(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0026958
(43) 공개일자 2013년03월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04W 8/18* (2009.01)
(21) 출원번호 10-2011-0104171
(22) 출원일자 2011년10월12일
심사청구일자 없음
(30) 우선권주장
1020110089841 2011년09월05일 대한민국(KR)

(71) 출원인
주식회사 케이티
경기도 성남시 분당구 불정로 90 (정자동 206 번지)
(72) 발명자
이진형
서울특별시 서초구 태봉로 151, KT연구개발센터 (우면동)
윤여민
서울특별시 서초구 태봉로 151, KT연구개발센터 (우면동)
김성철
서울특별시 서초구 태봉로 151, KT연구개발센터 (우면동)
(74) 대리인
송해모, 김은구

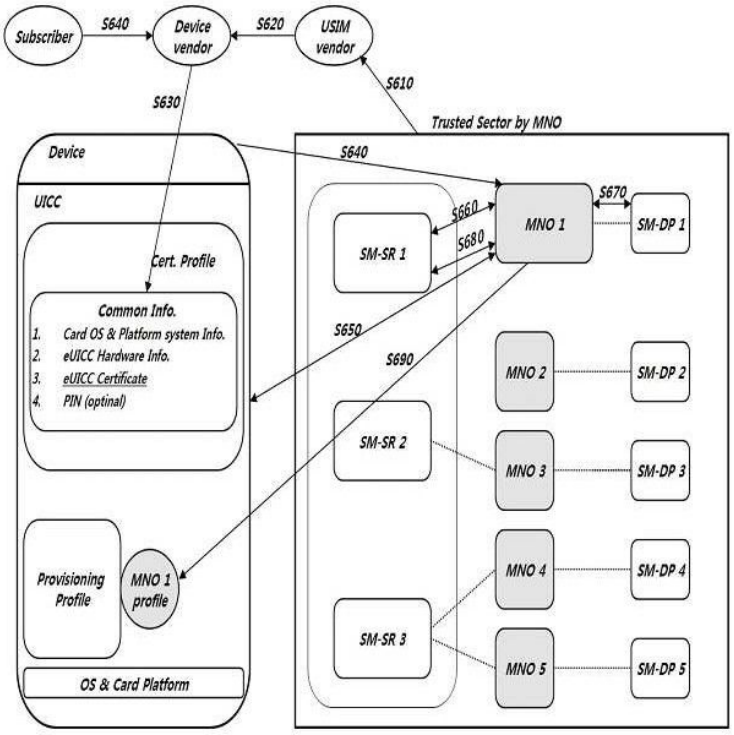
전체 청구항 수 : 총 26 항

(54) 발명의 명칭 **내장 ＵＩＣＣ의 인증정보를 이용한 인증방법과, 그를 이용한 프로비저닝 및 ＭＮＯ 변경 방법, 그를 위한 내장 ＵＩＣＣ, ＭＮＯ 시스템 및 기록매체**

(57) 요 약

본 발명은 MNO(Mobile Network Operator), SM(Subscription Manager), eUICC(Embedded UICC) 등으로 구성된 시스템에서 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 저장하고, 프로비저닝 또는 MNO 변경 과정에서 eUICC 인증정보를 MNO 시스템 또는 SM으로 전송하며, MNO 시스템 또는 SM은 수신한 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증하고, 검증된 경우에 한하여 프로파일을 암호화하여 eUICC로 전송함으로써, 프로비저닝 또는 MNO 변경과 같은 과정에서 eUICC를 검증할 수 있도록 한다.

대 표 도



특허청구의 범위

청구항 1

통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)의 인증방법으로서,

상기 eUICC는 상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 저장하는 단계;

상기 eUICC는 상기 eUICC 인증정보를 상기 MNO 시스템 또는 상기 SM으로 전송하는 단계;를 포함하는 것을 특징으로 하는 eUICC 인증방법.

청구항 2

제1항에 있어서,

상기 eUICC 인증정보는, 1)상기 eUICC의 하드웨어 및 카드 OS, 플랫폼 중 하나에 대하여 검정되었다는 정보, 2)상기 MNO 시스템 및 SM이 신뢰할 수 있는 eUICC로 사전 검정되었다는 정보 및 3)상기 MNO 시스템이 MNO 서비스들을 탑재할 수 있다고 검증되었다는 정보 중 하나 이상인 것을 특징으로 하는 eUICC 인증방법

청구항 3

제1항에 있어서,

상기 eUICC 인증정보는 카드 OS 정보, 카드 플랫폼 정보를 포함하는 공통정보(Common Information) 내에 포함되어 저장되는 것을 특징으로 하는 eUICC 인증방법.

청구항 4

제3항에 있어서,

상기 eUICC 인증정보를 포함하는 공통정보는 eUICC 인증 프로파일 내에 포함되는 것을 특징으로 하는 eUICC 인증방법.

청구항 5

제3항에 있어서,

상기 공통정보는 상기 eUICC의 PIN(Personal Identification Number)를 추가로 포함하는 것을 특징으로 하는 eUICC 인증방법.

청구항 6

통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서, 상기 eUICC는 상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate) 및 카드 OS 정보와 카드 플랫폼 정보, PIN(Personal Identification Number) 정보 중 하나 이상을 포함하는 eUICC 인증 프로파일을 저장하고, 상기 eUICC 인증 프로파일은 상기 eUICC 인증정보를 상기 MNO 시스템 또는 상기 SM으로 전송하는 것을 특징으로 하는 eUICC.

청구항 7

제6항에 있어서,

상기 eUICC 인증정보는, 1) 상기 eUICC의 하드웨어 및 카드 OS, 플랫폼 중 하나에 대하여 검정되었다는 정보, 2) 상기 MNO 시스템 및 SM이 신뢰할 수 있는 eUICC로 사전 검정되었다는 정보 및 3) 상기 MNO 시스템이 MNO 서비스들을 탑재할 수 있다고 검증되었다는 정보 중 하나 이상인 것을 특징으로 하는 eUICC.

청구항 8

통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 상기 MNO 시스템 및 SM과 연동되어 있는 내장 UICC(eUICC)로

서, 상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 포함하는 eUICC를 이용하는 프로비저닝 방법으로서,

상기 eUICC는 eUICC 제조 단계에서 생성된 상기 eUICC 인증정보를 수신하여 저장하는 단계;

상기 eUICC는 상기 eUICC 인증정보를 상기 MNO 시스템으로 전송하는 단계;

상기 MNO 시스템은 상기 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증하는 단계;

상기 MNO 시스템은 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 단계;

를 포함하는 것을 특징으로 하는 프로비저닝 방법.

청구항 9

제8항에 있어서,

상기 eUICC 인증정보는, 1) 상기 eUICC의 하드웨어 및 카드 OS, 플랫폼 중 하나에 대하여 검정되었다는 정보, 2) 상기 MNO 시스템 및 SM이 신뢰할 수 있는 eUICC로 사전 검정되었다는 정보 및 3) 상기 MNO 시스템이 MNO 서비스들을 탑재할 수 있다고 검증되었다는 정보 중 하나 이상인 것을 특징으로 하는 프로비저닝 방법.

청구항 10

제8항에 있어서,

상기 오퍼레이션 프로파일은 MNO 프로파일 키로 1차 암호화된 후, MNO OTA키로 2차 암호화되는 것을 특징으로 하는 프로비저닝 방법.

청구항 11

제10항에 있어서,

상기 MNO OTA 키는 상기 MNO 시스템이 상기 SM으로부터 제공받는 것을 특징으로 하는 프로비저닝 방법.

청구항 12

통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 상기 MNO 시스템 및 SM과 연동되어 있는 내장 UICC(eUICC)로서, 상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 포함하는 eUICC를 이용하는 MNO 변경 방법으로서,

상기 eUICC는 eUICC 제조 단계에서 생성된 상기 eUICC 인증정보를 수신하여 저장하는 단계;

상기 eUICC는 상기 eUICC 인증정보를 리시빙 MNO 시스템으로 전송하는 단계;

상기 리시빙 MNO 시스템은 상기 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증하는 단계;

상기 리시빙 MNO 시스템은 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 단계;

상기 eUICC는 MNO 변경 사실을 상기 리시빙 MNO 시스템 및 도너 MNO 시스템에게 통지하는 단계;

를 포함하는 것을 특징으로 하는 MNO 변경 방법.

청구항 13

제12항에 있어서,

상기 eUICC 인증정보는, 1) 상기 eUICC의 하드웨어 및 카드 OS, 플랫폼 중 하나에 대하여 검정되었다는 정보, 2) 상기 MNO 시스템 및 SM이 신뢰할 수 있는 eUICC로 사전 검정되었다는 정보 및 3) 상기 MNO 시스템이 MNO 서비스들을 탑재할 수 있다고 검증되었다는 정보 중 하나 이상인 것을 특징으로 하는 MNO 변경 방법.

