(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0009969
(43) 공개일자 2016년01월27일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04W 8/18* (2009.01)
H04W 88/18 (2009.01)
(21) 출원번호 10-2014-0090591
(22) 출원일자 2014년07월17일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
박종한
서울특별시 구로구 고척로16가길 7-9 2층 (오류동)
이덕기
서울특별시 서초구 신반포로 32 주공아파트 56동 505호 (반포본동)
(뒷면에 계속)
(74) 대리인
윤동열

전체 청구항 수 : 총 22 항

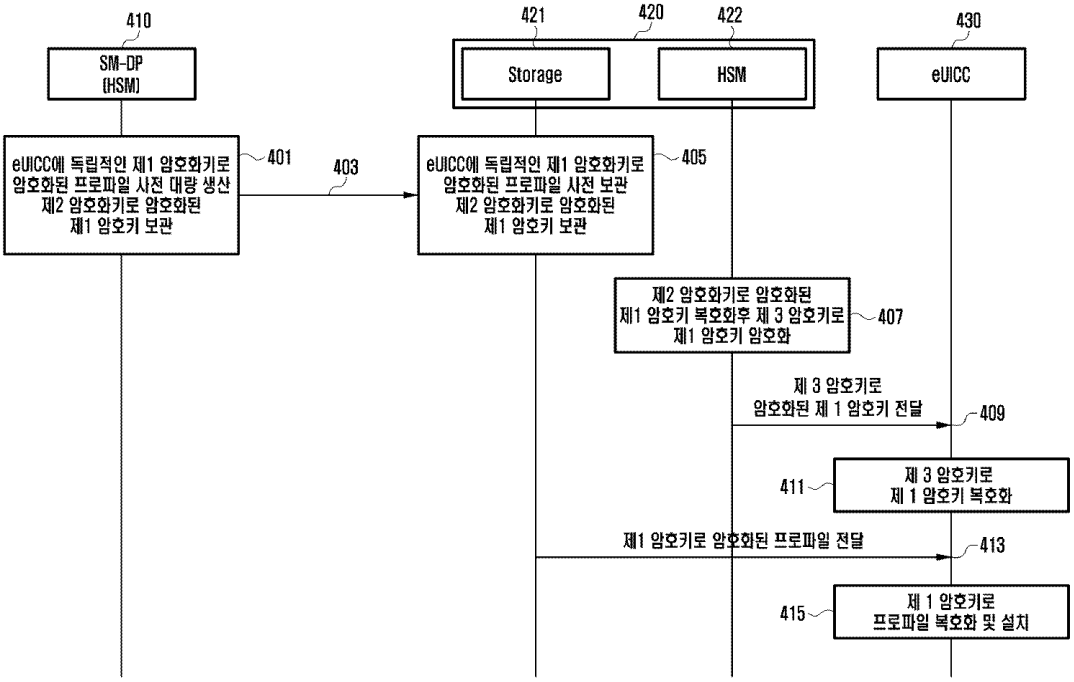
(54) 발명의 명칭 **eUICC의 프로파일 설치 방법 및 장치**

(57) 요 약

본 발명은 eUICC(embedded Universal Integrated Circuit Card)의 프로파일 설치 방법 및 장치에 관한 것으로, 더욱 상세하게는, UICC(Universal Integrated Circuit Card)를 대체하여 단말기 내부에 착탈이 불가능하게끔 내장이 되는 보안모듈에 이동통신 가입자 정보(프로파일)를 원격으로 설치하는 방법 및 장치에 관한 것이다.

(뒷면에 계속)

대 표 도



이에 따른 본 발명은, 네트워크 장치의 eUICC(embedded Universal Integrated Circuit Card)를 위한 프로파일 설치 방법에 있어서, 제1 암호 키로 암호화된 적어도 하나의 프로파일 및 제2 암호 키로 암호화된 적어도 하나의 제1 암호 키 중 적어도 하나를 획득하는 단계 및 상기 eUICC를 위한 프로파일 설치가 개시되면, 상기 암호화된 적어도 하나의 프로파일 및 상기 암호화된 적어도 하나의 제1 암호 키를 적어도 하나의 eUICC로 전달하는 단계를 포함하되, 상기 제1 암호 키는 제3 암호 키로 재암호화되어 상기 적어도 하나의 eUICC로 전달되고, 상기 암호화된 프로파일은 상기 제1 암호 키로 복호하되어 상기 적어도 하나의 eUICC에 각각 설치되는 것을 특징으로 하는 프로파일 설치 방법 및 장치에 관한 것이다.

(72) 발명자

조성연

서울특별시 동작구 여의대방로10길 14 경남교수아파트 103동 1704호 (신대방동)

이상수

경기도 용인시 기흥구 흥덕2로 126 흥덕마을7단지 흥덕힐스테이트아파트 703동 904호

명 세 서

청구범위

청구항 1

네트워크 장치의 eUICC(embedded Universal Integrated Circuit Card)를 위한 프로파일 설치 방법에 있어서,

암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 프로파일을 각각 암호화하는 적어도 하나의 제1 암호 키 중 적어도 하나를 획득하는 단계; 및

상기 eUICC를 위한 프로파일 설치가 개시되면, 상기 암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키를 적어도 하나의 eUICC로 전달하는 단계를 포함하되,

상기 적어도 하나의 제1 암호 키는 제3 암호 키로 암호화되어 상기 적어도 하나의 eUICC로 전달되고, 상기 적어도 하나의 암호화된 프로파일은 상기 적어도 하나의 제1 암호 키로 복호화되어 상기 적어도 하나의 eUICC에 각각 설치되는 것을 특징으로 하는 프로파일 설치 방법.

청구항 2

제1항에 있어서, 상기 획득하는 단계는,

프로파일 제공 서버(Subscription Manager Data Preparation; SM-DP)로부터 상기 적어도 하나의 제1 암호 키로 각각 암호화된 적어도 하나의 프로파일 및 제2 암호 키로 암호화된 상기 적어도 하나의 제1 암호 키를 수신하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 3

제2항에 있어서, 상기 전달하는 단계는,

상기 제2 암호 키로 암호화된 상기 적어도 하나의 제1 암호 키를 복호화하는 단계;

상기 제3 암호 키로 상기 복호화된 적어도 하나의 제1 암호 키를 암호화하는 단계; 및

상기 제3 암호 키로 암호화된 상기 적어도 하나의 제1 암호 키 및 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일을 상기 eUICC로 전달하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 4

제1항에 있어서, 상기 획득하는 단계는,

SM-DP로부터 제2 암호 키로 암호화된 적어도 하나의 프로파일을 수신하는 단계;

상기 제2 암호 키로 암호화된 적어도 하나의 프로파일을 복호화하는 단계;

상기 적어도 하나의 제1 암호 키를 생성하는 단계; 및

상기 복호화된 적어도 하나의 프로파일을 상기 적어도 하나의 제1 암호 키로 각각 암호화하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 5

제4항에 있어서, 상기 전달하는 단계는,

상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키를 SM-DP로 전달하는 단계를 포함하되,

상기 적어도 하나의 제1 암호 키는 상기 SM-DP에 의하여 상기 제3 암호 키로 암호화되어 상기 적어도 하나의 eUICC로 전달되는 것을 특징으로 하는 프로파일 설치 방법.

청구항 6

제5항에 있어서, 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일은,

APDU(Application Protocol Data Unit) 형태로 상기 적어도 하나의 eUICC에 전달되는 것을 특징으로 하는 프로파일 설치 방법.

청구항 7

제1항에 있어서, 상기 획득하는 단계는,

SM-DP로부터 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일을 수신하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 8

제7항에 있어서, 상기 전달하는 단계는,

프로파일을 설치할 eUICC 목록을 상기 SM-DP로 전송하는 단계; 및

상기 SM-DP로부터 상기 제3 암호키로 암호화된 상기 적어도 하나의 제1 암호 키를 수신하는 단계;

상기 제3 암호키로 암호화된 상기 적어도 하나의 제1 암호 키 및 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일을 상기 eUICC 목록에 포함된 상기 적어도 하나의 eUICC로 전송하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 9

제1항에 있어서, 상기 적어도 하나의 제1 암호키는,

적어도 하나의 프로파일에 각각 대응되며 상기 적어도 하나의 프로파일을 각각 암호화하기 위하여 생성되는 랜덤 키인 것을 특징으로 하는 프로파일 설치 방법.

청구항 10

제1항에 있어서, 상기 제3 암호 키는,

상기 적어도 하나의 eUICC에 각각 대응되며 상기 적어도 하나의 제1 암호 키를 각각 암호화하기 위하여 생성되는 세션 키인 것을 특징으로 하는 프로파일 설치 방법.

청구항 11

프로파일 제공 서버(Subscription Manager Data Preparation; SM-DP)의 eUICC(embedded Universal Integrated Circuit Card)를 위한 프로파일 설치 방법에 있어서,

암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 프로파일을 각각 암호화하는 적어도 하나의 제1 암호 키 중 적어도 하나를 네트워크 장치로 전송하는 단계를 포함하되,

상기 암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키는, 상기 eUICC를 위한 프로파일 설치가 개시되면, 적어도 하나의 eUICC로 전달되고,

상기 적어도 하나의 제1 암호 키는 제3 암호 키로 암호화되어 상기 적어도 하나의 eUICC로 전달되고, 상기 적어도 하나의 암호화된 프로파일은 상기 적어도 하나의 제1 암호 키로 복호화되어 상기 적어도 하나의 eUICC에 각각 설치되는 것을 특징으로 하는 프로파일 설치 방법.

청구항 12

제11항에 있어서, 상기 전송하는 단계는,

상기 적어도 하나의 제1 암호 키로 각각 암호화된 적어도 하나의 프로파일 및 제2 암호 키로 암호화된 상기 적어도 하나의 제1 암호 키를 상기 네트워크 장치로 전송하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 13

제11항에 있어서, 상기 전송하는 단계는,

제2 암호 키로 암호화된 적어도 하나의 프로파일을 상기 네트워크 장치로 전송하는 단계를 포함하고,

상기 네트워크 장치로부터 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키를 수신하는 단계; 및

상기 적어도 하나의 제1 암호 키를 상기 제3 암호 키로 암호화하여 상기 적어도 하나의 eUICC로 전송하는 단계를 더 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 14

제11항에 있어서, 상기 전송하는 단계는,

상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일을 상기 적어도 하나의 eUICC로 전송하는 단계를 더 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 15

eUICC(embedded Universal Integrated Circuit Card)를 위한 프로파일을 설치하는 네트워크 장치로,

데이터 통신을 수행하는 통신부;

암호화 및 복호화를 수행하는 암호화 장치; 및

암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 프로파일을 각각 암호화하는 적어도 하나의 제1 암호 키 중 적어도 하나를 획득하는 저장 장치를 포함하되,

상기 통신부는,

상기 eUICC를 위한 프로파일 설치가 개시되면, 상기 암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키를 적어도 하나의 eUICC로 전달하고,

상기 암호화 장치는,

상기 적어도 하나의 제1 암호 키를 제3 암호 키로 암호화하여 상기 적어도 하나의 eUICC로 전달하고,

상기 적어도 하나의 암호화된 프로파일은,

상기 적어도 하나의 제1 암호 키로 복호화되어 상기 적어도 하나의 eUICC에 각각 설치되는 것을 특징으로 하는 네트워크 장치.

