크는 AUTS의 MAC-S(Message Authentication Code-Synchronization)를 확인하고, MAC-S 값이 유효하면 SQN을 갱신한 후에 새로운 인증 벡터를 생성하여 단말과 재인증 절차를 수행한다. 일반적으로 재동기화 이후에 인증은 성공하여야 한다.
- [145]
- [146] 도 10은 본 발명의 다른 실시예에 따른 이동통신사업자 정보 제공 방법을 나타내는 흐름도로서, eUICC를 구비한 단말에서 수행되는 처리 과정을 예시한 것이다.
- [147] 도 10을 참조하면, 먼저, 단말은 인증키 등과 같은 이동통신사업자 정보가 캡슐화되어 있는 데이터(예를 들면, 인증 처리 모듈)를 네트워크로부터 수신한다(S1001).
- [148] 단말은 상기 데이터를 상기 eUICC 내에 저장한다(S1003). 여기서, 수신된 데이터에 캡슐화되어 포함된 이동통신사업자 정보는 데이터에 캡슐화된 상태로 eUICC 내에 저장된다.
- [149] 이후, 단말은 네트워크로부터 인증 요청이 수신되는가를 판단하고(S1005), 인증 요청이 수신되는 경우, 상기 인증 요청에 포함된 파라미터들을 인증 인터페이스를 통해 eUICC에 전송한다(S1007).
- [150] 이후, 단말은 eUICC로부터 인증 요청에 상응하는 응답을 수신한다(S1009). 여기서, 상기 인증 요청에 상응하는 응답은 도 6 내지 도 9를 참조하여 설명한 바와 같이, 인증 성공 응답, 인증 실패 응답 및 동기화 실패 응답 중 어느 하나가 될 수 있다.
- [151] 단말은 eUICC로부터 수신한 응답에 상응하는 메시지를 네트워크로 전송한다(S1011).

[152]

[153] 상술한 바와 같은 본 발명의 실시예에 따른 이동통신사업자의 정보 제공 방법 및 장치에 따르면, eUICC에 제공하기 위해 전달하는 인증키를 최상위 보안 기법을 적용하여 전달할 수 있다. 일반적으로 단말의 개통되기 이전에는 eUICC 내에 이동통신사업자의 프로파일(Profile)이 존재하지 않기 때문에, 단말과 이동통신사업자 네트워크간에 인증이 이루어지지 않게 되고 이에 따라 보안이 이루어지지 않은 공개된 무선 네트워크를 통해 이동통신사업자의 정보를 전달해야 한다. 본 발명의 실시예에 따른 이동통신사업자의 정보 제공 방법은 이와 같은 환경에서 더 큰 보안 효과를 기대할 수 있다.

[154] 또한, 본 발명에서는 eUICC의 내부에 인증키를 캡슐화하여 저장하여 인증키에 접근할 수 인터페이스가 존재하지 않도록 구성함으로써 인터페이스를 이용한 외부 해킹 공격에 의해 인증키가 노출되지 않게 되고, 이에 따라 eUICC의 복제를 방지할 수 있다.

[155]

[156] 이상 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

[157]