청구항 14

사업자 시스템(MNO), 가입 관리 시스템(Subcription Manager; SM)을 구성하는 SM-SR(Secure Routing) 및 SM-DP(Data Preparation) 장치와 연동된 내장 UICC(eUICC)를 이용한 프로비저닝 방법으로서,

상기 eUICC가 eUICC 제조사 시스템 또는 단말 제조사 시스템으로부터 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 수신하여 상기 eUICC 내에 저장하는 단계;

가입자의 개통요청에 따라 상기 활성화 요청 또는 개통 요청 메시지를 상기 MNO 시스템으로 전송하는 단계;

상기 MNO 시스템이 상기 eUICC으로부터 상태 요청 및 기술성능 제어 확인을 수행하면서, 상기 eUICC로부터 상기 eUICC 인증정보를 수신하는 단계;

상기 MNO 시스템이 상기 SM-SR로부터 단말 관련 정보를 수집하는 과정 중에 상기 eUICC 인증정보를 SM-SR로 전송하는 단계;

상기 MNO 시스템 또는 상기 SM-SR가 상기 eUICC 인증정보를 통한 eUICC 검증이 된 경우에 한하여, 상기 MNO 시스템이 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 단계;

를 포함하는 것을 특징으로 하는 프로비저닝 방법.

청구항 15

제14항에 있어서,

상기 eUICC 인증정보는, 1) 상기 eUICC의 하드웨어 및 카드 OS, 플랫폼 중 하나에 대하여 검정되었다는 정보, 2) 상기 MNO 시스템 및 SM이 신뢰할 수 있는 eUICC로 사전 검정되었다는 정보 및 3) 상기 MNO 시스템이 MNO 서비스들을 탑재할 수 있다고 검증되었다는 정보 중 하나 이상인 것을 특징으로 하는 프로비저닝 방법.

청구항 16

제14항에 있어서,

상기 오퍼레이션 프로파일은 MNO 프로파일 키로 1차 암호화된 후, MNO OTA키로 2차 암호화되는 것을 특징으로 하는 프로비저닝 방법.

청구항 17

사업자 시스템(MNO), 가입 관리 시스템(Subcription Manager; SM)을 구성하는 SM-SR(Secure Routing) 및 SM-DP(Data Preparation) 장치와 연동된 내장 UICC(eUICC)를 이용한 MNO 변경 방법으로서,

상기 eUICC가 eUICC 제조사 시스템 또는 단말 제조사 시스템으로부터 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 수신하여 상기 eUICC 내에 저장하는 단계;

MNO 변경요청에 따라 상기 eUICC가 활성화 요청 또는 개통 요청 메시지를 리시빙 MNO 시스템으로 전송하는 단계;

상기 리시빙 MNO 시스템이 상기 eUICC으로부터 상태 요청 및 기술성능 제어 확인을 수행하면서, 상기 eUICC로부터 상기 eUICC 인증정보를 수신하는 단계;

상기 리시빙 MNO 시스템이 상기 SM-SR로부터 단말 관련 정보를 수집하는 과정 중에 상기 eUICC 인증정보를 SM-SR로 전송하는 단계;

상기 리시빙 MNO 시스템이 도너 MNO 시스템과 MNO 변경을 위한 협상 및 권리이전을 수행하는 단계;

상기 리시빙 MNO 시스템 또는 상기 SM-SR가 상기 eUICC 인증정보를 통한 eUICC 검증이 된 경우에 한하여, 상기 리시빙 MNO 시스템이 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 단계;

를 포함하는 것을 특징으로 하는 MNO 변경 방법.

청구항 18

제17항에 있어서,

상기 eUICC 인증정보는, 1) 상기 eUICC의 하드웨어 및 카드 OS, 플랫폼 중 하나에 대하여 검정되었다는 정보, 2) 상기 MNO 시스템 및 SM이 신뢰할 수 있는 eUICC로 사전 검정되었다는 정보 및 3) 상기 MNO 시스템이 MNO 서비스들을 탑재할 수 있다고 검증되었다는 정보 중 하나 이상인 것을 특징으로 하는 MNO 변경 방법.

청구항 19

제17항에 있어서,

상기 오퍼레이션 프로파일은 MNO 프로파일 키로 1차 암호화된 후, MNO OTA키로 2차 암호화되는 것을 특징으로 하는 MNO 변경 방법.

청구항 20

통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 상기 MNO 시스템 및 SM과 연동되어 있으며, 상기 MNO에 대한 오퍼레이션 프로파일을 관리하는 내장 UICC(eUICC)로서,

상기 eUICC는 eUICC 제조 단계에서 생성된 eUICC 인증정보를 수신하여 저장하고, 상기 eUICC 인증정보를 상기 MNO 시스템으로 전송하며, 상기 MNO 시스템으로부터 전송된 암호화된 상기 오퍼레이션 프로파일을 수신하여 복호화하는 것을 특징으로 하는 eUICC.

청구항 21

제20항에 있어서,

상기 eUICC 인증정보는, 1) 상기 eUICC의 하드웨어 및 카드 OS, 플랫폼 중 하나에 대하여 검정되었다는 정보, 2) 상기 MNO 시스템 및 SM이 신뢰할 수 있는 eUICC로 사전 검정되었다는 정보 및 3) 상기 MNO 시스템이 MNO 서비스들을 탑재할 수 있다고 검증되었다는 정보 중 하나 이상인 것을 특징으로 하는 eUICC.

청구항 22

제20항에 있어서,

상기 오퍼레이션 프로파일은 이중 암호화(Double Ciphered)된 프로파일인 것을 특징으로 하는 eUICC.

청구항 23

가입 관리시스템(SM) 및 내장 UICC(eUICC)와 연동된 MNO 시스템으로서,

상기 MNO 시스템은 프로비저닝 또는 MNO 변경 과정에서,

상기 eUICC로부터 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 수신하고, 상기 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증한 후, 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 것을 특징으로 하는 MNO 시스템.

청구항 24

제23항에 있어서,

상기 eUICC 인증정보는, 1) 상기 eUICC의 하드웨어 및 카드 OS, 플랫폼 중 하나에 대하여 검정되었다는 정보, 2) 상기 MNO 시스템 및 SM이 신뢰할 수 있는 eUICC로 사전 검정되었다는 정보 및 3) 상기 MNO 시스템이 MNO 서비스들을 탑재할 수 있다고 검증되었다는 정보 중 하나 이상인 것을 특징으로 하는 MNO 시스템.

청구항 25

통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)에 설치되는 프로그램으로서, 상기 프로그램은,

상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 상기 eUICC 내에 저장하는 기능;

상기 eUICC 인증정보를 상기 MNO 시스템 또는 상기 SM으로 전송하는 기능을 수행할 수 있는 프로그램을 기록한 기록매체.

청구항 26

통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 상기 MNO 시스템 및 SM과 연동되어 있으며, 상기 MNO에 대한

오퍼레이션 프로파일을 관리하는 내장 UICC(eUICC)에 설치되는 프로그램으로서, 상기 프로그램은,

상기 eUICC 제조 단계에서 생성된 eUICC 인증정보를 수신하여 저장하는 기능과, 상기 eUICC 인증정보를 상기 MNO 시스템으로 전송하는 기능과, 상기 MNO 시스템으로부터 전송된 암호화된 상기 오퍼레이션 프로파일을 수신하여 복호화하는 기능을 수행하는 상기 프로그램을 기록한 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 내장 UICC(Embedded Universal Integrated Circuit Card; 이하 'eUICC'라 함)의 인증정보를 이용한 가입(Subscription) 및 MNO(Mobile Network Operator) 변경 방법 및 장치, 그를 위한 내장 UICC 등에 관한 것이다.

배 경 기 술

[0002] UICC(Universal Integrated Circuit Card)는 단말기 내에 삽입되어 사용자 인증을 위한 모듈로서 사용될 수 있는 스마트 카드이다. UICC는 사용자의 개인 정보 및 사용자가 가입한 이동 통신 사업자에 대한 사업자 정보를 저장할 수 있다. 예를 들면, UICC는 사용자를 식별하기 위한 IMSI(International Mobile Subscriber Identity)를 포함할 수 있다. UICC는 GSM(Global System for Mobile communications) 방식의 경우 SIM(Subscriber Identity Module) 카드, WCDMA(Wideband Code Division Multiple Access) 방식의 경우 USIM(Universal Subscriber Identity Module) 카드로 불리기도 한다.

[0003] 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.

[0004] 소형화가 요구되는 단말, 예를 들면 기계 대 기계(Machine to Machine, M2M) 통신을 위한 단말은 UICC를 착탈할 수 있는 구조로 제조할 경우 단말의 소형화가 어려워진다. 그리하여, 착탈할 수 없는 UICC인 eUICC 구조가 제안되었다. eUICC는 해당 UICC를 사용하는 사용자 정보가 IMSI 형태로 수록되어야 한다.