청구항 16

제15항에 있어서, 상기 저장 장치는,

프로파일 제공 서버(Subscription Manager Data Preparation; SM-DP)로부터 상기 적어도 하나의 제1 암호 키로 각각 암호화된 적어도 하나의 프로파일 및 제2 암호 키로 암호화된 상기 적어도 하나의 제1 암호 키를 수신하고,

상기 암호화 장치는,

상기 제2 암호 키로 암호화된 상기 적어도 하나의 제1 암호 키를 복호화하고, 상기 제3 암호 키로 상기 복호화된 적어도 하나의 제1 암호 키를 암호화하고, 상기 제3 암호 키로 암호화된 상기 적어도 하나의 제1 암호 키 및 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일을 상기 eUICC로 전달하는 것을 특징으로 하는 네트워크 장치.

청구항 17

제15항에 있어서, 상기 저장 장치는,

SM-DP로부터 제2 암호 키로 암호화된 적어도 하나의 프로파일을 수신하고,

상기 암호화 장치는,

상기 제2 암호 키로 암호화된 적어도 하나의 프로파일을 복호화하고, 상기 적어도 하나의 제1 암호 키를 생성하고, 상기 복호화된 적어도 하나의 프로파일을 상기 적어도 하나의 제1 암호 키로 각각 암호화하고, 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키를 SM-DP로 전달하되,

상기 적어도 하나의 제1 암호 키는 상기 SM-DP에 의하여 상기 제3 암호 키로 암호화되어 상기 적어도 하나의 eUICC로 전달되는 것을 특징으로 하는 네트워크 장치.

청구항 18

제15항에 있어서, 상기 네트워크 장치는,

SM-DP로부터 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일을 수신하고, 프로파일을 설치할 eUICC 목록을 상기 SM-DP로 전송하고, 상기 SM-DP로부터 상기 제3 암호키로 암호화된 상기 적어도 하나의 제1 암호 키를 수신하고, 상기 제3 암호키로 암호화된 상기 적어도 하나의 제1 암호 키 및 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일을 상기 eUICC 목록에 포함된 상기 적어도 하나의 eUICC로 전송하는 것을 특징으로 하는 네트워크 장치.

청구항 19

eUICC(embedded Universal Integrated Circuit Card)를 위한 프로파일을 설치하는 프로파일 제공 서버(Subscription Manager Data Preparation; SM-DP)로,

데이터 통신을 수행하는 통신부; 및

암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 프로파일을 각각 암호화하는 적어도 하나의 제1 암호 키 중 적어도 하나를 네트워크 장치로 전송하도록 제어하는 제어부를 포함하되,

상기 암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키는, 상기 eUICC를 위한 프로파일 설치가 개시되면, 적어도 하나의 eUICC로 전달되고,

상기 적어도 하나의 제1 암호 키는 제3 암호 키로 암호화되어 상기 적어도 하나의 eUICC로 전달되고, 상기 적어도 하나의 암호화된 프로파일은 상기 적어도 하나의 제1 암호 키로 복호화되어 상기 적어도 하나의 eUICC에 각각 설치되는 것을 특징으로 하는 SM-DP.

청구항 20

제19항에 있어서, 상기 제어부는,

상기 적어도 하나의 제1 암호 키로 각각 암호화된 적어도 하나의 프로파일 및 제2 암호 키로 암호화된 상기 적어도 하나의 제1 암호 키를 상기 네트워크 장치로 전송하는 것을 특징으로 하는 SM-DP.

청구항 21

제19항에 있어서, 상기 제어부는,

제2 암호 키로 암호화된 적어도 하나의 프로파일을 상기 네트워크 장치로 전송하고, 상기 네트워크 장치로부터 상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키를 수신하고, 상기 적어도 하나의 제1 암호 키를 상기 제3 암호 키로 암호화하여 상기 적어도 하나의 eUICC로 전송하는 것을 특징으로 하는 SM-DP.

청구항 22

제19항에 있어서, 상기 제어부는,

상기 적어도 하나의 제1 암호 키로 각각 암호화된 상기 적어도 하나의 프로파일을 상기 적어도 하나의 eUICC로 전송하는 것을 특징으로 하는 SM-DP.

발명의 설명

기 술 분 야

[0001] 본 발명은 eUICC(embedded Universal Integrated Circuit Card)의 프로파일 설치 방법 및 장치에 관한 것으로, 더욱 상세하게는, UICC(Universal Integrated Circuit Card)를 대체하여 단말기 내부에 착탈이 불가능하게끔 내장이 되는 보안모듈에 이동통신 가입자 정보(프로파일)를 원격으로 설치하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] UICC(Universal Integrated Circuit Card)는 이동통신 단말기에 삽입하여 사용하는 스마트카드로서 이동통신 가입자의 네트워크 접속 인증 정보, 전화번호부, SMS와 같은 개인정보가 저장된다. UICC는 GSM, WCDMA, LTE 등과 같은 이동통신 네트워크에 접속 시 가입자 인증 및 트래픽 보안 키 생성을 수행하여 안전한 이동통신 이용을 가능케 한다.

[0003] UICC에는 가입자가 접속하는 이동통신 네트워크의 종류에 따라 SIM, USIM, ISIM 등의 통신 어플리케이션이 탑재된다. 또한 UICC는 전자지갑, 티켓팅, 전자여권 등과 같은 다양한 응용 어플리케이션의 탑재를 위한 상위 레벨의 보안 기능을 제공한다.

[0004] 종래의 UICC는 카드 제조 시 특정 이동통신 사업자의 요청에 의해 해당 사업자를 위한 전용 카드로 제조되었다. 이에 따라, UICC는 해당 사업자의 네트워크 접속을 위한 인증 정보(예: USIM 어플리케이션 및 IMSI, Ki 값)가 사전 탑재되어 출고된다. 제조된 UICC 카드는 해당 이동통신 사업자가 납품 받아 가입자에게 제공하며, 필요한 경우, OTA(Over The Air) 등의 기술을 활용하여 UICC 내 어플리케이션의 설치, 수정, 삭제 등의 관리를 수행한다. 가입자는 소유한 이동통신 단말기에 UICC 카드를 삽입하여 해당 이동통신 사업자의 네트워크 및 응용 서비스를 이용할 수 있으며, 단말기 교체 시에는 UICC 카드를 기존 단말기에서 새로운 단말기로 이동 삽입함으로써 해당 UICC 카드에 저장된 인증정보, 이동통신 전화번호, 개인 전화번호부 등을 새로운 단말기에서 그대로 사용할 수 있다.

[0005] UICC 카드는 ETSI(European Telecommunications Standards Institute)라는 표준화 단체에서 그 물리적 형상 및 논리적 기능을 정의하여 국제적인 호환성을 유지하고 있다. 물리적 형상을 정의하는 Form Factor 측면을 살펴보면, UICC 카드는 가장 광범위하게 사용되고 있는 Mini SIM으로부터, 몇 년 전부터 사용되기 시작한 Micro SIM, 그리고 최근에 등장한 Nano SIM에 이르기까지 점점 그 크기가 작아지고 있다. 이는 이동통신 단말기의 소형화에 많은 기여를 하고 있다.

[0006] 최근에는 Nano SIM보다 더 작은 크기의 UICC카드가 제정되고 있으나, 이는 사용자의 분실 우려로 인해 표준화되기 힘들 것으로 예상되며, 착탈형 UICC 카드의 특성상 단말기에 추가로 착탈 슬롯을 장착하기 위한 공간이 필요하므로 더 이상의 소형화가 힘들 것으로 예상되고 있다.

[0007] 또한 지능형 가전제품, 전기/수도 미터기, CCTV 카메라 등 다양한 설치 환경에서 사람의 직접적인 조작 없이 이동통신 데이터망 접속을 수행하는 M2M(Machine-to-Machine) 기기에는 착탈형 UICC 카드가 적합하지 않은 상황이다.

[0008] 이러한 문제점을 해결하기 위해, UICC와 유사한 기능을 수행하는 보안 모듈을 이동통신 단말기 제조 시 단말기에 내장하여, 종래의 착탈식 UICC를 대체하기 위한 요구사항이 대두되고 있다.

[0009] 이러한 요구에 따라 등장한 단말 내장 보안 모듈은 단말기 제조 시 단말기 내부에 장착되는 보안 모듈로써, 착탈이 불가능하기 때문에 단말기 제조 시 USIM의 IMSI, K와 같은 특정 이동통신 사업자의 네트워크 접속인증 정보를 사전 탑재할 수 없다. 이에 따라 단말 내장 보안 모듈은 해당 단말 내장 보안 모듈이 탑재된 단말을 구입한 사용자가 특정 이동통신 사업자에 가입을 한 이후에, 인증정보를 설정할 수 있다.

[0010] 새롭게 도입된 단말 내장 보안 모듈을 지원하는 네트워크에서, 단말이 프로비저닝 프로파일을 이용하여 임의의 이동통신 망에 접속하는 경우, 프로파일 제공 서버는 실시간으로 단말과 상호인증을 하여 생성된 세션 키를 이용하여 프로파일을 암호화하고, 암호화된 프로파일을 단말로 전송한다. 프로파일 암호화를 위해 프로파일 제공 서버에 구비되는 하드웨어 보안 모듈은 실시간으로 소량의 프로파일을 암호화하는데에는 적합할 수 있지만, 대량의 단말이 단말 내장 보안 모듈을 위한 프로파일을 제공받고자 하는 경우 전체 프로파일에 대한 실시간 암호화를 거쳐야 하므로 프로파일 제공이 불가능할 수 있다. 따라서, 대량의 단말 내장 보안 모듈 탑재 단말에 대하여 프로파일 프로비저닝을 수행하는 경우, 기술적 어려움이 따를 수 있다.

[0011] 또한, 대량의 단말에게 단말 내장 보안 모듈을 위한 프로파일을 제공하는 경우, 단말과 SM-DP(Subscription

Manager Data Preparation)를 연결하는 외부 네트워크 상태가 열악하다면 일부 단말에게 올바르게 프로파일을 제공할 수 없는 문제가 발생할 수 있다.

[0012] 따라서, 외부 네트워크의 연동 없이 단말 내장 보안 모듈을 위한 프로파일을 프로비저닝하고, 사전에 대량의 단말들을 위한 프로파일을 미리 암호화하여 보관할 수 있는 방법이 요구된다.

발명의 내용

해결하려는 과제

[0013] 본 발명은 상기와 같은 문제점을 해결하기 위한 것으로, 단말에게 프로파일을 제공할 때, 외부 네트워크 연동없이 프로파일 프로비저닝을 수행할 수 있는 방법 및 장치를 제공한다.

[0014] 또한, 본 발명은 프로파일 프로비저닝 이전에 미리 대량의 프로파일 및 이를 암호화한 암호키를 암호화하여 보관하였다가, 단말의 프로파일 프로비저닝 수행 시, 암호화된 프로파일 관련 정보를 단말에게 제공하는 방법 및 장치를 제공한다.