청구범위

- [청구항 1] eUICC(Embedded Universal Integrated Circuit Card)를 구비한 단말에서 수행되는 이동통신사업자 정보 제공 방법에 있어서, 이동통신사업자 정보가 캡슐화되어 포함된 데이터를 수신하는 단계; 및
상기 수신한 데이터를 상기 eUICC에 저장하는 단계를 포함하는 이동통신사업자 정보 제공 방법.
- [청구항 2] 청구항 1에 있어서,
상기 이동통신사업자 정보가 캡슐화되어 포함된 데이터를 수신하는 단계는,
상기 단말의 인증을 위한 인증키 정보가 캡슐화되어 포함된 데이터를 수신하는 것을 특징으로 하는 이동통신사업자 정보 제공 방법.
- [청구항 3] 청구항 2에 있어서,
상기 인증키 정보가 캡슐화되어 포함된 데이터는 상기 단말의 인증을 처리하는 인증 처리 모듈의 데이터인 것을 특징으로 하는 이동통신사업자 정보 제공 방법.
- [청구항 4] 청구항 1에 있어서,
상기 이동통신사업자 정보가 캡슐화되어 포함된 데이터를 수신하는 단계는,
상기 단말의 인증을 위한 인증키 정보의 형식을 이전과 다른 형식으로 생성하는 암호화 모듈 데이터를 수신하는 것을 특징으로 하는 이동통신사업자 정보 제공 방법.
- [청구항 5] 청구항 1에 있어서,
상기 수신한 데이터를 상기 eUICC에 저장하는 단계는,
상기 단말의 인증을 처리하는 인증 처리 모듈을 상기 eUICC에 저장하고, 상기 이동통신사업자 정보는 인증키를 포함하되, 상기 인증키는 상기 인증 처리 모듈에 캡슐화된 상태로 상기 eUICC에 저장되는 것을 특징으로 하는 이동통신사업자 정보 제공 방법.
- [청구항 6] 청구항 5에 있어서,
상기 인증 처리 모듈은 상기 eUICC에 저장된 후, 상기 단말로부터 제공된 인증 요청에 상응하여 인증 처리를 수행한 후, 인증 처리 결과에 대한 응답으로 인증 성공 응답, 인증 실패 응답 및 동기화 실패 응답 중 어느 하나의 응답을 상기 단말에 제공하는 것을 특징으로 하는 이동통신사업자 정보 제공 방법.
- [청구항 7] 청구항 5에 있어서,
상기 이동통신사업자 정보 제공 방법은,

상기 인증 처리 모듈이 상기 eUICC에 저장된 후, 상기 인증키가 사용되는 경우, 상기 인증키의 노출을 방지하기 위한 처리를 수행하는 단계를 더 포함하는 것을 특징으로 하는 이동통신사업자 정보 제공 방법.

[청구항 8] 이동통신사업자 서버에서 수행되는 이동통신사업자 정보 제공 방법에 있어서,

이동통신사업자 정보를 캡슐화한 모듈을 생성하는 단계; 및
상기 캡슐화한 모듈을 특정 단말로 전송하는 단계를 포함하는 이동통신사업자 정보 제공 방법.

[청구항 9] 청구항 8에 있어서,

상기 이동통신사업자 정보를 캡슐화한 모듈을 생성하는 단계는, 인증 처리를 수행하는 인증 처리 모듈에 상기 이동통신사업자 정보로 인증키를 캡슐화하여 포함시켜 상기 캡슐화한 모듈을 생성하는 것을 특징으로 하는 이동통신사업자 정보 제공 방법.

[청구항 10] 청구항 8에 있어서,

상기 이동통신사업자 정보를 캡슐화한 모듈을 생성하는 단계는, 상기 캡슐화한 모듈을 애플릿 파일과 동일한 형태의 파일로 생성하는 것을 특징으로 하는 이동통신사업자 정보 제공 방법.

[청구항 11] 청구항 8에 있어서,

상기 캡슐화한 모듈을 특정 단말로 전송하는 단계는,
상기 캡슐화한 모듈을 SM-DP(Subscription Manager - Data Preparation)에 전송하는 단계;
상기 SM-DP가 상기 캡슐화한 모듈을 SM-SR(Subscription Manager Secure Routing)에 전송하는 단계; 및
상기 SM-SR이 상기 캡슐화한 모듈을 OTA(Over The Air) 통신 방식을 통해 상기 특정 단말로 전송하는 단계를 포함하는 것을 특징으로 하는 이동통신사업자 정보 제공 방법.

[청구항 12] 이동통신사업자 정보가 캡슐화된 모듈; 및
상기 이동통신사업자 정보가 캡슐화된 모듈을 다운로드 하기 위한 처리를 수행하는 처리부를 구비하는 eUICC(Embedded Universal Integrated Circuit Card)를 포함하는 장치.