[0005] 기존의 UICC는 단말에 착탈이 가능하여, 단말의 종류나 이동 통신 사업자에 구애받지 않고 사용자는 단말을 개통할 수 있다. 그러나, 단말을 제조할 때부터 제조된 단말은 특정 이동 통신 사업자에 대해서만 사용된다는 전제가 성립되어야 eUICC 내의 IMSI를 할당할 수 있다. 단말을 발주하는 이동 통신 사업자 및 단말 제조사는 모두 제품 재고에 신경을 쓸 수 밖에 없고 제품 가격이 상승하는 문제가 발생하게 된다. 사용자는 단말에 대해 이동 통신 사업자를 바꿀 수 없는 불편이 있다. 그러므로, eUICC의 경우에도 이동 통신 사업자에 구애받지 않고 사용자가 단말을 개통할 수 있는 방법이 요구된다.

[0006] 한편, 최근 eUICC의 도입으로 인하여 여러 이통통신 사업자의 가입자 정보를 원격에서 UICC로 업데이트 할 필요가 생기게 되었고, 그에 따라 가입자 정보 관리를 위한 가입 관리 장치(Subscription Manager; 이하 'SM'이라 함) 또는 프로파일 관리장치(Profile Manager; 이하 'PM'이라 함)가 논의되고 있다.

[0007] 이러한 SM은 주로 eUICC에 대한 정보 관리와, 여러 이동 통신 사업자에 대한 정보 관리와, 이동통신 사업자 변경시 그에 대한 인증 및 원격 정보 변경 등의 기능을 담당하는 것으로 논의되고 있으나, 정확한 기능이나 역할에 대해서는 아직 결정된 바가 없는 실정이다.

[0008] 또한, eUICC 환경에서는 복수의 MNO, SM, 단말 제조사(Device Vendor), USIM 제조사(USIM vendor) 등이 관련되어 있기 때문에, 가입 및 MNO 변경 등의 과정에서 각 엔터티(Entity)들의 신뢰도를 확인할 필요가 있으나 이에 대한 방안이 없는 실정이다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 내장 UICC를 포함하는 통신 환경에서 인증정보를 이용한 가입 및 MNO 변경 방법 및 그를 위한 내장 UICC 장치를 제공한다.

[0010] 본 발명의 다른 목적은 MNO와 SM(SM-SR, SM-DP 포함 가능) 시스템에 의해서 신뢰성있게 인증될 수 있는 eUICC의

인증정보를 eUICC 내부에 미리 설치하는 방법을 제공하는 것이다.

[0011] 본 발명의 다른 목적은 eUICC의 아이덴터티(identity)를 검증 하거나 MNO와 SM들이 신뢰할 수 있는 eUICC인지 여부, 또는 MNO 서비스 수행이 가능한지 사전 증명하기 위한 인증정보를 eUICC 내부에 포함시키는 방법을 제공하는 것이다.

[0012] 본 발명의 다른 목적은 신뢰성 있는 섹터(Trusted sector) 내부의 특정 시스템이 eUICC의 증명을 위한 인증정보를 발급하는 방법을 제공하는 것이다.

[0013] 본 발명의 또다른 목적은 MNO와 SM-SR사이에서 eUICC에 대한 아이덴터티 검증(identity verification)을 수행하기 위한 eUICC 인증정보를 생성하여 미리 eUICC에 저장/관리하는 방법을 제공하는 것이다.

[0014] 본 발명의 다른 목적은 이러한 eUICC 인증정보(eUICC Certification)를 이용하여, 신뢰성 있는 가입 및 MNO 변경(또는 가입 변경) 과정을 수행하는 방법을 제공하는 것이다.

과제의 해결 수단

[0015] 본 발명의 일 실시예는, 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)의 인증방법으로서, 상기 eUICC는 상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 저장하는 단계와, 상기 eUICC는 상기 eUICC 인증정보를 상기 MNO 시스템 또는 상기 SM으로 전송하는 단계를 포함하는 eUICC 인증방법을 제공한다.

[0016] 본 발명의 다른 실시예는 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서, 상기 eUICC는 상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate) 및 카드 OS 정보와 카드 플랫폼 정보, PIN(Personal Identification Number) 정보 중 하나 이상을 포함하는 eUICC 인증 프로파일을 저장하고, 상기 eUICC 인증 프로파일은 상기 eUICC 인증정보를 상기 MNO 시스템 또는 상기 SM으로 전송하는 eUICC를 제공한다.

[0017] 본 발명의 다른 실시예는 통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 상기 MNO 시스템 및 SM과 연동되어 있는 내장 UICC(eUICC)로서, 상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 포함하는 eUICC를 이용하는 프로비저닝 방법으로서, 상기 eUICC는 eUICC 제조 단계에서 생성된 상기 eUICC 인증정보를 수신하여 저장하는 단계와, 상기 eUICC는 상기 eUICC 인증정보를 상기 MNO 시스템으로 전송하는 단계와, 상기 MNO 시스템은 상기 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증하는 단계와, 상기 MNO 시스템은 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 단계를 포함하는 프로비저닝 방법을 제공한다.

[0018] 본 발명의 다른 실시예는, 통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 상기 MNO 시스템 및 SM과 연동되어 있는 내장 UICC(eUICC)로서, 상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 포함하는 eUICC를 이용하는 MNO 변경 방법으로서, 상기 eUICC는 eUICC 제조 단계에서 생성된 상기 eUICC 인증정보를 수신하여 저장하는 단계와, 상기 eUICC는 상기 eUICC 인증정보를 리시빙 MNO 시스템으로 전송하는 단계와, 상기 리시빙 MNO 시스템은 상기 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증하는 단계와, 상기 리시빙 MNO 시스템은 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 단계, 및 상기 eUICC는 MNO 변경 사실을 상기 리시빙 MNO 시스템 및 도너 MNO 시스템에게 통지하는 단계를 포함하는 MNO 변경 방법을 제공한다.

[0019] 본 발명의 다른 실시예는, 사업자 시스템(MNO), 가입 관리 시스템(Subscription Manager; SM)을 구성하는 SM-SR(Secure Routing) 및 SM-DP(Data Preparation) 장치와 연동된 내장 UICC(eUICC)를 이용한 프로비저닝 방법으로서, 상기 eUICC가 eUICC 제조사 시스템 또는 단말 제조사 시스템으로부터 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 수신하여 상기 eUICC 내에 저장하는 단계와, 가입자의 개통요청에 따라 상기 활성화 요청 또는 개통 요청 메시지를 상기 MNO 시스템으로 전송하는 단계와, 상기 MNO 시스템이 상기 eUICC으로부터 상태 요청 및 기술성능 제어 확인을 수행하면서, 상기 eUICC로부터 상기 eUICC 인증정보를 수신하는 단계와, 상기 MNO 시스템이 상기 SM-SR로부터 단말 관련 정보를 수집하는 과정 중에 상기 eUICC 인증정보를 SM-SR로 전송하는 단계, 및 상기 MNO 시스템 또는 상기 SM-SR가 상기 eUICC 인증정보를 통한 eUICC 검증이 된 경우에 한하여, 상기 MNO 시스템이 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 단계를 포함하는 프로비저닝 방법을 제공한다.

[0020] 본 발명의 다른 실시예는, 사업자 시스템(MNO), 가입 관리 시스템(Subscription Manager; SM)을 구성하는 SM-

SR(Secure Routing) 및 SM-DP(Data Preparation) 장치와 연동된 내장 UICC(eUICC)를 이용한 MNO 변경 방법으로서, 상기 eUICC가 eUICC 제조사 시스템 또는 단말 제조사 시스템으로부터 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 수신하여 상기 eUICC 내에 저장하는 단계와, MNO 변경요청에 따라 상기 eUICC가 활성화 요청 또는 개통 요청 메시지를 리시빙 MNO 시스템으로 전송하는 단계와, 상기 리시빙 MNO 시스템이 상기 eUICC으로부터 상태 요청 및 기술성능 제어 확인을 수행하면서, 상기 eUICC로부터 상기 eUICC 인증정보를 수신하는 단계와, 상기 리시빙 MNO 시스템이 상기 SM-SR로부터 단말 관련 정보를 수집하는 과정 중에 상기 eUICC 인증정보를 SM-SR로 전송하는 단계와, 상기 리시빙 MNO 시스템이 도너 MNO 시스템과 MNO 변경을 위한 협상 및 권리이전을 수행하는 단계, 및 상기 리시빙 MNO 시스템 또는 상기 SM-SR가 상기 eUICC 인증정보를 통한 eUICC 검증이 된 경우에 한하여, 상기 리시빙 MNO 시스템이 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 단계를 포함하는 MNO 변경 방법을 제공한다.

[0021] 본 발명의 다른 실시예는, 통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 상기 MNO 시스템 및 SM과 연동되어 있으며, 상기 MNO에 대한 오퍼레이션 프로파일을 관리하는 내장 UICC(eUICC)로서, 상기 eUICC는 eUICC 제조 단계에서 생성된 eUICC 인증정보를 수신하여 저장하고, 상기 eUICC 인증정보를 상기 MNO 시스템으로 전송하며, 상기 MNO 시스템으로부터 전송된 암호화된 상기 오퍼레이션 프로파일을 수신하여 복호화하는 eUICC를 제공한다.