과제의 해결 수단

[0015] 상기와 같은 목적을 달성하기 위한 본 발명의 네트워크 장치의 eUICC(embedded Universal Integrated Circuit Card)를 위한 프로파일 설치 방법은, 제1 암호 키로 암호화된 적어도 하나의 프로파일 및 제2 암호 키로 암호화된 적어도 하나의 제1 암호 키 중 적어도 하나를 획득하는 단계 및 상기 eUICC를 위한 프로파일 설치가 개시되면, 상기 암호화된 적어도 하나의 프로파일 및 상기 암호화된 적어도 하나의 제1 암호 키를 적어도 하나의 eUICC로 전달하는 단계를 포함하되, 상기 제1 암호 키는 제3 암호 키로 재암호화되어 상기 적어도 하나의 eUICC로 전달되고, 상기 암호화된 프로파일은 상기 제1 암호 키로 복호하되어 상기 적어도 하나의 eUICC에 각각 설치되는 것을 특징으로 한다.

[0016] 상기한 제 1 암호키, 제 2 암호키, 제 3 암호키는 각각 하나 또는 복수개의 정보로 이루어 질수 있다. 예를 들면, 제1 암호 키, 제2 암호 키, 제3 암호 키는 하나 이상의 키 정보를 합친 암호키 세트일 수도 있다. 또한 개별 암호키는 SCP 80키 이거나 SCP 81키 이거나, SCP 03키일 수 있으며, 비대칭키일 수 있다. 비대칭키의 예로 RSA 기반의 인증서, 인증서에 평문으로 포함되어 있는 공개키 및 공개키와 쌍으로 생성되어 인증서를 소유한 엔티티에 안전하게 보관되는 개인키를 들 수 있다. 이후 설명하는 과정에서 인증서를 이용하여 암호화하는 것은, 암호화 내용을 수신할 엔티티의 인증서에 포함된 공개키로 암호화하여 전송하는 것을 의미하며, 이를 수신한 엔티티는 내부에 보관된 상기한 개인키를 이용하여 복호화를 수행할 수 있다.

[0017] 또한, 본 발명의 프로파일 제공 서버(Subscription Manager Data Preparation; SM-DP)의 eUICC(embedded Universal Integrated Circuit Card)를 위한 프로파일 설치 방법은, 암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 프로파일을 각각 암호화하는 적어도 하나의 제1 암호 키 중 적어도 하나를 네트워크 장치로 전송하는 단계를 포함하되, 상기 암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키는, 상기 eUICC를 위한 프로파일 설치가 개시되면, 적어도 하나의 eUICC로 전달되고, 상기 적어도 하나의 제1 암호 키는 제3 암호 키로 암호화되어 상기 적어도 하나의 eUICC로 전달되고, 상기 적어도 하나의 암호화된 프로파일은 상기 적어도 하나의 제1 암호 키로 복호화되어 상기 적어도 하나의 eUICC에 각각 설치되는 것을 특징으로 한다.

[0018] 또한, 본 발명의 eUICC(embedded Universal Integrated Circuit Card)를 위한 프로파일을 설치하는 네트워크 장치는, 데이터 통신을 수행하는 통신부; 암호화 및 복호화를 수행하는 암호화 장치; 및 암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 프로파일을 각각 암호화하는 적어도 하나의 제1 암호 키 중 적어도 하나를 획득하는 저장 장치를 포함하되, 상기 통신부는, 상기 eUICC를 위한 프로파일 설치가 개시되면, 상기 암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 제1 암호 키를 적어도 하나의 eUICC로 전달하고, 상기 암호화 장치는, 상기 적어도 하나의 제1 암호 키를 제3 암호 키로 암호화하여 상기 적어도 하나의 eUICC로 전달하고, 상기 적어도 하나의 암호화된 프로파일은, 상기 적어도 하나의 제1 암호 키로 복호화되어 상기 적어도 하나의 eUICC에 각각 설치되는 것을 특징으로 한다.

[0019] 또한, 본 발명의 eUICC(embedded Universal Integrated Circuit Card)를 위한 프로파일을 설치하는 프로파일 제공 서버(Subscription Manager Data Preparation; SM-DP)는, 데이터 통신을 수행하는 통신부; 및 암호화된 적어도 하나의 프로파일 및 상기 적어도 하나의 프로파일을 각각 암호화하는 적어도 하나의 제1 암호 키 중 적어도 하나를 네트워크 장치로 전송하도록 제어하는 제어부를 포함하되, 상기 암호화된 적어도 하나의 프로파일

및 상기 적어도 하나의 제1 암호 키는, 상기 eUICC를 위한 프로파일 설치가 개시되면, 적어도 하나의 eUICC로 전달되고, 상기 적어도 하나의 제1 암호 키는 제3 암호 키로 암호화되어 상기 적어도 하나의 eUICC로 전달되고, 상기 적어도 하나의 암호화된 프로파일은 상기 적어도 하나의 제1 암호 키로 복호화되어 상기 적어도 하나의 eUICC에 각각 설치되는 것을 특징으로 한다.

발명의 효과

[0020] 본 발명의 다양한 실시 예에 따르면, 대량의 단말 내장 보안 모듈 탑재 단말에 대하여 동시에 프로파일을 프로비저닝하는 경우, 성능 열화 또는 데이터 손실 없이 암호화된 프로파일을 제공할 수 있다.

[0021] 또한, 본 발명의 다양한 실시 예에 따르면, 프로파일 제공 서버와 단말을 연결하는 외부 네트워크의 상태가 열악한 경우에도, 대량의 단말을 위하여 프로파일 프로비저닝을 수행할 수 있다.

도면의 간단한 설명

[0022] 도 1은 eUICC를 지원하는 네트워크의 구조를 나타낸 도면이다.

도 2는 eUICC를 위한 프로파일 설치 방법을 나타낸 흐름도이다.

도 3은 본 발명에 따른 eUICC를 지원하는 네트워크의 구조를 나타낸 도면이다.

도 4는 본 발명의 제1 실시 예에 따른 eUICC를 위한 프로파일 설치 방법을 나타낸 흐름도이다.

도 5는 본 발명의 제2 실시 예에 따른 eUICC를 위한 프로파일 설치 방법을 나타낸 흐름도이다.

도 6은 본 발명의 제3 실시 예에 따른 eUICC를 위한 프로파일 설치 방법을 나타낸 흐름도이다.

도 7은 본 발명의 실시 예에 따른 장치들의 구조를 나타낸 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 발명은 단말 내장 보안 모듈을 장착한 단말로써, 스마트 폰(Smart Phone), 휴대 단말(Portable Terminal), 이동 단말(Mobile Terminal), 개인 정보 단말(Personal Digital Assistant: PDA), PMP(Portable Multimedia Player) 단말, 노트북 컴퓨터, 와이브로(Wibro) 단말, 스마트 TV, 스마트 냉장고 등의 일반적인 전자 단말뿐만 아니라, 단말 내장 보안 모듈을 지원하는 모든 장치 또는 서비스를 위하여 적용될 수 있다.

[0024] 본 발명은 단말내장 보안모듈, 프로파일 제공서버, 그리고 단말내장 보안모듈의 프로파일 설치를 지원하는 네트워크 장치로 구성된다.

[0025] 단말 내장 보안 모듈은 eSE(embedded Secure Element)라고 명명되며, 대표적인 예로 eUICC를 들 수 있다. 이하의 실시 예들은 eUICC를 위주로 설명되나, eUICC를 포함한 다양한 종류의 단말 내장 보안 모듈에 본 발명이 적용될 수 있음은 자명하다. 본 명세서에서 용어 eUICC는 eSIM(embedded Subscriber Identity Module)과 혼용될 수 있다.

[0026] 단말내장 보안모듈 내에 설치되는 프로파일은 기존 UICC 카드에 저장되는 하나 또는 복수 개의 어플리케이션 및 가입자 인증정보, 전화번호부 등의 데이터 정보를 총칭한다. 프로파일은 용도에 따라 오퍼레이셔널 프로파일(Operational Profile)과 프로비저닝 프로파일(Provisioning Profile)(또는 부트스트랩 프로파일(Bootstrap Profile))을 포함할 수 있다. 오퍼레이셔널 프로파일은 단말의 사용자가 가입한 이동통신사의 가입정보를 소프트웨어 형태로 패키징한 것을 의미할 수 있다. 프로비저닝 프로파일은 사용자가 특정 통신사에 가입하기 이전에 단말이 임의의 국가의 임의의 이동통신망에 접속하는데 필요한 프로파일로서 사전에 eUICC에 탑재되는 프로파일을 의미할 수 있다. 프로비저닝 프로파일은 오퍼레이셔널 프로파일을 원격으로 다운로드하기 위한 네트워크 접속 환경을 제공하는 용도로만 사용될 수 있으며, 임의의 이동통신망에 접속하는데 필요한 정보로써 IMSI 및 Ki 값 등을 포함할 수 있다.

[0027] 프로파일 제공 서버는 SM-DP(Subscription Manager Data Preparation)로 명명되며, off-card entity of Profile Domain, 프로파일 암호화 서버, 프로파일 생성서버, 프로파일 프로비저너(Profile Provisioner) 또는 프로파일 제공자(Profile Provider) 등과 같은 의미로 사용될 수 있다.

[0028] 단말내장 보안모듈의 프로파일 설치를 지원하는 네트워크 장치는 서버 등의 형태로 구현될 수 있으며, 프로파일의 암호화 및 복호화를 수행하는 암호화 장치 및 적어도 하나의 프로파일을 저장하는 저장 장치 중 적어도 하나

를 포함하여 구성될 수 있다. 네트워크 장치가 암호화 장치와 저장 장치 중 어느 하나만을 포함하여 구성되는 경우, 네트워크 장치는 암호와 장치 또는 저장 장치 그 자체일 수 있다. 또는, 네트워크 장치가 암호화 장치와 저장 장치 모두를 포함하여 구성되는 경우, 네트워크 장치는 암호화 장치와 저장 장치를 포함하는 하나의 장치로써 동작하거나, 별개로 존재하는 암호화 장치와 저장 장치를 통칭하는 개념으로 해석될 수도 있다.

[0029] 암호화 장치는 하드웨어 보안 모듈(Hardware Security Module; HSM)을 포함하거나, HSM 그 자체로 명명될 수 있다.

[0030] 그 외에, 본 명세서에서는 eUICC를 지원하는 네트워크에서 정의되는 다양한 용어들이 사용될 수 있다.

[0031] 예를 들어, 본 명세서에서 사용되는 용어로써, SM-SR(Subscription Manager Secure Routing)은 프로파일 관리 서버로 표현될 수 있으며, 암호화된 프로파일을 OTA로 eUICC에게 전달하는 역할을 수행할 수 있다. SM-SR은 또한 off-card entity of eUICC Profile Manager 또는 Profile Manager로 표현될 수 있다.

[0032] 또한, 본 명세서에서 사용되는 용어로써, eUICC 식별자(eUICC Identifier; EID)는 단말에 내장된 eUICC를 구분하는 고유 식별자로, eUICC에 프로비저닝 프로파일이 미리 탑재되어 있는 경우 해당 프로비저닝 프로파일의 프로파일 ID이거나, 단말과 eUICC(또는 eSIM) 칩이 분리되지 않을 경우 단말 ID일 수 있다. 또한, E-UICC ID는, eSIM칩의 특정 보안 도메인(Secure Domain)을 지칭할 수도 있다.

[0033] 또한, 본 명세서에서 사용되는 용어로써, eUICC 정보 세트(eUICC Information Set; EIS)는 SM-SR에 저장되는 EUICC 관련 정보들로, EID, ICCID 등을 포함할 수 있다.