[청구항 13] 청구항 12에 있어서,

상기 이동통신사업자 정보가 캡슐화된 모듈은
상기 장치의 인증을 위한 인증키가 캡슐화되어 포함되고, 인증을 위한 처리를 수행하는 인증 처리 모듈인 것을 특징으로 하는 장치.

[청구항 14] 청구항 13에 있어서,

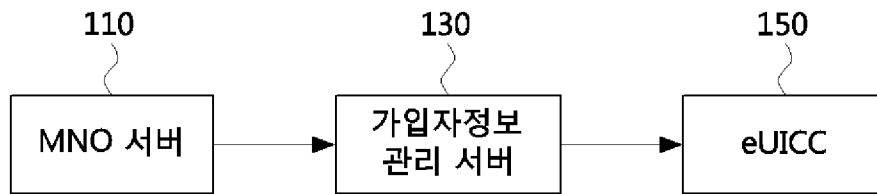
상기 처리부는,
상기 장치로부터 인증 요청 메시지를 수신하여 상기 인증 처리

[청구항 15]

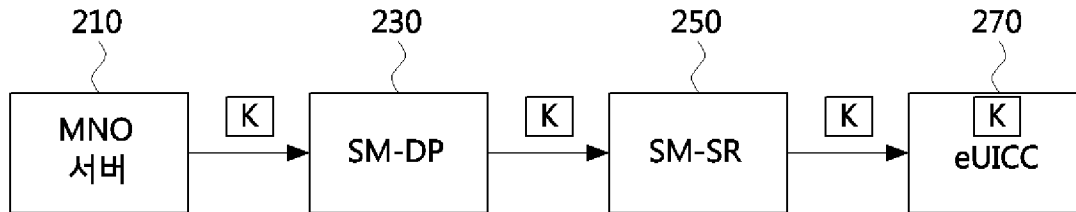
모듈에 제공하고, 상기 인증 처리 모듈로부터 인증 결과로 제공된 응답을 수신하여 상기 장치에 제공하는 것을 특징으로 하는 장치.
청구항 13에 있어서,

상기 인증 처리 모듈은, 상기 처리부로부터 제공된 인증 요청에 상응하여 인증 처리를 수행한 후, 인증 성공을 지시하는 인증 성공 응답, 인증 실패를 지시하는 인증 실패 응답 및 동기화 실패를 지시하는 동기화 실패 응답 중 어느 하나의 응답을 상기 처리부를 통해 상기 장치에 제공하는 것을 특징으로 하는 장치.