[0022] 본 발명의 다른 실시예는 가입 관리시스템(SM) 및 내장 UICC(eUICC)와 연동된 MNO 시스템으로서, 상기 MNO 시스템은 프로비저닝 또는 MNO 변경 과정에서, 상기 eUICC로부터 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 수신하고, 상기 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증한 후, 자신의 오퍼레이션 프로파일을 암호화하여 상기 eUICC로 전송하는 MNO 시스템을 제공한다.

[0023] 본 발명의 다른 실시예는, 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)에 설치되는 프로그램으로서, 상기 프로그램은, 상기 MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 상기 eUICC 내에 저장하는 기능 및 상기 eUICC 인증정보를 상기 MNO 시스템 또는 상기 SM으로 전송하는 기능을 수행할 수 있는 프로그램을 기록한 기록매체를 제공한다.

[0024] 본 발명의 또다른 실시예는, 통신사업자(MNO) 시스템, 가입 관리시스템(SM) 및 상기 MNO 시스템 및 SM과 연동되어 있으며, 상기 MNO에 대한 오퍼레이션 프로파일을 관리하는 내장 UICC(eUICC)에 설치되는 프로그램으로서, 상기 프로그램은, 상기 eUICC 제조 단계에서 생성된 eUICC 인증정보를 수신하여 저장하는 기능과, 상기 eUICC 인증정보를 상기 MNO 시스템으로 전송하는 기능과, 상기 MNO 시스템으로부터 전송된 암호화된 상기 오퍼레이션 프로파일을 수신하여 복호화하는 기능을 수행하는 상기 프로그램을 기록한 기록매체를 제공한다.

도면의 간단한 설명

[0025] 도 1은 본 발명이 적용되는 eUICC를 포함한 전체 서비스 아키텍처를 도시한다.

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

도 3은 본 발명의 일 실시예에 의한 프로비저닝 과정의 전체 흐름도이다.

도 4는 본 발명의 일 실시예에 의한 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.

도 5는 본 발명이 적용되는 전체시스템 및 eUICC의 내부 구성을 도시한다.

도 6은 본 발명의 일실시예에 의한 eUICC 인증정보를 이용한 최초 프로비저닝(Provisioning) 과정을 도시한다.

도 7은 본 발명의 일실시예에 의한 eUICC 인증정보를 이용한 MNO 변경 과정을 도시한다.

도 8은 본 발명의 다른 실시예에 의한 eUICC 인증정보를 이용한 프로비저닝 과정을 도시한다.

도 9는 본 발명의 다른 실시예에 의한 eUICC 인증정보를 이용한 MNO 변경 과정을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0026] 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 구

체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0027] 현재 GSMA에서 활발하게 논의되는 M2M(Machine-to-Machine) 단말은 특성상 크기가 작아야 하는데, 기존 UICC를 사용하는 경우에는, M2M 단말에 UICC를 장착하는 모듈을 별도 삽입해야 하므로, UICC를 탈착가능한 구조로 M2M 단말을 제조하게 되면, M2M 단말의 소형화가 힘들게 된다.

[0028] 따라서, UICC 착탈이 불가능한 내장(Embedded) UICC 구조가 논의되고 있는데, 이때 M2M 단말에 장착되는 eUICC에는 해당 UICC를 사용하는 이동통신 사업자(Mobile Network Operator; 이하 'MNO'라 함)정보가 국제 모바일 가입자 식별자(International Mobile Subscriber Identity, IMSI) 형태로 UICC에 저장되어 있어야 한다.

[0029] 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.

[0030] 이와 같이, 기존의 착탈식 형태의 SIM과는 달리 단말에 일체형으로 탑재되는 eUICC 또는 eSIM은 그 물리적 구조 차이로 인해 개통 권한, 부가 서비스 사업 주도권, 가입자 정보 보안 등에 대한 많은 이슈들이 존재한다. 이를 위해 GSMA 및 ETSI의 국제 표준화 기관에서는 사업자, 제조사, SIM 제조사 등의 유관 회사들과 최상위 구조를 포함한 필요한 요소에 대해 표준화 활동을 전개하고 있다. eSIM이 표준화 단체들을 통해 논의되면서 이슈의 중심에 있는 것은 Subscription Manager라고 불리는 SM으로 사업자 정보 (Operator Credential, MNO Credential, Profile, eUICC Profile, Profile Package 등 다른 표현으로 사용될 수 있음)를 eSIM에 발급하고 가입(Subscription) 변경 또는 MNO 변경에 대한 프로세스를 처리하는 등 eSIM에 대한 전반적인 관리 역할을 수행하는 개체 또는 그 기능/역할을 의미한다.

[0031] 최근 GSMA에서는 SM의 역할을 사업자 정보를 생성하는 역할을 수행하는 SM-DP (Data Preparation)과 eSIM에 사업자 정보의 직접적 운반을 수행하는 SM-SR (Secure Routing)로 분류한 구조와, 프로파일을 암호화하여 전송하는 방안을 제안하였으나 세부적인 내용이 부족하다.

[0032] 또한, eUICC 환경에서는 복수의 MNO, SM, 단말 제조사(Device Vendor), USIM 제조사(USIM vendor) 등이 관련되어 있기 때문에, 가입 및 MNO 변경 등의 과정에서 eUICC가 MNO와 SM들이 신뢰할 수 있는 eUICC인지 여부, 또는 MNO 서비스 수행이 가능한지 등을 검증할 필요가 있다.

[0033] 본 명세서에서는 eSIM과 eUICC를 동등한 개념으로 사용한다.

[0034] 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.

[0035] 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.

[0036] 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.

[0037] GSMA에서는 SM의 역할을 SM-DP와 SM-SR로 분류할 수 있다. 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.

[0038] 그리고 아래 도 1의 "신뢰 서클(Circle of Trust)"이라는 구조를 제안하여 각 유사 개체 또는 엔터티 들간에 신뢰 관계의 중첩을 통해 MNO와 eSIM 간의 엔드-투-엔드(End-to-End) 신뢰 관계를 구축한다는 개념을 제안하였

다. 즉, MNO1는 SM1과, SM1은 SM4, SM4는 eSIM과 신뢰관계를 형성하여, 이를 통해 MNO와 eSIM 간의 신뢰관계를 형성한다는 개념이다.

[0039] 본 발명을 설명하기 전에 우선 본 명세서에서 사용할 용어에 대하여 설명한다.

[0040] MNO(Mobile Network Operator)는 이동통신 사업자를 의미하며, 모바일 네트워크를 통해 고객에게 통신 서비스를 제공하는 엔터티를 의미한다.

[0041] SM(Subscription manager)는 가입 관리 장치로서, eUICC의 관리 기능을 수행한다.

[0042] eUICC 공급자(eUICC Supplier)는 eUICC 모듈과 내장 소프트웨어(펌웨어와 오퍼레이팅 시스템 등)를 공급하는 자를 의미한다.

[0043] 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.

[0044] 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.

[0045] 가입(Subscription)은 가입자와 무선통신 서비스 제공자 사이의 서비스 제공을 위한 상업적인 관계를 의미한다.

[0046] 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.

[0047] 프로파일 엑세스 크레덴셜(Profile access credentials)은 프로파일 내부 또는 eUICC 내부에 존재하는 데이터로서, 프로파일 구조 및 그 데이터를 보호 또는 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 데이터를 의미한다.

[0048] 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.

[0049] 오퍼레이션 프로파일(Operation Profile) 또는 사업자 정보는 사업자 가입(Operational Subcription)과 관련된 모든 종류의 프로파일을 의미한다.

[0050] 도 1은 본 발명이 적용될 수 있는 eSIM(eUICC)을 포함한 전체 서비스 아키텍처를 도시한다.

[0051] 전체 시스템에 대해서 설명하면 다음과 같다. 그러나 본 발명이 도 1과 같은 시스템에 한정되어 적용되는 것은 아니며, 본 발명의 사상에 따라 eUICC를 포함하는 시스템에서 eUICC를 인증할 수 있는 인증정보를 이용할 수 있는 한 그 형태에 제한이 있는 것은 아니다.

[0052] 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.

[0053] 도 1에서 점선은 신뢰 서클(Circle of Trust)을 도시하고, 2개 실선은 안전한 링크를 의미한다.

[0054] 가입정보가 저장되어 전달되는 시나리오가 필요하며, 이러한 시나리오는 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.

[0055] 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.

[0056] 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.

[0057] MNO 크레덴셜 또는 프로파일은 K, 알고리즘, 알고리즘 파라미터, 부가 서비스 어플리케이션, 부가 서비스 데이

터 등을 포함하는 가입 크레덴셜을 의미할 수 있다.

[0058] 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.

[0059] 오퍼레이터는 자신의 크레덴셜에 대해서 완전한 제어권을 가져야 하며, 오퍼레이터는 SM 오퍼레이션에 대해서 강한 감독권과 제어권한을 가져야 한다.

[0060] SM 기능은 MNO 또는 제3 기관에 의하여 제공되어야 하며, 만약 제3 기관에 의하여 제공된다면 SM과 MNO 사이에는 상업적인 관계가 설정되어 있는 경우 등일 것이다.