[0034] 또한, 본 명세서에서 사용되는 용어로써, 기본 파일(Elementary File; EF)는 eUICC 내부 프로파일 내 각종 정보를 저장하는 파일을 의미하는 것으로 IMSI, MSISDN 등을 저장할 수 있다.

[0035] 또한, 본 명세서에서 사용되는 용어로써, MNO(Mobile Network Operator)는 이동통신 사업자 또는 이동통신 사업자 시스템을 의미할 수 있다.

[0036] 또한, 본 명세서에서 사용되는 용어로써, 하드웨어 보안 모듈(Hardware Security Module; HSM)은 암호 키를 노출시키지 않고 암호화, 복호화를 수행하는 하드웨어 보안 모듈을 의미한다.

[0037] 이하의 설명에서 사용되는 특정 용어들은 본 발명의 이해를 돕기 위해서 제공된 것이며, 이러한 특정 용어의 사용은 본 발명의 기술적 사상을 벗어나지 않는 범위에서 다른 형태로 변경될 수 있다.

[0038] 본 명세서에서 사용되는 기술적 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명의 사상을 한정하려는 의도가 아님을 유의해야 한다. 또한, 본 명세서에서 사용되는 기술적 용어는 본 명세서에서 특별히 다른 의미로 정의되지 않는 한, 본 발명이 속하는 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 의미로 해석되어야 하며, 과도하게 포괄적인 의미로 해석되거나, 과도하게 축소된 의미로 해석되지 않아야 한다.

[0039] 또한, 본 명세서에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "구성된다." 또는 "포함한다." 등의 용어는 명세서상에 기재된 여러 구성 요소들, 또는 여러 단계를 반드시 모두 포함하는 것으로 해석되지 않아야 한다.

[0040] 이하 본 발명의 바람직한 실시 예를 첨부된 도면을 참조하여 설명한다. 그리고, 본 발명을 설명함에 있어서, 관련된 공지기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단된 경우 그 상세한 설명은 생략할 것이다. 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0041] 도 1은 eUICC를 지원하는 네트워크의 구조를 나타낸 도면이다.

[0042] 도 1을 참조하면, eUICC를 지원하는 네트워크는 단말(100), SM 서버(110) 및 MNO(120)를 포함하여 구성될 수 있다. SM 서버(110)는 SM-SR(111) 및 SM-DP(112)로 구성될 수 있다.

[0043] 단말(100)은 단말에 실장된 보안 모듈로써, eUICC(102)를 포함하여 구성된다. eUICC는 고유의 식별자로 EID를 가질 수 있으며, 단말(100)에는 물리적으로 또는 소프트웨어 적으로 EID가 표기될 수 있다.

[0044] 단말(100)은 제어부(101)의 제어에 따라 eUICC(102)에 저장된 적어도 하나의 프로파일을 이용하여 프로파일에

대응하는 이동통신 망에 접속하여 데이터 통신을 수행한다. 특히, eUICC(102)에는 단말(100)이 실질적으로 사용할 프로파일을 다운로드 및 설치하기 위하여 임시로 망에 접속하는데 이용되는 프로비저닝 프로파일이 저장될 수 있다.

[0045] 단말(100)은 프로파일 설치 이벤트가 트리거링됨에 따라 프로파일 설치 동작을 수행할 수 있다. 구체적으로, 단말(100)은 SM-SR(111)로 EID를 포함하는 프로파일 요청을 전송하고, SM-SR(111)과의 인증 과정을 거쳐, SM-DP(112)와 사전 공유된 세션 키로 암호화된 프로파일을 수신한다. 단말(100)은 세션 키로 프로파일을 복호화하여 이동통신 망 접속에 사용한다.

[0046] 다양한 실시 예에서, 단말(100)은 디지털 인증 방식을 이용하여 SM-DP(112)와 세션 키를 공유할 수 있다. 예를 들어, 단말(100)은 SM-SR(111)을 통하여 SM-DP(112)로부터 자신의 eUICC(112)에 대응하는 디지털 인증서를 수신하고, 수신된 디지털 인증서를 이용하여 세션 키를 생성한 후, 이를 암호화하여 SM-DP(112)로 전송할 수 있다. SM-DP(112)는 디지털 인증서를 이용하여 수신된 세션 키를 복호화한 후, 해당 디지털 인증서에 대응하는 eUICC(112)를 위한 프로파일을 해당 세션 키로 암호화하여 단말(100)에게 전송할 수 있다. 디지털 인증 방식을 이용하는 경우에, SM-DP(112)는 디지털 인증서를 이용하여 생성된 공개 키(public key)를 이용하여 프로파일을 암호화하고, 단말(100)은 디지털 인증서를 이용하여 생성된 비밀 키(private key)를 이용하여 프로파일을 복호화할 수 있다. 상기에서는 세션 키 공유 방법으로 디지털 인증서를 이용하는 방법을 예로 들었으나, 이에 한정되지 않고 다양한 인증 알고리즘을 SM-DP(112)와 단말(100)이 공유하는 방식이 사용될 수 있다.

[0047] SM-SR(111)은 복수의 단말을 위한 프로파일에 관한 정보를 관리한다. SM-SR(111)은 프로파일 설치 이벤트가 트리거링됨에 따라 eUICC(102)의 MSISDN으로 프로파일 다운로드를 위한 SMS를 전송할 수 있다. 다양한 실시 예에서, SM-SR(111)은 암호화된 세션 키 또는 암호화된 프로파일 등을 SM-DP(112) 및 단말(100) 간 전달하는 기능을 수행할 수 있다. SM-SR(111)은 검증된 OTA 기술을 이용하여 단말(100)과 데이터를 송수신할 수 있다. 즉, SM-SR(111)은 OTA Key를 이용하여 단말(100)에게 송신할 데이터를 암호화하여 전송할 수 있다. SM-SR(111)은 eUICC(102)내에서 프로파일의 복호화 및 설치가 완료된 이후에는 프로파일의 활성화, 비활성화, 제거 등의 프로파일 관리 역할을 수행할 수 있다.

[0048] SM-DP(112)는 단말(100)에 실장되는 eUICC(102)를 위한 프로파일을 생성하고 세션 키를 이용하여 이를 암호화한다. SM-DP(112)는 임의의 eUICC(102)로부터 프로파일 설치 요청이 수신되면, 해당 eUICC(102)와 사전 공유된 세션 키로 프로파일을 암호화하여 전송할 수 있다. 또는, SM-DP(112)는 단말(100)로부터 검증된 세션 키가 수신되면, 해당 세션 키로 암호화된 프로파일을 단말(100)로 전송한다. SM-DP(112)는 MNO(120)에 의해 직접 운영되거나 MNO(120)와 완전한 신뢰 관계에 있는 다른 업체에 의해 운영될 수 있다. 비즈니스 및 계약 관계에 따라, SM-DP(112)는 하나 또는 복수 개의 MNO(120)를 위한 서비스를 제공할 수도 있다.

[0049] 네트워크에는 적어도 하나의 MNO(120)가 존재할 수 있다. MNO(120)는 단말(100)에 통신 서비스를 제공한다. MNO(120)는 SM-DP(112)를 운영할 수 있으며, 단말(100) 사용자가 서비스 가입을 신청하면, SM-DP(112)를 이용하여, 단말(100)의 프로파일 설치를 도울 수 있다. 적어도 하나의 MNO(120) 각각은 별개의 SM-DP(112)를 운영할 수 있다. 또는, 신뢰할 수 있는 계약 관계에 의해 하나의 SM-DP(112)가 복수의 MNO(120)를 위한 서비스를 제공할 수 있다.

[0050] 이하에서는, 도 1에 도시된 네트워크에서 eUICC를 위한 프로파일 설치 방법을 설명한다.

[0051] 도 2는 eUICC를 위한 프로파일 설치 방법을 나타낸 흐름도이다. 도 2에서는 SM-DP(230)와 eUICC(210) 간 데이터를 전달하는 SM-SR(220)의 데이터 흐름은 도시하지 않았으나, SM-SR(220)은 SM-DP(230)로부터 암호화된 프로파일 및 세션 키를 구성할 수 있는 전체 혹은 부분 정보를 eUICC(210)로 전달하거나, eUICC(210)로부터 암호화된 세션키를 구성할 수 있는 전체 혹은 부분에 관한 정보를 SM-DP(230)로 전달할 수 있다.

[0052] 도 2를 참조하면, eUICC(210)와 SM-DP(230)는 개별 eUICC 인증 및 세션 키 생성 과정을 수행한다(201).

[0053] 구체적으로, SM-DP(230)는 EID를 통해 구분되는 각각의 eUICC(210) 별로 인증을 통해 세션키를 생성하고 생성된 세션키를 이용하여 암호화한 프로파일을 생성한다. 이러한 실시간 인증과정을 거쳐 eUICC(210)도 세션키를 획득하게 되고, eUICC(210)는 획득한 세션 키를 이용하여 SM-DP(230)가 전달한 암호화된 프로파일을 복호화 할 수 있다.

[0054] SM-DP(230)는 각각의 eUICC(210)를 위한 프로파일을 각각의 eUICC(210)에 대응하는 세션 키로 암호화하여

(203), eUICC(210)로 전달한다(205). eUICC(210)는 실시간 인증과정에서 생성된 세션 키로 프로파일을 복호화하여 설치한다. 각각의 세션 키는 각각의 eUICC(210)에 1:1로 대응되기 때문에, 각각의 세션 키로 암호화된 프로파일은 세션 키에 대응하는 특정 eUICC(210)만 복호화할 수 있다.

[0055] 상기한 과정은 eUICC(210)가 실질적으로 프로파일 설치를 시작할 때 수행되며, 각각의 eUICC(210)에 대하여 개별적으로 진행된다. SM-DP(230)는 프로파일 암호화를 위한 별도의 암호화 모듈을 구비할 수 있는데, 암호화 모듈에서 암호화를 수행하는 데에는 일정한 시간이 소모되므로, 대량의 eUICC(210)가 동시에 프로파일 설치를 요청하는 경우에는 프로파일 설치가 올바르게 진행될 수 없다. 또한, 프로파일 설치를 개별적으로 수행하는 도중에 네트워크의 단절로 프로파일 설치가 중단되면, 모든 eUICC(210)를 위하여 올바르게 프로파일을 설치할 수 없는 문제가 발생할 수 있다.

[0056] 따라서, eUICC(210)의 프로파일 설치의 개시 이전에, SM-DP(230)에서 대량의 단말(210)을 위해 미리 암호화된 프로파일을 보관하였다가, 실질적으로 프로파일 설치가 개시될 때 이를 단말(210)로 전달함으로써 효율적으로 프로파일을 설치할 수 있는 방법이 요구된다. 또한, eUICC(210)의 프로파일 설치 시, SM-DP(230)가 존재하는 외부 네트워크와 독립적으로 프로파일을 다운로드할 수 있는 방법이 요구된다.

[0057] 이하에서는, 상기한 기술적 특징을 제공할 수 있는 본 발명에 따른 프로파일 설치 방법을 설명한다.

[0058] 도 3은 본 발명에 따른 eUICC를 지원하는 네트워크의 구조를 나타낸 도면이다.

[0059] 도 3을 참조하면, 본 발명에 따른 eUICC를 지원하는 네트워크는 eUICC의 프로파일 설치를 지원하는 네트워크 장치(330)를 포함하여 구성된다.