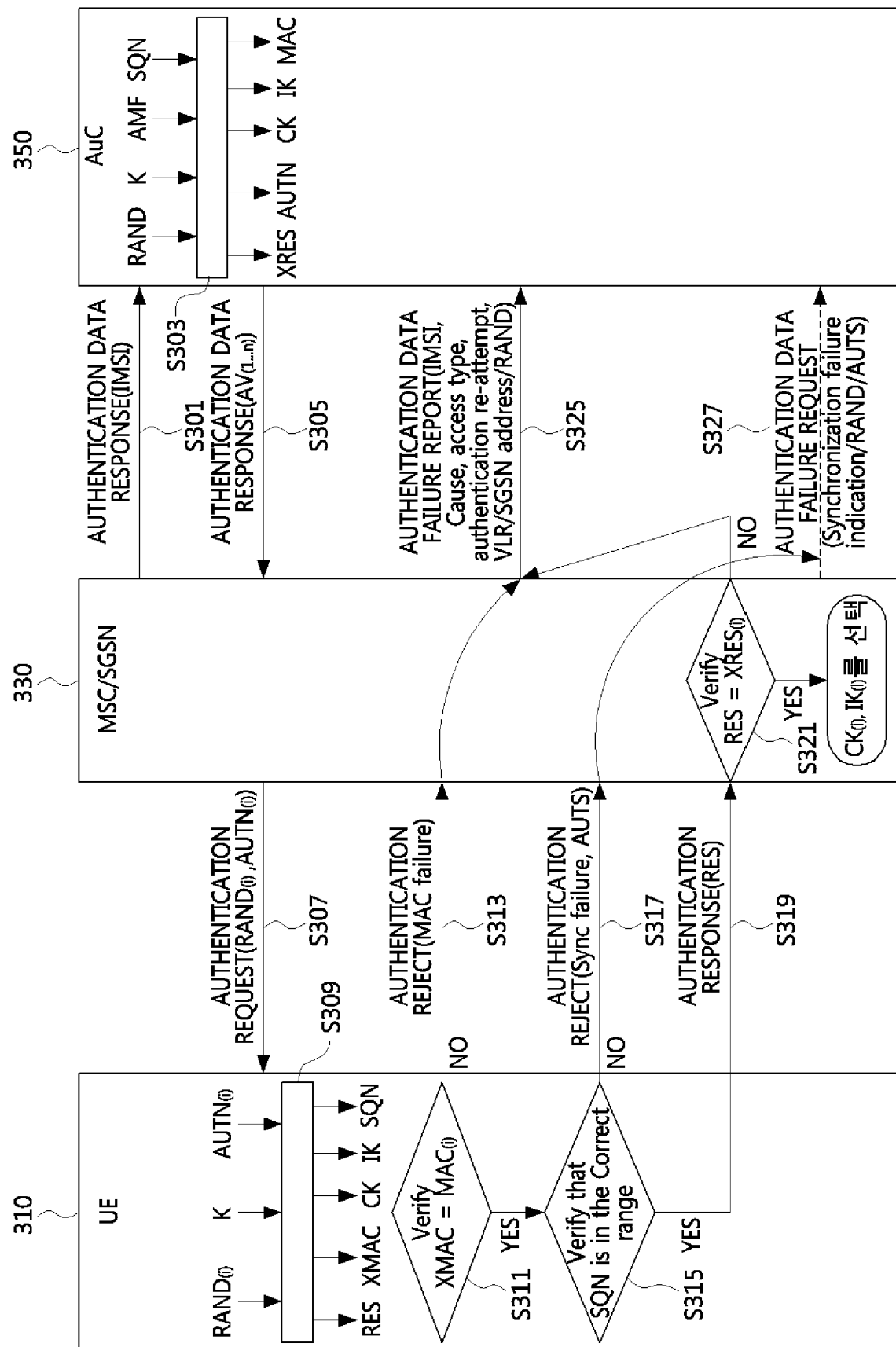
[Fig. 1]



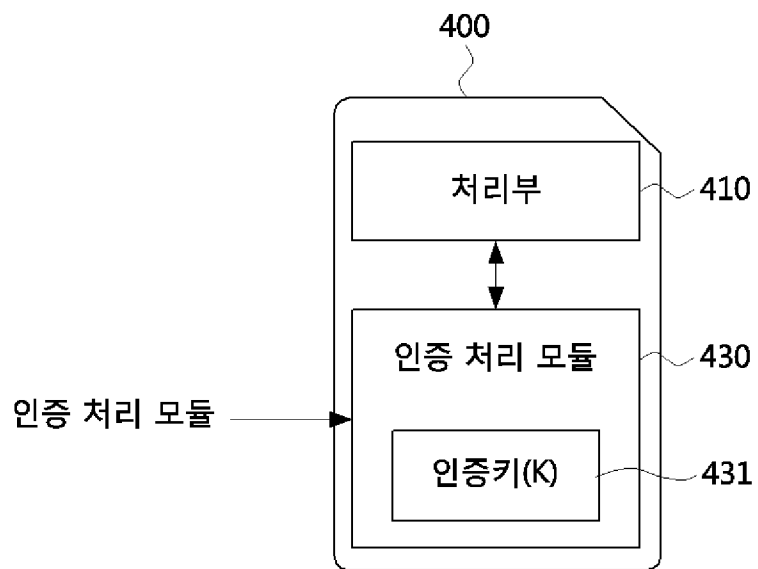
[Fig. 2]