[0061] 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.

[0062] 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.

[0063] 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.

[0064] SM의 역할은 SM-SR, SM-DP와 같은 2개의 서브 기능으로 나뉘어 질 수 있다.

[0065] 실제로, 이러한 SM-SR, SM-DP 기능들은 다른 엔터티에 의하여 제공될 수도 있고, 동일한 엔터티에 의해서 제공될 수도 있다. 따라서, SM-DP와 SM-SR의 기능을 명확하게 경계지을 필요가 있고, 이들 엔터티들 사이의 인터페이스를 정의할 필요가 있다.

[0066] 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.

[0067] 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, 스캐러빌러티(Scalability) 및 신뢰도에 대한 요구사항이 중요할 것으로 예상된다.

[0068] 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.

[0069] 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.

[0070] 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 엔

드-투-엔드 링크가 필요하다.

[0071] 즉, 도 1에서 110은 SM들 끼리, 더 구체적으로는 SM-SR 멤버 사이에 형성되는 신뢰 서클을 나타내고, 120은 MNO 파트너들의 신뢰 서클이며, 130은 엔드투엔드 신뢰 링크를 도시한다.

[0072] 도 2는 SM 분리 환경에서 SM-SR 및 SM-DP가 시스템에 위치하는 구성을 도시한다.

[0073] 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.

[0074] 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)

[0075] 도 3은 본 발명이 적용될 수 있는 도 1과 같은 시스템에서 제1차 가입 또는 프로비저닝 과정의 전체 흐름도이다.

[0076] 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)

[0077] S330단계에서 MNO는 SM-SR과 사이에서 단말(Device) 또는 eUICC에 대한 정보를 수집한다(eUICC identity verification 및 collect information about device). S330단계에서, MNO는 해당 eUICC에 대한 암호화 키, 구체적으로는 eUICC에 대응되는 공개키 등을 SM-SR로부터 획득할 수 있다. 이러한 암호화키는 프로파일을 암호화하여 eUICC로 전달하기 위한 것으로서, 반드시 공개키에 한정되는 것은 아니며, 기타 대칭키 방식에 의한 키가 사용될 수도 있을 것이다.

[0078] 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.

[0079] 동적인 암호키 획득방법은, MNO로부터 요청(특정 eUICC 식별정보 포함)이 있는 경우, SM-SR은 해당되는 eUICC에게 공개키 전송을 요청하고, 해당 eUICC는 eUICC 탑재 단말 내의 발급 처리 모듈(이 용어에 한정되지 않으며, 통신모듈, 프로비저닝 모듈, 발급 모듈, 개통 모듈 등으로 칭할 수 있으며, eUICC 프로비저닝을 위한 eUICC 탑재 단말 외부와의 통신 및 프로비저닝 관리의 역할을 수행함) 또는 eUICC 내의 보안모듈(암호키 생성 모듈, 암호키 처리 모듈, Security Policy 모듈, Credential Manager, Profile Manager 등 eUICC 내의 암호키 생성 및 암호키를 활용한 보안 연산을 수행하는 모듈)을 이용하여 공개키를 생성한 후 SM-SR로 전달하는 방식으로 수행될 수 있다.

[0080] 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.

[0081] 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.

[0082] 물론, 이러한 프로파일의 생성 및 eUICC 공개키를 이용한 암호화가 반드시 SM-DP에 의하여 수행될 필요는 없으며, MNO 시스템이 자체적으로 수행할 수도 있을 것이다.

[0083] 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)

[0084] 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.

[0085] 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.

[0086] S370 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.

[0087] 이러한 각 단계에 대한 주요 구성을 추가로 설명하면 다음과 같다.

[0088] S310단계에서, eUICC 식별 정보(eICCid 등)는 공개된 데이터이며 eUICC 내부에 통합 보호되어야 한다.

[0089] S320, S330단계에서 상태 요청 및 기술적 가능성 제어는 eUICC 아이덴터티의 증명을 제공(신뢰할 수 있는 eUICC)하며, MNO 서비스를 위한 eUICC 특성의 적격성을 확인할 수 있어야 한다.

[0090] 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.

[0091] S370 단계에서, SM-SR 데이터베이스는 가입 설치(Subscription installation)의 마무리 단계에서 업데이트 될 수 있다.

[0092] 도 4는 본 발명이 적용될 수 있는 시스템에서의 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.

[0093] 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’)

[0094] 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.

[0095] 도 4에 의한 MNO 변경 과정을 구체적으로 설명하면 다음과 같다.

[0096] 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)

[0097] S430단계에서 리시빙 MNO는 SM-SR과 사이에서 eUICC 아이덴터티 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.

[0098] 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.

[0099] 동적인 암호키 획득방법은 도 3과 관련하여 설명한 바와 동일하므로, 중복을 피하기 위하여 설명을 생략한다.

[0100] 해당 eUICC의 공개키(암호키)를 획득한 리시빙 MNO는 SM-DP를 통해서 MNO에 맞는 새로운 eUICC 프로파일을 생성하고 그 프로파일을 획득한 eUICC 공개키(암호키)로 암호화한 후 MNO로 전달한다.(1차 암호화, S440 단계) 이때, 인증성(Authenticity)을 제공하기 위해 SM-DP는 자신의 개인키로 추가적인 전자서명을 생성할 수 있다. 즉, S440 단계에서 SM-DP는 인증을 위한 자신의 개인키 또는 비밀키로 프로파일을 전자서명(Sign)할 수 있다.

[0101] 또한, S440 단계 이전 또는 이후에 협상 및 권리 전송 단계(S440’)가 수행될 수 있다. 이러한 협상 및 권리 전

송 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.

[0102] 즉, S440' 단계에서는 새로운 MNO(Receiving MNO)가 가입 스위칭 또는 MNO 변경에 대해서 통지한 후 도너 MNO의 인증을 요청하며, 이러한 인증은 정책 제어 기능(Policy Control Function)에 의해서 제공될 수 있다.

[0103] 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)

[0104] 그런 다음, MNO는 이중 암호화(Double Ciphered)된 eUICC 프로파일을 해당 eUICC로 전송한다.(S460 단계) 이때, 인증성을 제공하기 위해 SM-DP의 공개키 또는 인증서(Certification)를 함께 eUICC로 전송할 수 있다.

[0105] eUICC는 이미 eUICC 관리키를 알고 있으므로 1차로 복호화한 후, 자신 공개키에 대응되는 비밀키(제조 또는 공개키 동적 생성 단계에서 이미 알고 있음)를 이용하여 2차 복호화함으로써 MNO 변경에 사용될 프로파일을 완전히 복호화 할 수 있다. 이때, eUICC는 인증서 확인 (MNO로부터 획득한 공개키에 해당되는 SM-DP로부터 생성된 eUICC 프로파일인지 확인하기 위해)을 위해 SM-DP의 공개키 (인증서의 경우, 신뢰할 수 있는 제 3의 개체로부터 해당 인증서의 유효성을 검증 받을 수 있음)로 서명 검증을 수행할 수 있다.

[0106] S470 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.

[0107] 한편, 이와 같이 eUICC, 다수의 MNO 시스템 및 SM 등이 관련된 시스템에서 프로비저닝 또는 MNO 변경과 같은 절차를 수행하는 과정에서, eUICC의 ID만 확인하고 필요한 프로파일 등을 암호화하여 안전하게 전달하는 방안만 논의되고 있을 뿐, 해당 eUICC가 신뢰할 수 있는 엔터티인지 여부를 확인하기 위해서 eUICC의 아이덴터티를 검증(Verification) 또는 인증하는 절차가 필요할 수도 있다.

[0108] 따라서, 본 발명의 일 실시예에서는, 이러한 eUICC 시스템 아키텍처 하에서, MNO 시스템 또는 SM이 상기 eUICC의 아이덴터티를 검증(Verification)할 수 있는 eUICC 인증 정보(eUICC Certificate)를 저장하고, 프로비저닝 또는 MNO 변경 과정에서 eUICC 인증정보를 MNO 시스템 또는 SM으로 전송할 수 있다. MNO 시스템 또는 SM은 수신한 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증하고, 검증된 경우에 한하여 MNO 오퍼레이션 프로파일을 암호화하여 eUICC로 전송한다.

[0109] 이 때, eUICC 인증정보는, 1) 상기 eUICC의 하드웨어 및 카드 OS, 플랫폼 중 하나에 대하여 검정되었다는 정보, 2) 상기 MNO 시스템 및 SM이 신뢰할 수 있는 eUICC로 사전 검정되었다는 정보 및 3) 상기 MNO 시스템이 MNO 서비스들을 탑재할 수 있다고 검증되었다는 정보 등이 될 수 있으며, 그 구체적인 형태나 형식에는 제한이 없다.