[0060] 네트워크 장치(330)는 프로파일을 암호화 및 복호화를 수행하는 암호화 장치(331) 및 적어도 하나의 프로파일을 저장하는 저장 장치(332) 중 적어도 하나를 포함하여 구성될 수 있다.

[0061] 암호화 장치(331)는 HSM을 포함하거나 HSM 그 자체로 명명될 수 있으며, 암호 키를 노출시키지 않고 프로파일의 암호화 및 복호화를 수행할 수 있다.

[0062] 저장 장치(332)는 적어도 하나의 프로파일을 저장한다. 저장 장치(332)는 하드디스크 타입(hard disk type), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다.

[0063] 네트워크 장치(330)가 암호화 장치(331)와 저장 장치(332) 중 어느 하나만을 포함하여 구성되는 경우, 네트워크 장치(330)는 암호와 장치(331) 또는 저장 장치(332) 그 자체일 수 있다. 또는, 네트워크 장치(330)가 암호화 장치(331)와 저장 장치(332) 모두를 포함하여 구성되는 경우, 네트워크 장치(330)는 암호화 장치(331)와 저장 장치(332)를 포함하는 하나의 장치로써 동작하거나, 별개로 존재하는 암호화 장치(331)와 저장 장치(332)를 통칭하는 개념으로 해석될 수도 있다.

[0064] 추가로, 네트워크 장치(330)는 통신부(333)를 포함하여 구성될 수 있다. 통신부(330)는 데이터를 송수신한다. 네트워크 장치(330)가 암호화 장치(331)와 저장 장치(332)를 포함하는 하나의 장치로써 동작하는 경우, 통신부(333)는 네트워크 장치(330) 자체를 위하여 구비될 수 있다. 반면, 네트워크 장치(330)가 별개로 존재하는 암호화 장치(331)와 저장 장치(332)를 통칭하는 개념으로 해석되는 경우에, 통신부(333)는 암호화 장치(331)와 저장 장치(332)에 각각 구비될 수 있다. 이 경우, 암호화 장치(331)와 저장 장치(332)는 통신부(333)를 통하여 상호간 데이터를 송수신할 수 있다.

[0065] 네트워크 장치(330)는 서버 등의 형태로 구현될 수 있다. 네트워크 장치(330)가 암호화 장치(331)와 저장 장치(332)를 포함하는 하나의 장치로써 동작하는 경우, 네트워크 장치(330)는 암호화 장치(331)와 저장 장치(332)를 중앙에서 통제하는 별도의 제어 장치를 구비할 수도 있다.

[0066] 상기에서는 본 발명에 따른 eUICC를 지원하는 네트워크에 포함되는 엔티티들의 일 예를 설명한 것이며, eUICC를 위한 프로파일의 제공 및 설치를 위하여 필요한 다양한 엔티티를 더 포함하거나, 동일 또는 유사한 기능을 수행하는 장치 간에 생략 또는 통합하여 구성될 수 있다. 이 경우에도, 본 발명의 기술적 특징이 변형되지 않는 범위 내에서, 네트워크를 구성하는 엔티티들이 본 발명의 기술적 요지에 따른 동작을 수행하는 경우에는 해당 실시 예는 본 발명의 권리 범위에 속함은 자명하다.

[0067] 이하에서는, 상기한 본 발명의 실시 예에 따른 네트워크가 실질적으로 eUICC를 위한 프로파일을 설치하는 방법을 보다 구체적으로 설명한다.

[0068] 도 4는 본 발명의 제1 실시 예에 따른 eUICC를 위한 프로파일 설치 방법을 나타낸 흐름도이다.

[0069] 도 4를 참조하면, 본 발명의 제1 실시 예에서, SM-DP(410)는 제1 암호화 키로 암호화 된 프로파일 및 제2 암호화 키로 암호화된 제1 암호 키 쌍을 생성한다(401).

[0070] SM-DP(410)는 복수의 eUICC(430)를 위한 프로파일을 생성한다. SM-DP(410)는 각각의 eUICC(430)에 대한 프로파일을 구성하기 위한 정보로써, 각 eUICC(430)의 IMSI와 비밀 키 K 값을 생성할 수 있다.

[0071] SM-DP(410)는 각각의 프로파일에 대응하는 제1 암호 키로 각각의 프로파일을 암호화한다. 제1 암호 키는 SM-DP(410)에 구비되는 HSM에 의하여 랜덤하게 생성되는 랜덤 키로, 대칭 키이거나 비 대칭 키, 또는 SCP 03 세션 키일 수 있다. 제1 암호 키는 eUICC(430)에 대하여 독립적이며(즉, EID에 매핑되지 않는다.), 각각의 프로파일에 1:1로 대응될 수 있다. 따라서, 제1 암호 키로 암호화된 프로파일은 특정 eUICC(430)를 위한 것이 아니라 벌크(bulk) 형태로 생성된다. SM-DP(410)는 제1 암호 키로 암호화된 벌크 형태의 프로파일을 대량으로 생성하여 보관할 수 있다.

[0072] SM-DP(410)는 제1 암호 키를 제2 암호 키로 암호화하여 보관한다. 제2 암호 키는 마스터 키(Master key)로 대칭 키이거나 비 대칭 키일 수 있다. 또한, 제2 암호 키는 SM-DP(410)와 네트워크 장치 간 사전에 공유된 키로 상호를 인증할 수 있는 키일 수 있다.

[0073] SM-DP(410)는 제1 암호 키로 암호화된 프로파일 및 제2 암호 키로 암호화된 제1 암호 키 쌍을 저장 장치(421)로 전송한다(403). 저장 장치(421)는 제1 암호 키로 암호화된 프로파일 및 제2 암호 키로 암호화된 제1 암호 키 쌍을 프로파일 설치 개시 이전에 사전 보관한다(405).

[0074] 임의의 시점에서, eUICC(430)의 프로파일 설치가 실질적으로 개시되면, 암호화 장치(422)는 제2 암호 키로 암호화된 제1 암호 키를 복호하고, 이를 다시 제3 암호 키로 암호화한다(407).

[0075] 제3 암호 키는 eUICC(430) 별로 발행되는 전자 키로써, 대칭 키 또는 비 대칭 키일 수 있다. 제3 암호 키는 디지털 인증 방식에 의한 키로, 사전에 공유된 인증 방식에 따라 생성되는 공개 키 및 비밀 키 쌍으로 구성될 수 있다. 제3 암호 키는 eUICC(430)에 1:1로 대응되며, 따라서 해당 제3 암호 키에 대응하는 특정 eUICC(430)에서만 복호화가 가능할 수 있다.

[0076] 암호화 장치(422)와 eUICC(430)는 프로파일 설치 개시 이전에 또는 프로파일 설치 개시 이후에 오프라인 공유 방식 또는 네트워크 통신 방식으로 제3 암호 키를 사전 공유할 수 있다. 일 실시 예에서, 암호화 장치(422)와 eUICC(430)는 디지털 인증서를 공유하는 방식으로 제3 암호 키를 사전 공유할 수 있다. 즉, 암호화 장치(422)와 eUICC(430)는 같은 디지털 인증서를 공유함으로써, 해당 디지털 인증서로부터 생성되는 공개 키와 비밀 키 페어를 이용하여 상호 인증(데이터 암호화 및 복호화)을 수행할 수 있다.

[0077] 암호화 장치(422)는 제3 암호 키로 암호화된 제1 암호 키를 eUICC(430)로 전달한다(409). eUICC(430)는 사전에 공유된 제3 암호 키로 제1 암호 키를 복호화하여 보관한다(411).

[0078] 이후에, eUICC(430)는 저장 장치(421)로부터 제2 암호 키로 암호화된 프로파일을 수신한다(413).

[0079] 다양한 실시 예에서, 네트워크 장치(420)는 암호화된 프로파일 및 제1 키를 구성할 수 있는 전체 또는 부분 정보를 eUICC(430)로 전달할 수 있다.

[0080] eUICC(430)는 복호화된 제1 암호 키를 이용하여 암호화된 프로파일을 복호화한 후, 해당 프로파일을 설치할 수 있다(415).

[0081] 상술한 제1 실시 예에 따르면, SM-DP(410)는 eUICC(430)의 프로파일 설치 개시 이전에 암호화된 프로파일을 시간적인 제약 없이 대량으로 생성할 수 있다. 또한 SM-DP(410)는 암호화된 프로파일 및 암호화에 사용된 제1 암호 키를 네트워크 장치(420)와 사전 공유된 암호 키로 암호화하여 네트워크 장치(420)에 미리 보관시킴으로써, eUICC(430)의 프로파일 설치 시 SM-DP(410)와 직접적인 연동 없이도 eUICC(430)로 프로파일이 전달될 수 있도록 한다.

[0082] 도 5는 본 발명의 제2 실시 예에 따른 eUICC를 위한 프로파일 설치 방법을 나타낸 흐름도이다.

[0083] 도 5를 참조하면, 본 발명의 제2 실시 예에서, SM-DP(510)는 제2 암호 키로 암호화된 프로파일을 생성한다(501). 여기서 SM-DP(510)는 SIM 제조사의 프로파일 제공 서버일 수 있다.

[0084] SM-DP(510)는 복수의 eUICC(540)를 위한 프로파일을 생성한다. SM-DP(510)는 각각의 eUICC(540)에 대한 프로파일을 구성하기 위한 정보로써, 각 eUICC(540)의 IMSI와 비밀 키 K 값을 생성할 수 있다.

[0085] SM-DP(510)는 제2 암호 키로 각각의 프로파일을 암호화한다. 제2 암호 키는 마스터 키로 대칭 키이거나 비 대칭 키일 수 있다. 또한, 제2 암호 키는 SM-DP(510)와 네트워크 장치(520) 간 사전 공유된 키일 수 있다. 제2 암호 키는 eUICC(540)에 대하여 독립적이며, 각각의 프로파일에 1:1로 대응되거나 프로파일과 무관하게 동일할 수 있다. 따라서, 제2 암호 키로 암호화된 프로파일은 특정 eUICC(540)를 위한 것이 아니라 임의로 생성되어 암호화되는 것일 수 있다.

[0086] SM-DP(510)는 제2 암호 키로 암호화된 프로파일을 네트워크 장치(520)로 전송한다(503). 네트워크 장치(520)는 제2 암호 키로 암호화된 프로파일을 복호화한다(505).

[0087] 이후에, 네트워크 장치(520)는 직접 제1 암호 키를 생성한다(507). 제1 암호 키는 네트워크 장치(520)에 구비되는 암호화 장치에 의하여 랜덤하게 생성되는 랜덤 키로, 대칭 키이거나 비 대칭 키, 또는 SCP 03 세션 키일 수 있다.

[0088] 네트워크 장치(520)는 프로파일을 제1 암호 키로 재암호화하여 제1 암호 키로 암호화된 프로파일을 생성한다(509).

[0089] 일 실시 예에서, 네트워크 장치(520)는 Remote APDU(Application Protocol Data Unit) 형태로 암호화된 프로파일을 생성할 수 있다. Remote APDU는 원격서버와 eUICC 간 암호화된 명령어를 전달하는 규격(ETSI TS 102.226)의 일종으로, 데이터를 바이트 어레이 버퍼 단위로 분할하여 전송할 때 생성하는 데이터 단위이다. 네트워크 장치(520)는 프로파일을 제1 암호 키로 재암호화하여 Remote APDU를 생성할 수 있다.