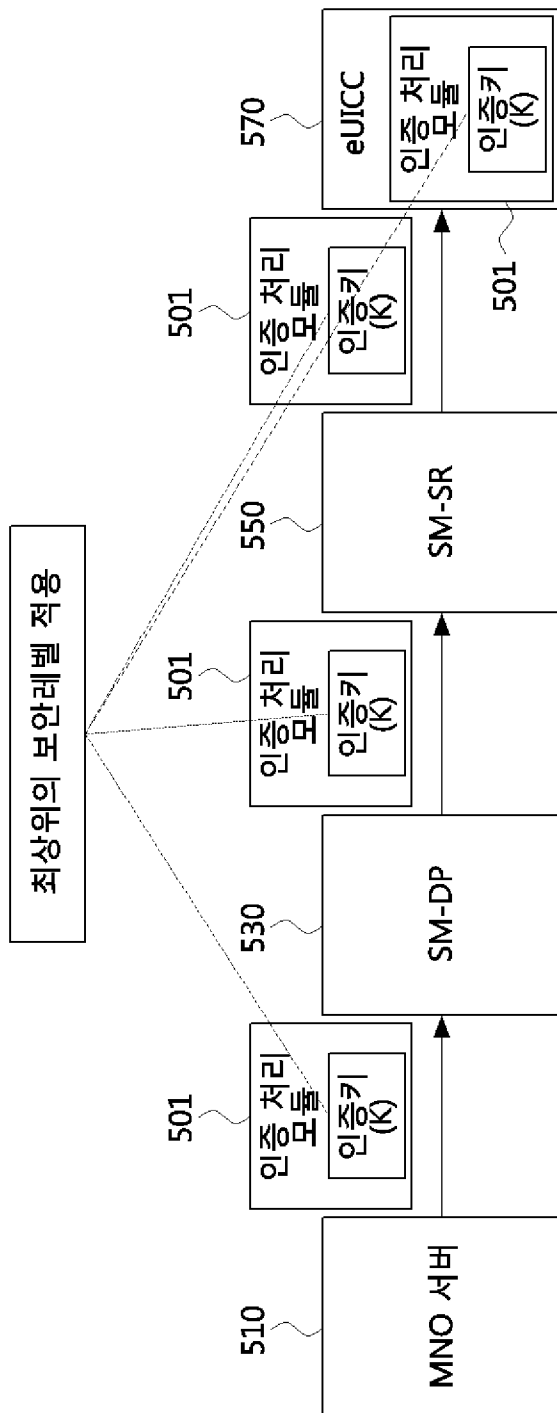
[Fig. 3]