[0110] 다시 설명하면, 도 1 내지 4와 같은 종래의 방식에서는 MNO를 변경 요청 받은 리시빙(Receiving) MNO가 변경 요청한 eUICC의 아이덴터티 검증(identity verification)을 위한 정보, 즉 eUICC 인증정보 및 단말(device)에 대한 정보들을 SM(구체적으로는 SM-SR)로부터 가져 온다. 그리고 최종적으로 가입자 변경을 도너(Donor) MNO에게 통지 하는 형태 인데, 이를 위해서는 도너 MNO에 가입되어 있는 eUICC가 리시빙 MNO로 변경을 요청하면 리시빙 MNO와 관련된 SM-SR이 사전에 해당 eUICC의 아이덴터티를 검증할 수 있는 정보나 단말 정보들을 모두 알아야 한다. 이렇게 하기 위해서는 수많은 SM-SR들이 해당 정보들을 모두 공유해야 하는 문제점이 있다.

[0111] 이러한 문제점을 극복하기 위하여, 본 발명의 일 실시예에서는 MNO 또는 SM이 특정 eUICC를 인증할 수 있는 정보, 즉 eUICC 인증정보를 사전에 혹은 동적으로 eUICC내에 저장하며, 이러한 eUICC 인증정보는 MNO와 SM들이 신뢰할 수 있는 eUICC인지 여부 또는 MNO 제공하는 서비스들에 해당 eUICC가 적합한지 등에 대한 증명 정보로서, 도 1과 같은 신뢰 서클(Circle of Trust) 내부의 임의의 엔터티가 발급할 수 있다.

[0112] 도 5는 본 발명의 일 실시예에 의한 전체 시스템의 구성을 도시한다.

[0113] 도 5와 같이, 본 발명의 일 실시예에 의한 전체 시스템은 단말(Device; 510) 및 그 내부에 장착되는 eUICC(520)와, 외부의 다수의 MNO 시스템 및 SM-SR, SM-예로 구성된 신뢰 섹터(Trusted Sector by MNO)로 구성된다.

[0114] 도 5와 같이, 각 섹터는 MNO(들)에 의하여 강한 신뢰 관계로 형성되며, 도 5의 점선은 강한 신뢰 관계(Strong trust relationship)임을 나타낸다.

[0115] SM-SR은 MNO들이 직접 운영을 하거나 강한 신뢰(strong trust)관계로 MNOs들과 TSM 형태로 MNOs 네트워크 내부에서 운영될 수 있다. SM-SR 들 사이에도 신뢰 관계(trust relationship) 가 형성되어 있고 SM-SR은 여러 개의

MNO 들와 관련되어 있을 수 있다. SM-SR은 실제 가입요청을 처리하며 MNO 프로파일을 eUICC에 OTA로 로딩(loading)하는 주체이다.

[0116] SM-DP(Subscription Manager ? Data Preparation)는 MNO 들이 직접 운영 하거나 강한 신뢰 관계로 MNOs들과 TSM 형태로 MNOs 네트워크 내부에서 운영될 수 있다. (하지만, 가급적 MNOs들이 직접 운영하는 것이 바람직하다) SM-DP는 MNO 프로파일을 생성, 저장, 관리 한다.

[0117] 이 때, 본 발명의 일 실시예에 의한 eUICC 내부 구조는 도 5의 왼쪽 그림인 바, 본 발명의 실시예에서는 eUICC 인증 정보(eUICC Certification) 및 eUICC 인증 프로파일(Certification Profile)을 새로이 정의하며, 반드시 이러한 용어에 한정되는 것은 아니며, 아래와 같은 의미를 가지는 한 다른 용어로 표현될 수도 있을 것이다.

[0118] 인증 프로파일(eUICC Certification Profile)은 eUICC 내부에서 보안 및 eUICC 인증정보(certification)를 관리 할 수 있는 모듈이다.

[0119] 본 발명의 실시예에서는 eUICC 인증 정보(eUICC Certification)는 카드 OS(Operating System) 정보, 카드 플랫폼 정보 등과 같은 공통정보(Common Information)에 포함될 수 있는 정보로서, 아래와 같은 정보들을 포함할 수 있다.

[0120] 1) eUICC의 하드웨어 및 카드 OS, 카드 Platform 등에 대해서 검증되었다는 정보

[0121] 2) 기타, MNO와 SM들이 신뢰할 수 있는 eUICC인지를 사전 검증하였다는 정보

[0122] 3) MNO 서비스들을 탑재하는데 문제가 없는 소프트웨어들로 구성이 되었다고 검증된 정보 등

[0123] 즉, 본 발명의 실시예에서는 eUICC 인증 정보(eUICC Certification)는 MNO와 SM-SR사이에서 특정한 eUICC에 대한 아이덴터티 검증(identity verification)을 수행 할 수 있는 모든 정보를 의미한다.

[0124] 이러한 eUICC 인증정보를 이용하면, 가입자가 MNO 변경 시 모든 서로 다른 SM-SR간의 eUICC 검증 정보를 공유해야 하는 오버헤드를 없애 주고 보다 보안이 보장 되는 eUICC 메커니즘을 제공 할 수 있다.

[0125] 한편, 본 명세서에서 PIN(Personal Identification Number)은 선택적으로 사용되는 정보로서, 비밀번호를 의미하며, 상기 인증 프로파일 내에 선택적으로 포함될 수 있다.

[0126] 즉, 도 5의 왼쪽 그림과 같이, 본 발명의 일 실시예에 의한 인증 프로파일(521)은 카드 OS(Operating System) 정보, 카드 플랫폼 정보, eUICC 인증 정보 및 PIN 중 하나 이상을 선택적으로 포함하는 프로파일로서, eUICC 내에 구현되어 있다.

[0127] 다시 설명하면, 본 발명의 일 실시예에 의한 eUICC 인증정보는 공통정보(Common Information) 중의 하나로서 eUICC 인증 프로파일 형태로 저장될 수 있으며, 공통정보에는 상기 eUICC 인증정보 이외에도 카드 OS 및 플랫폼 정보와, eUICC 하드웨어 정보 및 PIN 정보 등을 포함할 수 있다.

[0128] 도 6은 본 발명의 일실시예에 의한 eUICC 인증정보를 이용한 최초 프로비저닝(Provisioning) 과정을 도시한다.

[0129] 도 6에 의하면,

[0130] 우선, 프리-프로비저닝(Pre-Provisioning) 또는 프로비저닝 과정에서, eUICC 또는 USIM 제조사 시스템은 신뢰 섹터내의 일정 엔터티로부터 eUICC 하드웨어 & 소프트웨어에 대한 eUICC 인증정보(certificate)를 발급받아 기타 카드 OS 및 eUICC 하드웨어 정보와 함께 eUICC 내에 탑재한다.(S610)

[0131] 다음으로 S620 단계에서, 단말 제조사(Device Vendor)에게 eUICC인증정보가 포함된 eUICC를 제공하여 단말에 장착하도록 한다.

[0132] 그러면 S630 단계와 같이, 본 발명의 일 실시예에 의한 eUICC 인증정보가 다른 공통정보(Common Info.)와 함께 eUICC 인증 프로파일 형태로 eUICC 내부에 저장된다.

[0133] 그런 다음 가입자가 해당 단말을 구입하여 MNO1 시스템으로 개통 또는 프로비저닝을 요청한다.(S640) 이 때, 요청은 사전 탑재된 도 5와 같은 프로비저닝 프로파일(Provisioning Profile)을 통해 MNO1 네트워크로 전송될 수도 있으나, 오프라인 혹은 별도로 온라인(전용선)을 사용할 수 도 있다.

[0134] 가입 또는 프로비저닝 요청이 있는 경우, eUICC는 eUICC 인증 프로파일을 이용하여 카드 OS 정보, 카드 플랫폼 정보, eUICC 하드웨어 정보, eUICC 인증 정보 및 PIN 정보 중 하나 이상을 포함하는 공통정보를 MNO1 시스템으로 제공 한다.(S650) 한편, S650 단계에서 eUICC는 프로파일을 암호화할 수 있는 암호화키를 함께 제공할 수 있

으며, 이러한 암호화키는 eUICC 공개키, MNO 프로파일 키 등일 수 있다, 이러한 암호화키는 추후 MNO가 자신의 프로파일을 1차 암호화하여 전송할 때 사용하는 것으로서 그 형태에는 제한이 없을 것이다.

[0135] 그러면, S660단계에서 MNO1 시스템은 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증하고, 각종 공통정보들을 확인한 후, 검증된 경우에 한해서 SM-SR1으로부터 MNO1 OTA 키를 제공 받는다. MNO OTA 키는 전술한 S650 단계에서 제공된 암호화키에 이어서 2차 암호화할 때 사용되는 것으로서, 다른 표현 또는 형태일 수도 있을 것이다.

[0136] 그러면, MNO1 시스템은 SM-DP1를 통해 MNO1 프로파일(Profile)을 생성하고 S650 과정에 수신한 MNO1 프로파일 키로 해당 MNO1 프로파일을 1차 암호화(S670)하며, MNO1 시스템은 자체적 또는 SM-SR1을 통해서 MNO1 OTA 키로 MNO1 프로파일을 다시 암호화(ciphering), 즉 2차 암호화 한다(S680). 즉 MNO1 프로파일을 이중 암호화(Double Ciphering)한다.