[0090] 네트워크 장치(520)는 제1 암호 키 및 제1 암호 키로 암호화된 프로파일을 SM-DP(530)로 전송한다(511). 이때, SM-DP(530)는 SIM 제조사의 프로파일 제공 서버와 같은 SM-DP이거나, 단말 제조사에 의하여 별도로 운영되는 프로파일 제공 서버일 수 있다. SM-DP(530)는 제1 암호 키 및 제1 암호 키로 암호화된 프로파일을 프로파일 설치 개시 이전에 대량으로 보관할 수 있다.

[0091] 임의의 시점에서, eUICC(540)의 프로파일 설치가 실질적으로 개시되면, SM-DP(530)는 제3 암호 키로 제1 암호 키를 암호화한다(513). 제3 암호 키는 eUICC(540) 별로 발행되는 전자 키로써, 대칭 키 또는 비 대칭 키일 수 있다. 제3 암호 키는 디지털 인증 방식에 의한 키로, 사전에 공유된 인증 방식에 따라 생성되는 공개 키 및 비밀 키 쌍으로 구성될 수 있다. 제3 암호 키는 eUICC(540)에 1:1로 대응되며, 따라서 해당 제3 암호 키에 대응하는 특정 eUICC(540)에서만 복호화가 가능할 수 있다.

[0092] SM-DP(530)와 eUICC(540)는 프로파일 설치 개시 이전에 또는 프로파일 설치 개시 이후에 오프라인 공유 방식 또는 네트워크 통신 방식으로 제3 암호 키를 사전 공유할 수 있다. 일 실시 예에서, SM-DP(530)와 eUICC(540)는 디지털 인증서를 공유하는 방식으로 제3 암호 키를 사전 공유할 수 있다. 즉, SM-DP(530)와 eUICC(540)는 같은 디지털 인증서를 공유함으로써, 해당 디지털 인증서로부터 생성되는 공개 키와 비밀 키 페어를 이용하여 상호 인증(데이터 암호화 및 복호화)을 수행할 수 있다.

[0093] SM-DP(530)는 제3 암호 키로 암호화된 제1 암호 키를 eUICC(540)로 전달한다(515). 일 실시 예에서, SM-DP(530)는 CCCM Scenario #1에 따라 제1 암호 키를 eUICC(540)로 전달할 수 있다. Scenario #1은 세션 키를 암호화하여 전달하는 글로벌 플랫폼(Global Platform) 규격 기술의 하나로, 제1 암호 키 요청 및 응답(또는 제1 암호 키 전송 및 응답)을 통하여 SM-DP(530)와 eUICC(540) 간 직접 통신에 의해 제1 암호 키를 전달하는 방식일 수 있다.

[0094] eUICC(540)는 사전에 공유된 제3 암호 키로 제1 암호 키를 복호화하여 보관한다(517).

[0095] 이후에, eUICC(540)는 SM-DP(530)로부터 remote APDU 기반 프로파일 설치를 수행한다(519). eUICC(540)는 SM-DP(530)로부터 제1 암호 키로 암호화하여 생성된 remote APDU를 수신하고, 제1 암호 키를 이용하여 remote APDU를 복호화하여 프로파일을 획득한다. eUICC(540)는 획득된 프로파일을 설치할 수 있다.

[0096] 상술한 제2 실시 예에 따르면, SM-DP(510)는 eUICC(540)의 프로파일 설치 개시 이전에 네트워크 장치에 의하여

시간적인 제약 없이 생성된 암호화된 프로파일을 대량으로 미리 보관할 수 있다. 또한 SM-DP(540)는 암호화된 프로파일 및 암호화에 사용된 제1 암호 키를 Remote APDU 기반으로 프로비저닝함으로써, 네트워크 상황에 의한 영향을 적게 받으며 프로파일이 설치될 수 있도록 한다.

[0097] 제2 실시 예는 제1 실시 예와 비교하여, 제1 암호 키 생성 및 제1 암호 키로 복호화된 프로파일 생성 주체가 SM-DP로부터 네트워크 장치로 변경된다는 점에서 제1 실시 예와 구분될 수 있다. 또한, 제2 실시 예는 제1 실시 예와 비교하여, 암호화된 프로파일을 eUICC로 전달하는 주체가 네트워크 장치에서 SM-DP로 변경된다는 점에서 제1 실시 예와 구분될 수 있다. 그에 따라, 제2 실시 예는 제1 실시 예와 비교하여, 제3 암호 키로 암호화된 제1 암호 키의 전송 시 CCCM Scenario #1이 사용된다는 점 및 프로파일 설치가 Remote APDU 기반으로 수행된다는 점에서 제1 실시 예와 구분될 수 있다.

[0098] 도 6은 본 발명의 제3 실시 예에 따른 eUICC를 위한 프로파일 설치 방법을 나타낸 흐름도이다.

[0099] 도 6을 참조하면, 본 발명의 제3 실시 예에서, SM-DP(610)는 제1 암호화 키로 암호화된 프로파일을 생성한다(601).

[0100] SM-DP(610)는 복수의 eUICC(630)를 위한 프로파일을 생성한다. SM-DP(610)는 각각의 eUICC(630)에 대한 프로파일을 구성하기 위한 정보로써, 각 eUICC(630)의 IMSI와 비밀 키 K 값을 생성할 수 있다.

[0101] SM-DP(610)는 각각의 프로파일에 대응하는 제1 암호 키로 각각의 프로파일을 암호화한다. 제1 암호 키는 SM-DP(610)에 구비되는 HSM에 의하여 랜덤하게 생성되는 랜덤 키로, 대칭 키이거나 비 대칭 키, 또는 SCP 03 세션 키일 수 있다. 제1 암호 키는 eUICC(630)에 대하여 독립적이며, 각각의 프로파일에 1:1로 대응될 수 있다. 따라서, 제1 암호 키로 암호화된 프로파일은 특정 eUICC(650)를 위한 것이 아니라 벌크(bulk) 형태로 생성된다. SM-DP(610)는 제1 암호 키로 암호화된 벌크 형태의 프로파일을 대량으로 생성하여 보관할 수 있다.

[0102] SM-DP(610)는 제1 암호 키로 암호화된 프로파일을 네트워크 장치(620)로 전송한다(603). 네트워크 장치(620)는 제1 암호 키로 암호화된 프로파일을 프로파일 설치 개시 이전에 사전 보관한다(605).

[0103] 임의의 시점에서, eUICC(630)의 프로파일 설치가 실질적으로 개시되면, 네트워크 장치(620)는 프로파일을 설치할 적어도 하나의 eUICC를 결정한다(607). 네트워크 장치(620)는 eUICC(630) 또는 MNO의 요청 또는 기 설정된 조건에 따라 프로파일 설치 이벤트가 트리거링된 eUICC(630)를 판단하고, 판단 결과를 기초로 프로파일을 설치할 적어도 하나의 eUICC를 결정할 수 있다.

[0104] 네트워크 장치(620)는 프로파일을 설치할 적어도 하나의 eUICC에 관한 정보(목록)를 SM-DP(610)로 전송한다(609). 프로파일을 설치할 적어도 하나의 eUICC에 관한 정보는, 해당 eUICC의 식별자(EID), 해당 eUICC에 설치될 프로파일의 식별자, 해당 eUICC의 인증서 등을 포함할 수 있다.

[0105] eUICC 로부터 프로파일을 설치할 적어도 하나의 eUICC에 관한 정보를 수신한 SM-DP(610)는, 제1 암호 키를 제3 암호 키로 암호화한다(611). 제3 암호 키는 eUICC(630) 별로 발행되는 전자 키로써, 대칭 키 또는 비 대칭 키일 수 있다. 제3 암호 키는 디지털 인증 방식에 의한 키로, 사전에 공유된 인증 방식에 따라 생성되는 공개 키 및 비밀 키 쌍으로 구성될 수 있다. 제3 암호 키는 eUICC(630)에 1:1로 대응되며, 따라서 해당 제3 암호 키에 대응하는 특정 eUICC(630)에서만 복호화가 가능할 수 있다.

[0106] SM-DP(610)와 eUICC(630)는 프로파일 설치 개시 이전에 또는 프로파일 설치 개시 이후에 오프라인 공유 방식 또는 네트워크 통신 방식으로 제3 암호 키를 사전 공유할 수 있다. 일 실시 예에서, SM-DP(610)와 eUICC(630)는 디지털 인증서를 공유하는 방식으로 제3 암호 키를 사전 공유할 수 있다. 즉, SM-DP(610)와 eUICC(630)는 같은 디지털 인증서를 공유함으로써, 해당 디지털 인증서로부터 생성되는 공개 키와 비밀 키 페어를 이용하여 상호 인증(데이터 암호화 및 복호화)을 수행할 수 있다. 다양한 실시 예에서, 제3 암호 키로 암호화된 제1 암호 키는 SM-DP(610)로부터 eUICC(630) 직접 전달될 수 있다.

[0107] SM-DP(610)는 제3 암호 키로 암호화된 제1 암호 키를 네트워크 장치(620)로 전송한다(613). 네트워크 장치(620)는 eUICC(630)로 암호화된 제2 암호 키를 전달한다(615). 또한, 네트워크 장치(620)는 eUICC(630)로 제1 암호 키로 암호화된 프로파일을 전달한다(617).

[0108] eUICC(630)는 제3 암호 키로 암호화된 제1 암호 키를 복호화하여 제1 암호 키를 획득하고(619), 획득된 제1 암호 키를 이용하여 암호화된 프로파일을 복호화한 후, 해당 프로파일을 설치할 수 있다(621).

[0109] 상술한 제3 실시 예에 따르면, 네트워크 장치(620)는 eUICC(630)의 프로파일 설치 개시 이전에 SM-DP(610)에 의하여 시간적인 제약 없이 생성된 암호화된 프로파일을 대량으로 미리 보관할 수 있다.

[0110] 제3 실시 예는 제1 실시 예와 비교하여, 암호화 된 제1 암호 키의 전달이, 프로파일 설치 개시 이후, 네트워크 장치에 의해 요청된 eUICC에 대해서만 이루어 진다는 점에서 제1 실시 예와 구분될 수 있다.

[0111] 이하에서는, 상술한 본 발명의 실시 예들에 따라 동작하는 장치들의 구성을 설명하도록 한다.

[0112] 도 7은 본 발명의 실시 예에 따른 장치들의 구조를 나타낸 블록도이다.

[0113] 도 7을 참조하면, 본 발명의 실시 예에 따른 SM-DP(700)는 통신부(701), 제어부(702) 및 암호화부(703)를 포함하여 구성될 수 있다.

[0114] 통신부(701)는 다른 장치들로 데이터를 송신하거나 다른 장치로부터 데이터를 수신할 수 있다. 통신부(701)는 암호화 된 키, 암호화된 프로파일 등을 송신하거나 수신할 수 있다. 이를 위하여 통신부(701)는 적어도 하나의 통신 모듈과 안테나 등을 구비할 수 있다.

[0115] 제어부(702)는 본 발명에 따른 프로파일 설치를 위하여 SM-DP(700)의 각 구성 요소를 제어할 수 있다. 제어부(702)의 구체적인 동작을 상술한 바와 같다.