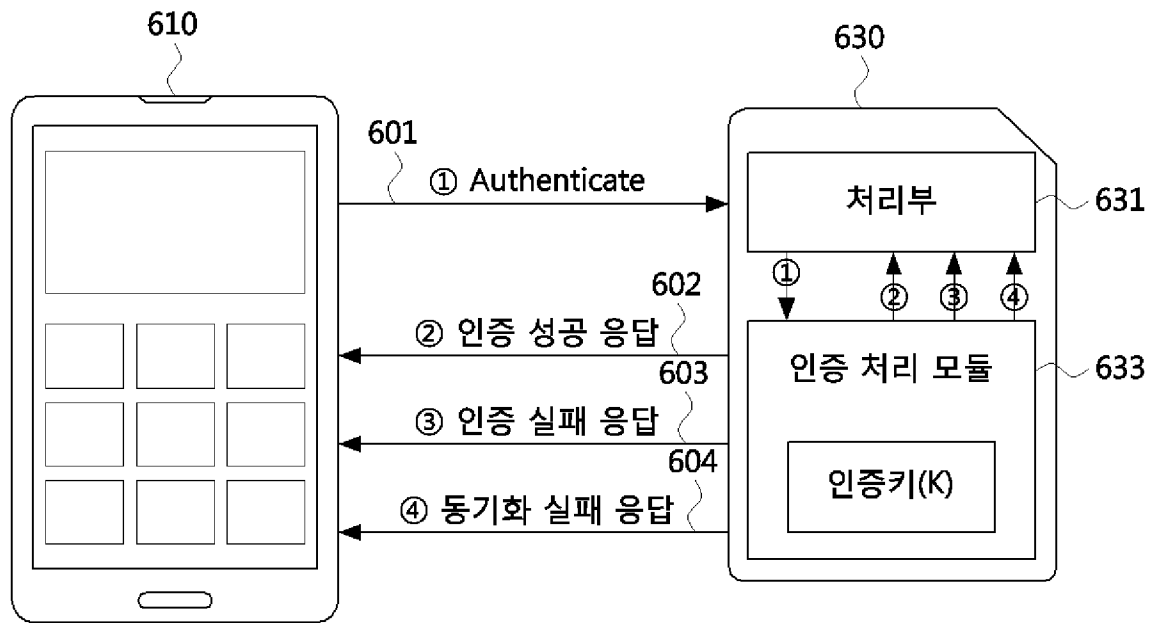
[Fig. 4]



[Fig. 5]



[Fig. 6]



[Fig. 7]

CLA	INS	P1	P2	Lc	DATA
00	88	00	아래 참조	22	아래 참조
P2	Authentication context: 0x81 = UMTS AKA				
DATA	인증 관련 데이터:				
	Byte	내용			길이
	1	RAND 길이 (0X10)			1
	2-17	RAND			16
	18	AUTN 길이 (0X10)			1
	19-34	AUTN			16
	AUTN 포맷				
	Byte	내용			길이
	1-6	SQN⊕AK			6
	7-8	AMF			2
	9-16	MAC			8

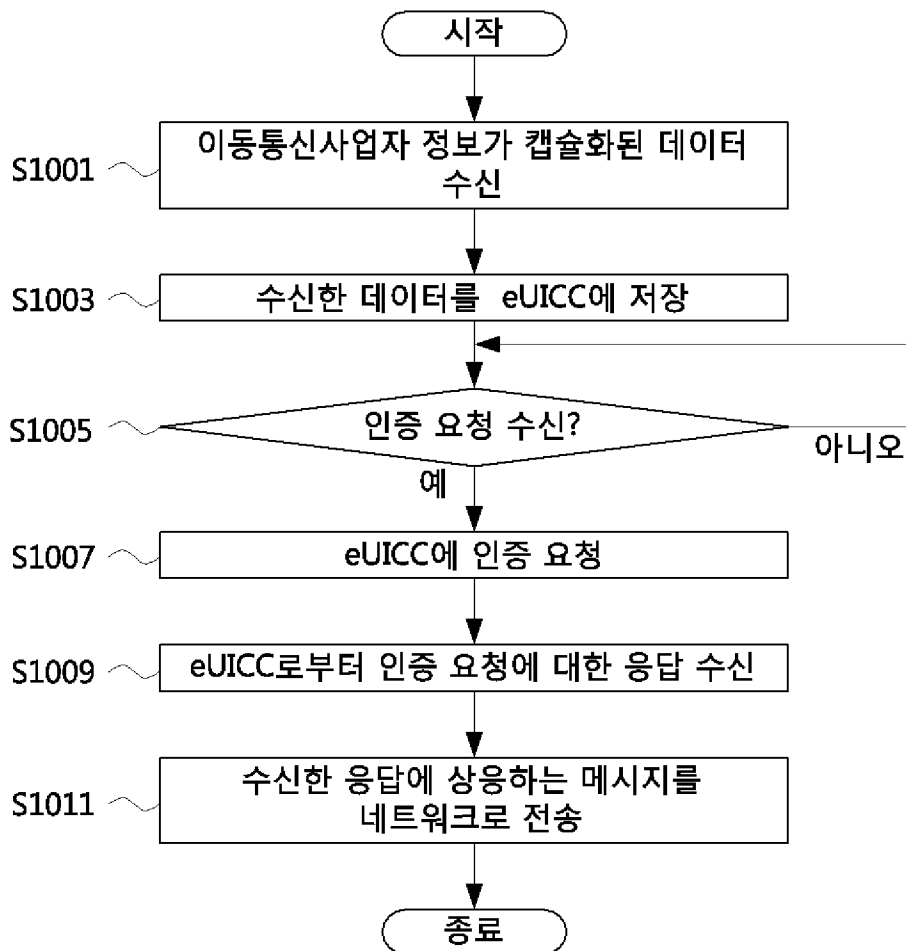
[Fig. 8]