[0137] MNO1 시스템은 이중 암호화(Double ciphered)된 MNO1 프로파일을 OTA 형태로 eUICC에게 전송한다(S690).

[0138] 이로써, 프로비저닝 과정이 종료되며, 이 과정에서 MNO1는 eUICC 인증정보를 이용하여 해당 eUICC를 검증(Verification)할 수 있게 되는 것이다.

[0139] 도 7은 본 발명에 의한 eUICC 인증 정보 및 인증 프로파일을 이용하여, MNO 변경을 수행하는 과정을 도시한다.

[0140] 우선, 가입자가 SM-SR1의 MNO1에서 SM-SR2의 MNO3으로 가입 변경을 하는 경우로 가정한다.

[0141] 그런 다음 가입자가 변경후의 리시빙 MNO 시스템인 MNO3 시스템으로 가입 변경 또는 MNO 변경을 요청한다.(S710) 이 때, 요청은 사전 탑재된 도 5와 같은 프로비저닝 프로파일(Provisioning Profile)을 통해 MNO3 네트워크로 전송될 수도 있으나, 오프라인 혹은 별도로 온라인(전용선)을 사용할 수 도 있다.

[0142] 가입 변경 또는 MNO 변경 요청이 있는 경우, eUICC는 eUICC 인증 프로파일을 이용하여 카드 OS 정보, 카드 플랫폼 정보, eUICC 하드웨어 정보, eUICC 인증 정보 및 PIN 정보 중 하나 이상을 포함하는 공통정보를 리시빙 MNO인 MNO3 시스템으로 제공 한다.(S720) 물론, S650 단계에서와 같이 S720 단계에서도 eUICC가 프로파일을 암호화할 수 있는 암호화키를 함께 제공할 수 있으며, 이러한 암호화키는 eUICC 공개키, MNO 프로파일 키 등일 수 있다, 이러한 암호화키는 추후 MNO가 자신의 프로파일을 1차 암호화하여 전송할 때 사용하는 것으로서 그 형태에는 제한이 없을 것이다.

[0143] 그러면, S730단계에서 리시빙 MNO3 시스템은 eUICC 인증정보를 이용하여 해당 eUICC의 아이덴터티를 검증하고, 각종 공통정보들을 확인한 후, 검증된 경우에 한해서 SM-SR2로부터 MNO3 OTA 키를 제공 받는다(S730). MNO OTA 키는 전술한 S720 단계에서 제공된 암호화키에 이어서 2차 암호화할 때 사용되는 것으로서, 다른 표현 또는 형태일 수도 있을 것이다.

[0144] 그러면, 리시빙 MNO3 시스템은 SM-DP3을 통해 MNO3 프로파일(Profile)을 생성하고 S720 과정에 수신한 암호화키로 해당 MNO3 프로파일을 1차 암호화(S740)하며, MNO3 시스템은 자체적 또는 SM-SR2를 통해서 MNO3 OTA 키로 MNO3 프로파일을 다시 암호화(ciphering), 즉 2차 암호화 한다(S750). 즉 MNO1 프로파일을 이중 암호화(Double Ciphering)한다.

[0145] 리시빙 MNO3 시스템은 이중 암호화(Double ciphered)된 MNO3 프로파일을 OTA 형태로 eUICC에게 전송한다(S760).

[0146] 다음으로, eUICC는 도너 MNO인 MNO1로부터 리시빙 MNO3로 가입 변경이 완료되었다는 메시지를 도너 MNO1 및 리시빙 MNO3로 통지하며, 도너 MNO1 및 리시빙 MNO3는 해당 eUICC의 eUICC 인증정보를 이용하여 eUICC 아이덴터티의 변경 확인 및 eUICC를 최종 검증함으로써, 최종 MNO 변경 사실을 서로 확인한다.(S770) 또한, S770 단계에서 eUICC는 내부에 있는 도너 MNO의 프로파일을 비활성화 또는 삭제하고, 리시빙 MNO 프로파일을 활성화시킨다.

[0147] 이러한 과정을 통함으로써, MNO 시스템 또는 SM은 각종 프로파일을 eUICC로 전송하기 전에 해당 eUICC의 아이덴터티를 검증할 수 있게 되므로, eUICC의 신뢰성을 담보할 수 있게 된다.

[0148] 도 8 및 도 9의 실시예는 본 발명에 의한 eUICC 인증정보를 이용한 프로비저닝 및 MNO 변경 과정을 도 3 및 4에 도시된 방식에 적용한 경우이다.

[0149] 도 8은 본 발명의 다른 실시예에 의한 eUICC 인증정보를 이용한 프로비저닝 과정을 도시한다.

[0150] 도 8은 프로비저닝 과정에서 본 발명의 일 실시예에 의한 eUICC 인증정보를 활용하는 예를 도시하며, 우선 단말

제조 또는 eUICC 제조 단계에서 단말 제조사 또는 eUICC 제조사는 신뢰 서클(Circle of Trust) 내의 특정 엔터티로부터 해당 eUICC의 인증정보를 수신(S810)한 후, 해당 eUICC 내에 저장한다(S820) 이 때, eUICC 인증정보를 생성 또는 발급하는 신뢰 서클 내부의 엔터티는 단말 제조사 시스템, eUICC 제조사 시스템, MNO 시스템, SM 등이 될 수 있으나, 그에 한정되는 것은 아니며 기타 다른 인증기관이 사용될 수도 있을 것이다.

[0151] 가입자가 해당 eUICC가 장착된 단말 또는 기기를 구입한 후 개통을 요청(S830)하면, eUICC는 IMEI 및 eICCid를 포함하는 활성화 요청 또는 개통 요청 메시지를 해당 MNO1 시스템으로 전송한다(Request activation; S840)

[0152] 그러면, 해당 MNO1 시스템은 해당 eUICC 사이에서 eUICC 상태 요청(Status Request) 및 기술 성능 제어(Technical Capability Control) 확인을 수행함과 동시에, 해당 eUICC로부터 eUICC 인증 정보를 획득한다(eUICC status request 및 technical capability control; S850)

[0153] MNO1은 SM-SR로부터 해당 단말(Device) 또는 eUICC와 관련된 정보를 수집하는 과정에서, 상기 S850 단계에서 획득한 eUICC 인증정보를 SM-SR로 전송하여 eUICC 아이덴터티를 검증(Identity Verification)하게 된다.(eUICC identity verification 및 collect information about device ; S860)

[0154] 그 이후의 프로비저닝 과정은 도 3의 S340 내지 S370 단계와 유사하게 진행될 수 있다.

[0155] 즉, eUICC 인증정보를 통해서 해당 eUICC의 아이덴터티가 검증된 경우에 한하여, MNO1 시스템은 SM-DP를 통해서 프로파일을 생성한 후 암호화키(eUICC 공개키 등)로 1차 암호화하고, SM-SR을 통해서 eUICC 관리키(eUICC OTA 키, GP ISD 키 등)로 2차 암호화를 수행한 후 eUICC로 전송한다.

[0156] 그러면, eUICC는 이중 암호화된 프로파일을 2단계에 걸쳐 복호화한 후 프로비저닝 과정을 완료하게 되며, 그 이후에 SM-SR와의 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.

[0157] 도 9는 본 발명의 다른 실시예에 의한 eUICC 인증정보를 이용한 MNO 변경 과정을 도시한다.

[0158] 우선, 단말 제조 또는 eUICC 제조 단계에서 단말 제조사 또는 eUICC 제조사는 신뢰 서클(Circle of Trust) 내의 특정 엔터티로부터 해당 eUICC의 인증정보를 수신한 후, 해당 eUICC 내에 저장되어 있는 점은 도 8의 프로비저닝 과정의 S810 및 S820과 동일하다. (S910~S930)

[0159] 이 상태에서, 가입자가 MNO1(도너 MNO)에서 MNO2(리시빙 MNO)로 변경을 요청하면, eUICC는 IMEI 및 eICCid를 포함하는 활성화 요청 또는 개통 요청 메시지를 해당 MNO2 시스템으로 전송한다(Request activation; S940)

[0160] 그러면, 해당 리시빙 MNO2 시스템은 해당 eUICC 사이에서 eUICC 상태 요청(Status Request) 및 기술 성능 제어(Technical Capability Control) 확인을 수행함과 동시에, 해당 eUICC로부터 eUICC 인증 정보를 획득한다(eUICC status request 및 technical capability control; S950)

[0161] MNO2는 5단계에서 SM-SR로부터 해당 단말 또는 eUICC와 관련된 정보를 수집하는 과정에서, S950 단계에서 획득한 eUICC 인증정보를 SM-SR2(MNO2와 연결되어 있는 SM-SR)로 전송하여 eUICC 아이덴터티를 검증(Identity Verification)하게 된다.(eUICC identity verification 및 collect information about device ; S960)

[0162] 다음으로, 리시빙 MNO2는 도너(Donor) MNO인 MNO1과 협상 및 권리이전(Negotiation and Right Transfer)를 수행하게 되는데, 이 과정에서 2개 MNO들 사이에서 eUICC 인증정보를 통한 검증을 추가로 수행할 수 있다.(S970)

[0163] 그 이후의 MNO 변경 과정은 도 4의 S440 내지 S470 단계와 유사하게 진행될 수 있다.