[0116] 암호화부(703)는 제어부(702)의 제어에 따라 키 또는 프로파일의 암호화 또는 복호화를 수행한다. 구현하기에 따라, 암호화부(703)는 제어부(702)에 내장되거나, 제어부(702)에 의하여 구동되는 소프트웨어 코드 형식으로 구현될 수 있다.

[0117] 도 7을 참조하면, 본 발명의 실시 예에 따른 네트워크 장치(710)는 통신 장치(711), 암호화 장치(712) 및 저장 장치(713)를 포함하여 구성될 수 있다.

[0118] 통신 장치(711)는 다른 장치들로 데이터를 송신하거나 다른 장치로부터 데이터를 수신할 수 있다. 통신 장치(711)는 암호화 된 키, 암호화된 프로파일 등을 송신하거나 수신할 수 있다. 이를 위하여 통신 장치(711)는 적어도 하나의 통신 모듈과 안테나 등을 구비할 수 있다.

[0119] 다양한 실시 예에서, 네트워크 장치(710)가 암호화 장치(712)와 저장 장치(713)를 포함하는 하나의 장치로써 동작하는 경우, 통신 장치(711)는 네트워크 장치(710) 자체를 위하여 구비될 수 있다. 반면, 네트워크 장치(710)가 별개로 존재하는 암호화 장치(712)와 저장 장치(713)를 통칭하는 개념으로 해석되는 경우에, 통신 장치(711)는 암호화 장치(712)와 저장 장치(713)에 각각 구비될 수 있다. 이 경우, 암호화 장치(712)와 저장 장치(713)는 통신 장치(711)를 통하여 상호간 데이터를 송수신할 수 있다.

[0120] 암호화 장치(712)는 암호화 장치(712)는 HSM을 포함하거나 HSM 그 자체로 명명될 수 있으며, 암호 키를 노출시키지 않고 프로파일의 암호화 및 복호화를 수행할 수 있다.

[0121] 저장 장치(713)는 적어도 하나의 프로파일을 저장한다. 저장 장치(713)는 하드디스크 타입(hard disk type), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다.

[0122] 네트워크 장치(710)는 서버 등의 형태로 구현될 수 있다. 네트워크 장치(710)가 암호화 장치(712)와 저장 장치(713)를 포함하는 하나의 장치로써 동작하는 경우, 네트워크 장치(710)는 암호화 장치(712)와 저장 장치(713)를 중앙에서 통제하는 별도의 제어 장치를 구비할 수도 있다.

[0123] 도 7을 참조하면, 본 발명의 실시 예에 따른 단말(720)은 통신부(721), 제어부(722) 및 eUICC(723)를 포함하여 구성될 수 있다.

[0124] 통신부(721)는 다른 장치들로 데이터를 송신하거나 다른 장치로부터 데이터를 수신할 수 있다. 통신부(721)는 암호화 된 키, 암호화된 프로파일 등을 수신할 수 있다. 이를 위하여 통신부(721)는 적어도 하나의 통신 모듈과 안테나 등을 구비할 수 있다.

[0125] 제어부(722)는 본 발명에 따른 프로파일 설치를 위하여 단말(720)의 각 구성 요소를 제어할 수 있다. 제어부(722)의 구체적인 동작을 상술한 바와 같다.

[0126] eUICC(723)은 단말(720)에 내장된 UICC칩으로, 적어도 하나의 프로파일을 저장, 관리, 삭제하는 기능을 수행한다. 프로파일은 기존 UICC 카드에 저장되는 하나 또는 복수 개의 어플리케이션 및 가입자 인증정보, 전화번호부 등의 데이터 정보를 총칭한다.

[0127] 이상에서 설명된 본 명세서와 도면에 개시된 본 발명의 실시 예들은 본 발명의 기술 내용을 쉽게 설명하고, 본 발명의 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 또한 앞서 설명된 본 발명에 따른 실시 예들은 예시적인 것에 불과하며, 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 범위의 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 다음의 특허청구범위에 의해서 정해져야 할 것이다.

부호의 설명

[0128] 100: 단말 101: 제어부

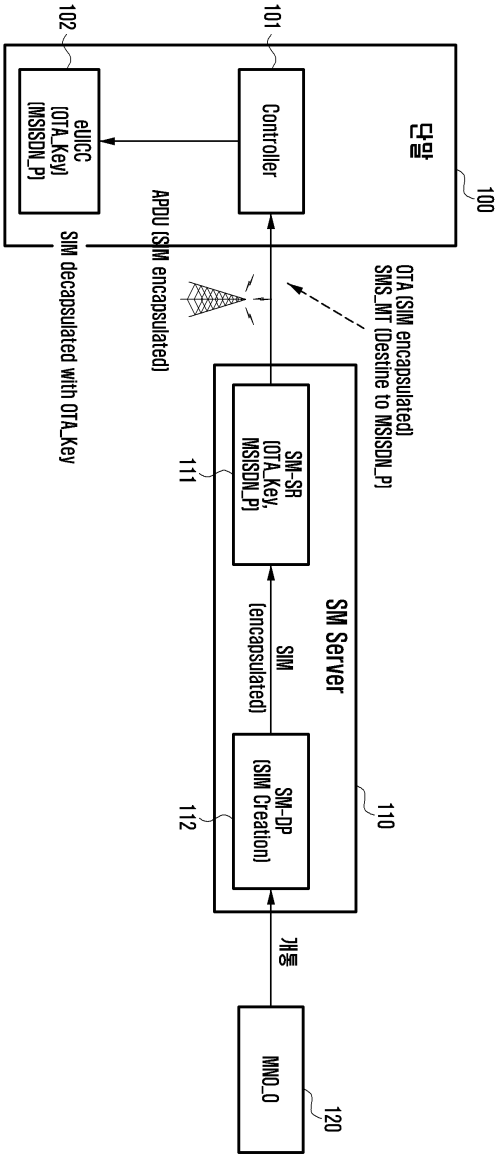
102: eUICC 110: SM 서버

111: SM-SR 112: SM-DP

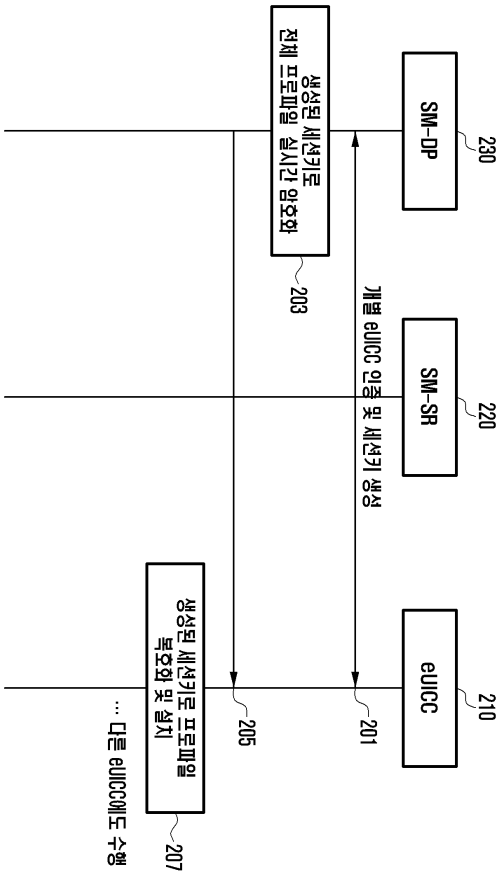
120: MNO

도면

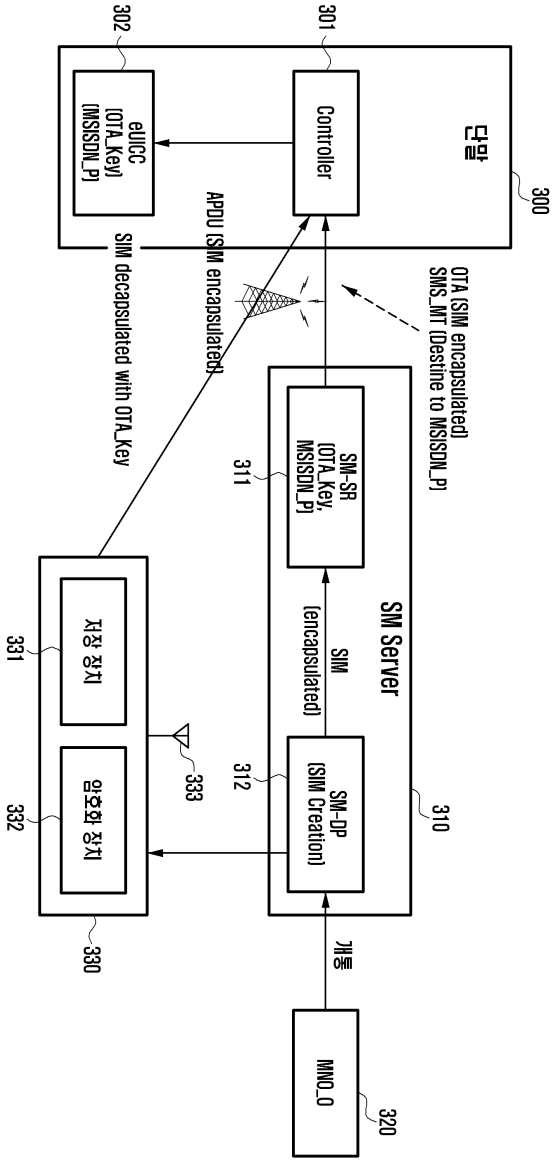
도면1


단말
100
Controller
101
eUICC
(OTA_Key)
(MSISDN_P)
102
APDU (SIM encapsulated)
SIM decapsulated with OTA_Key
OTA (SIM encapsulated)
SMS_MT (Destine to MSISDN_P)
SM Server
110
SM-SR
(OTA_Key,
MSISDN_P)
111
SIM
(encapsulated)
SM-DP
(SIM Creation)
112
개통
MNO_O
120