Byte	내용	길이
1	'DB'=UMTS 인증 성공 태그	1
2	RES 길이 (0X08)	1
3-10	RES	8
11	CK 길이 (0x10)	1
12-27	CK	16
28	IK 길이 (0x10)	1
29-44	IK	16
45	Kc 길이 (0x08)	1
46-53	Kc	8

[Fig. 9]

Byte	내용	길이
1	'DC'=동기화 실패 태그	1
2	'0E'=AUTS 길이	1
3-16	AUTS	14
AUTS 포맷		
Byte	내용	길이
1-6	$SQN_{Ms} \oplus AK^*$	6
7-14	MAC-S	8

[Fig. 10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2013/004536**A. CLASSIFICATION OF SUBJECT MATTER*****H04W 12/08(2009.01)i, H04W 12/06(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 12/08; H04W 4/06; H04N 7/12; H04W 36/08; G06Q 50/00; H04B 1/40; H04L 12/56; H04W 36/02; H04W 12/06; H04W 8/18

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: capsule, information, mobile communication, data, reception, storage

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2008-0033686 A (SAMSUNG ELECTRONICS CO., LTD.) 17 April 2008 See abstract; claims 1, 2 and 7; figures 4, 5.	1,8,12
A		2-7,9-11,13-15
A	KR 10-2008-0111374 A (SAMSUNG ELECTRONICS CO., LTD.) 23 December 2008 See abstract; claims 1, 12, 14 and 17; figures 2a, 2b, 3, 11a and 11b.	1-15
A	KR 10-2004-0041120 A (JUNG, Kyung Rae) 14 May 2004 See abstract; claim 1; figures 1-3.	1-15
A	KR 10-2005-0040961 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 04 May 2005 See abstract; claims 1, 5; figure 3.	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

20 AUGUST 2013 (20.08.2013)

Date of mailing of the international search report

20 AUGUST 2013 (20.08.2013)

Name and mailing address of the ISA/KR



Korean Intellectual Property Office
Government Complex-Daejeon, 189 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/KR2013/004536

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2008-0033686 A	17/04/2008	US 2008-0089256 A1 US 7907556 B2	17/04/2008 15/03/2011
KR 10-2008-0111374 A	23/12/2008	CA 2666573 A1 CA 2666573 C CA 2667571 A1 CA 2702054 A1 CN 101558589 A CN 101558643 A CN 101558643 B CN 101822009 A CN 101822009 B KR 10-1122200 B1 KR 10-1227029 B1 KR 10-2008-0100753 A KR 10-2008-0101616 A KR 10-2009-0036499 A KR 10-2010-0123808 A KR 10-2010-0123809 A KR 10-2010-0123810 A US 2008-0285556 A1 US 2008-0285679 A1 US 2008-0313678 A1 US 2009-0092092 A1 US 2009-0296624 A1 US 7983251 B2 US 8275002 B2 WO 2008-140261 A2 WO 2008-140261 A3 WO 2008-140263 A1 WO 2008-143435 A1 WO 2008-156257 A2 WO 2008-156257 A3 WO 2009-048208 A1	20/11/2008 29/01/2013 20/11/2008 16/04/2009 14/10/2009 14/10/2009 24/04/2013 01/09/2010 09/01/2013 12/06/2012 28/01/2013 19/11/2008 21/11/2008 14/04/2009 25/11/2010 25/11/2010 25/11/2010 20/11/2008 20/11/2008 18/12/2008 09/04/2009 03/12/2009 19/07/2011 25/09/2012 20/11/2008 31/12/2008 20/11/2008 27/11/2008 24/12/2008 12/03/2009 16/04/2009
KR 10-2004-0041120 A	14/05/2004	NONE	
KR 10-2005-0040961 A	04/05/2005	NONE	