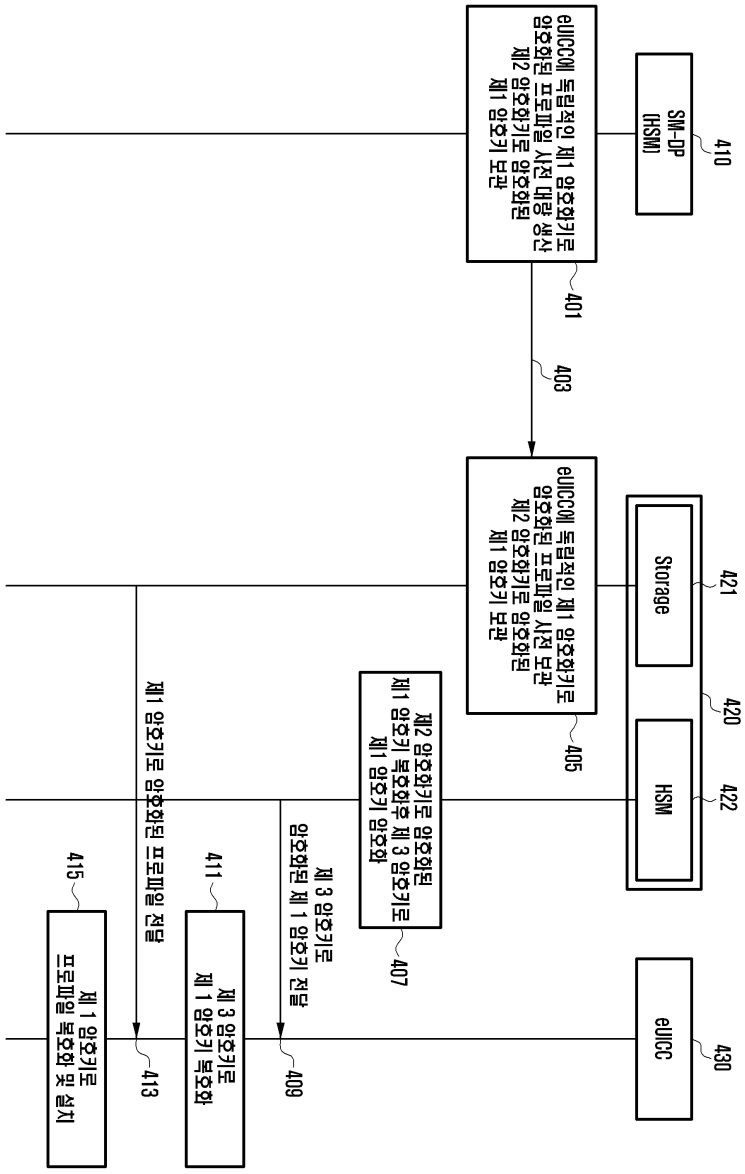
도면2


SM-DP
230
SM-SR
220
eUICC
210
생성된 세션키로
전체 프로파일 실시간 암호화
203
개별 eUICC 인증 및 세션키 생성
201
205
생성된 세션키로 프로파일
복호화 및 설치
207
… 다른 eUICC에도 수행

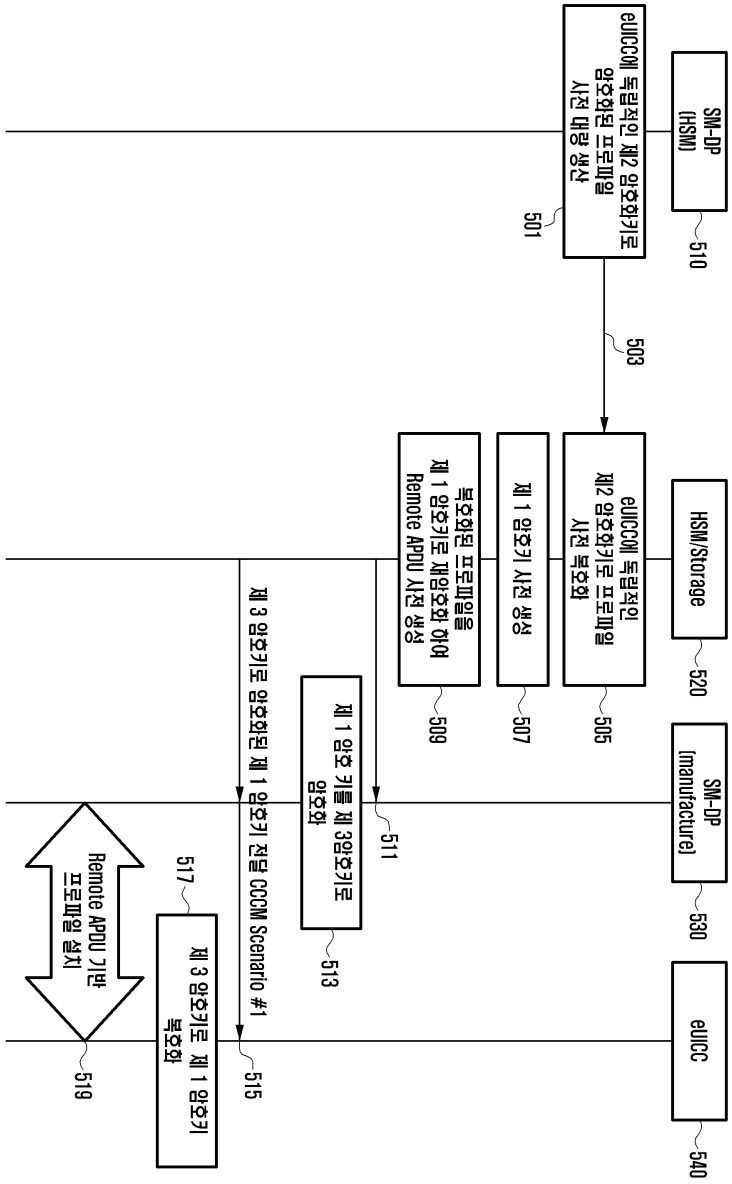
도면3


302
301
eUICC
(OTA_Key)
(MSISDN_P)
Controller
단말
300
APDU (SIM encapsulated)
SIM decapsulated with OTA_Key
OTA (SIM encapsulated)
SMS_MT (Destine to MSISDN_P)
311
SM-SR
(OTA_Key,
MSISDN_P)
SM Server
SIM
(encapsulated)
312
SM-DP
(SIM Creation)
310
331
저장 장치
332
암호화 장치
333
330
개통
MNO_O
320

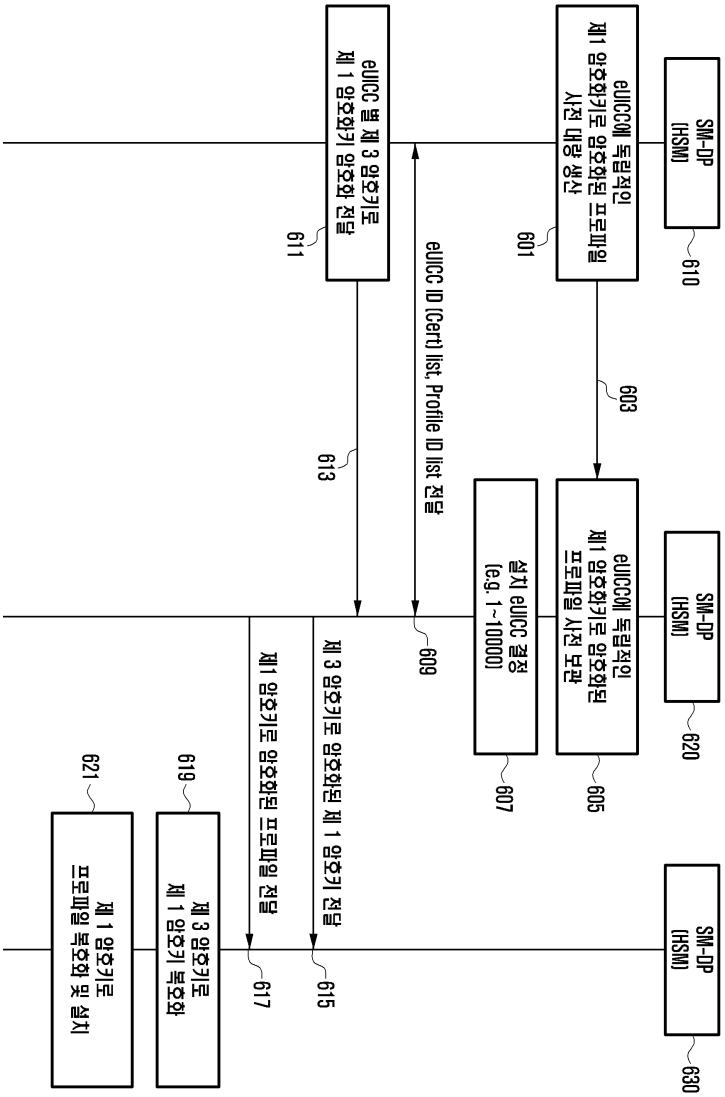
도면4


SM-DP (HSM)
410
eUICC에 독립적인 제1 암호화키로 암호화된 프로파일 사전 대량 생산 제2 암호화키로 암호화된 제1 암호키 보관
401
403
eUICC에 독립적인 제1 암호화키로 암호화된 프로파일 사전 보관 제2 암호화키로 암호화된 제1 암호키 보관
405
Storage
421
420
HSM
422
제2 암호화키로 암호화된 제1 암호키 복호화후 제3 암호키로 제1 암호키 암호화
407
제1 암호키로 암호화된 프로파일 전달
제3 암호키로 암호화된 제1 암호키 전달
409
eUICC
430
415
제1 암호키로 프로파일 복호화 및 설치
411
제3 암호키로 제1 암호키 복호화
413

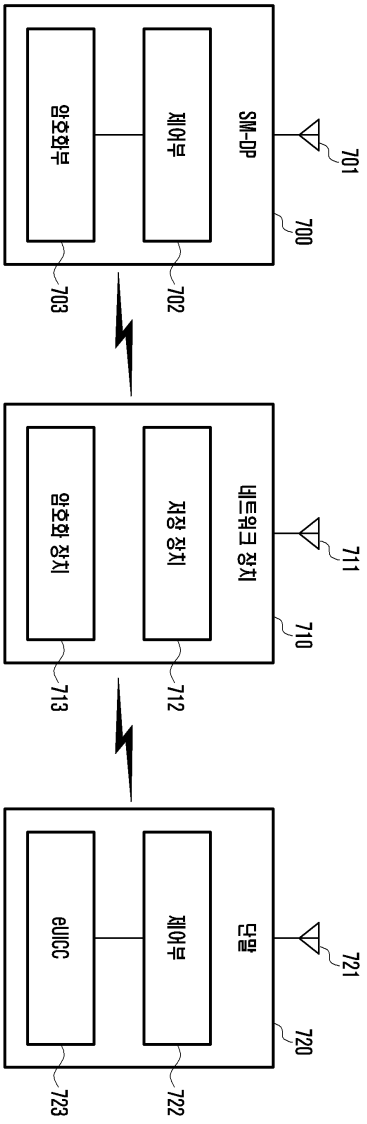
도면5


SM-DP (HSM)
510
eUICC에 독립적인 제2 암호화키로 암호화된 프로파일 사전 대량 생산
501
503
HSM/Storage
520
eUICC에 독립적인 제2 암호화키로 프로파일 사전 복호화
505
제 1 암호키 사전 생성
507
복호화된 프로파일을 제 1 암호키로 재암호화 하여 Remote APDU 사전 생성
509
SM-DP (manufacture)
530
제 1 암호 키를 제 3암호키로 암호화
511
513
제 3 암호키로 암호화된 제 1 암호키 전달 CCCM Scenario #1
eUICC
540
Remote APDU 기반 프로파일 설치
519
517
제 3 암호키로 제 1 암호키 복호화
515

도면6


SM-DP (HSM)
610
eUICC에 독립적인 제1 암호키로 암호화된 프로파일 사전 대량 생산
601
603
eUICC 별 제 3 암호키로 제 1 암호키 암호화 전달
611
613
eUICC ID (Cert) list, Profile ID list 전달
609
설치 eUICC 결정 (e.g. 1~10000)
607
eUICC에 독립적인 제1 암호키로 암호화된 프로파일 사전 보관
605
SM-DP (HSM)
620
제 3 암호키로 암호화된 제 1 암호키 전달
615
제1 암호키로 암호화된 프로파일 전달
617
제 3 암호키로 제 1 암호키 복호화
619
제 1 암호키로 프로파일 복호화 및 설치
621
SM-DP (HSM)
630

도면7


SM-DP
제어부
암호화부
701
700
702
703
네트워크 장치
저장 장치
암호화 장치
711
710
712
713
단말
제어부
eUICC
721
720
722
723