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 12/08(2009.01)i, H04W 12/06(2009.01)i, H04W 8/18(2009.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04W 12/08; H04W 4/06; H04N 7/12; H04W 36/08; G06Q 50/00; H04B 1/40; H04L 12/56; H04W 36/02; H04W 12/06; H04W 8/18

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 캡슐, 정보, 이동통신, 데이터, 수신, 저장

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-2008-0033686 A (삼성전자주식회사) 2008.04.17 요약; 청구항 1, 2, 7; 도면 4, 5 참조.	1, 8, 12
A		2-7, 9-11, 13-15
A	KR 10-2008-0111374 A (삼성전자주식회사) 2008.12.23 요약; 청구항 1, 12, 14, 17; 도면 2a, 2b, 3, 11a, 11b 참조.	1-15
A	KR 10-2004-0041120 A (정경래) 2004.05.14 요약; 청구항 1; 도면 1-3 참조.	1-15
A	KR 10-2005-0040961 A (한국전자통신연구원) 2005.05.04 요약; 청구항 1, 5; 도면 3 참조.	1-15

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

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

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

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

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

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

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

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

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2013년 08월 20일 (20.08.2013)

국제조사보고서 발송일

2013년 08월 20일 (20.08.2013)

ISA/KR의 명칭 및 우편주소

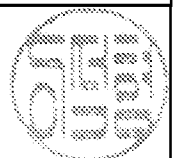
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-472-7140

심사관

이석형

전화번호 +82-42-481-5983



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2008-0033686 A	2008/04/17	US 2008-0089256 A1 US 7907556 B2	2008/04/17 2011/03/15
KR 10-2008-0111374 A	2008/12/23	CA 2666573 A1 CA 2666573 C CA 2667571 A1 CA 2702054 A1 CN 101558589 A CN 101558643 A CN 101558643 B CN 101822009 A CN 101822009 B KR 10-1122200 B1 KR 10-1227029 B1 KR 10-2008-0100753 A KR 10-2008-0101616 A KR 10-2009-0036499 A KR 10-2010-0123808 A KR 10-2010-0123809 A KR 10-2010-0123810 A US 2008-0285556 A1 US 2008-0285679 A1 US 2008-0313678 A1 US 2009-0092092 A1 US 2009-0296624 A1 US 7983251 B2 US 8275002 B2 WO 2008-140261 A2 WO 2008-140261 A3 WO 2008-140263 A1 WO 2008-143435 A1 WO 2008-156257 A2 WO 2008-156257 A3 WO 2009-048208 A1	2008/11/20 2013/01/29 2008/11/20 2009/04/16 2009/10/14 2009/10/14 2013/04/24 2010/09/01 2013/01/09 2012/06/12 2013/01/28 2008/11/19 2008/11/21 2009/04/14 2010/11/25 2010/11/25 2010/11/25 2008/11/20 2008/11/20 2008/12/18 2009/04/09 2009/12/03 2011/07/19 2012/09/25 2008/11/20 2008/12/31 2008/11/20 2008/11/27 2008/12/24 2009/03/12 2009/04/16
KR 10-2004-0041120 A	2004/05/14	없음	
KR 10-2005-0040961 A	2005/05/04	없음	