[0164] 즉, eUICC 인증정보를 통해서 해당 eUICC의 아이덴터티가 검증된 경우에 한하여, 리시빙 MNO2 시스템은 SM-DP2를 통해서 프로파일을 생성한 후 암호화키(eUICC 공개키 등)로 1차 암호화하고, SM-SR2을 통해서 eUICC 관리키(eUICC OTA 키, GP ISD 키 등)로 2차 암호화를 수행한 후 eUICC로 전송한다.

[0165] 그러면, eUICC는 이중 암호화된 프로파일을 2단계에 걸쳐 복호화한 후 MNO 변경 과정을 완료하게 되며, 그 이후에 SM-SR2와의 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.

[0166] 이상과 같이 MNO와 SM-SR 등 신뢰로 결합된 eUICC 전체 시스템(Trusted Sector)에서 특정한 eUICC에 대한 아이덴터티 검증(identity verification)을 수행 할 수 있는 정보로서의 인증 정보(eUICC Certification)를 정의하고, 그를 처리할 수 있는 인증 프로파일(Cert. Profile)을 이용함으로써, eUICC 단말의 가입 및 MNO 변경과정에서 해당 eUICC의 검증을 수행할 수 있는 효과가 있다.

[0167] 또한, 중복을 피하기 위하여 구체적인 설명은 생략하지만, 이상과 같이 eUICC 인증정보를 이용하는 eUICC, MNO 시스템 및 프로비저닝 방법, MNO 변경 방법 등은 컴퓨터가 읽을 수 있는 프로그램 형태로 구현될 수 있을 것이

다.

[0168] 이와 같이, 컴퓨터가 기록매체에 기록된 프로그램을 읽어 들여 위와 같은 여러 기능을 실행시키기 위하여, 전술한 프로그램은 컴퓨터의 프로세서(CPU)가 읽힐 수 있는 C, C++, JAVA, 기계어 등의 컴퓨터 언어로 코드화된 코드(Code)를 포함할 수 있다.

[0169] 이러한 코드는 전술한 기능들을 정의한 함수 등과 관련된 기능적인 코드(Function Code)를 포함할 수 있고, 전술한 기능들을 컴퓨터의 프로세서가 소정의 절차대로 실행시키는데 필요한 실행 절차 관련 제어 코드를 포함할 수 있다.

[0170] 또한, 이러한 코드는 전술한 기능들을 컴퓨터의 프로세서가 실행시키는데 필요한 추가 정보나 미디어가 컴퓨터의 내부 또는 외부 메모리의 어느 위치(주소 번지)에서 참조 되어야 하는지에 대한 메모리 참조 관련 코드를 더 포함할 수 있다.

[0171] 또한, 컴퓨터의 프로세서가 전술한 기능들을 실행시키기 위하여 원격(Remote)에 있는 어떠한 다른 컴퓨터나 서버 등과 통신이 필요한 경우, 코드는 컴퓨터의 프로세서가 컴퓨터의 통신 모듈(예: 유선 및/또는 무선 통신 모듈)을 이용하여 원격(Remote)에 있는 어떠한 다른 컴퓨터나 서버 등과 어떻게 통신해야만 하는지, 통신 시 어떠한 정보나 미디어를 송수신해야 하는지 등에 대한 통신 관련 코드를 더 포함할 수도 있다.

[0172] 그리고, 본 발명을 구현하기 위한 기능적인(Functional) 프로그램과 이와 관련된 코드 및 코드 세그먼트 등은, 기록매체를 읽어서 프로그램을 실행시키는 컴퓨터의 시스템 환경 등을 고려하여, 본 발명이 속하는 기술분야의 프로그래머 들에 의해 용이하게 추론되거나 변경될 수도 있다.

[0173] 전술한 바와 같은 프로그램을 기록한 컴퓨터로 읽힐 수 있는 기록매체는, 일 예로, ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 미디어 저장장치 등이 있다.

[0174] 또한 전술한 바와 같은 프로그램을 기록한 컴퓨터로 읽힐 수 있는 기록매체는 네트워크로 커넥션된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 이 경우, 다수의 분산된 컴퓨터 중 어느 하나 이상의 컴퓨터는 상기에 제시된 기능들 중 일부를 실행하고, 그 결과를 다른 분산된 컴퓨터들 중 하나 이상에 그 실행 결과를 전송할 수 있으며, 그 결과를 전송받은 컴퓨터 역시 상기에 제시된 기능들 중 일부를 실행하여, 그 결과를 역시 다른 분산된 컴퓨터들에 제공할 수 있다.

[0175] 특히, 본 발명의 실시예에 따른 eUICC 인증정보와 관련된 여러 기능 또는 방법을 실행시키기 위한 프로그램인 애플리케이션을 기록한 컴퓨터로 읽을 수 있는 기록매체는, 애플리케이션 스토어 서버(Application Store Server), 애플리케이션 또는 해당 서비스와 관련된 웹 서버 등의 애플리케이션 제공 서버(Application Provider Server)에 포함된 저장매체(예: 하드디스크 등)이거나, 애플리케이션 제공 서버 그 자체일 수도 있다.

[0176] 이상에서, 본 발명의 실시예를 구성하는 모든 구성 요소들이 하나로 결합되거나 결합되어 동작하는 것으로 설명되었다고 해서, 본 발명이 반드시 이러한 실시예에 한정되는 것은 아니다. 즉, 본 발명의 목적 범위 안에서라면, 그 모든 구성 요소들이 하나 이상으로 선택적으로 결합하여 동작할 수도 있다. 또한, 그 모든 구성 요소들이 각각 하나의 독립적인 하드웨어로 구현될 수 있지만, 각 구성 요소들의 그 일부 또는 전부가 선택적으로 조합되어 하나 또는 복수 개의 하드웨어에서 조합된 일부 또는 전부의 기능을 수행하는 프로그램 모듈을 갖는 컴퓨터 프로그램으로서 구현될 수도 있다. 그 컴퓨터 프로그램을 구성하는 코드들 및 코드 세그먼트들은 본 발명의 기술 분야의 당업자에 의해 용이하게 추론될 수 있을 것이다. 이러한 컴퓨터 프로그램은 컴퓨터가 읽을 수 있는 저장매체(Computer Readable Media)에 저장되어 컴퓨터에 의하여 읽혀지고 실행됨으로써, 본 발명의 실시예를 구현할 수 있다. 컴퓨터 프로그램의 저장매체로서는 자기 기록매체, 광 기록매체, 캐리어 웨이브 매체 등이 포함될 수 있다.

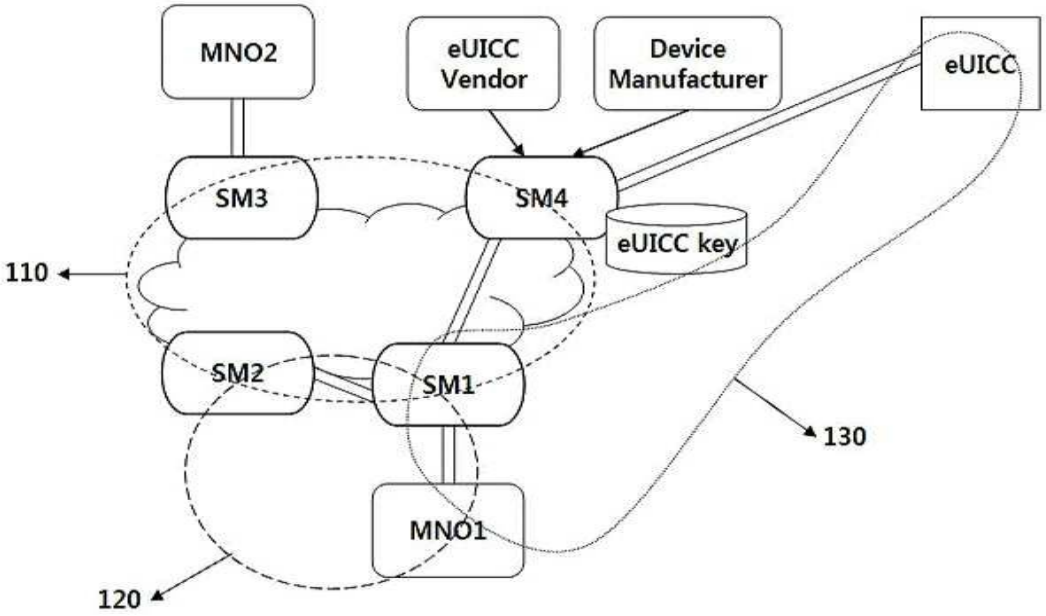
[0177] 또한, 이상에서 기재된 "포함하다", "구성하다" 또는 "가지다" 등의 용어는, 특별히 반대되는 기재가 없는 한, 해당 구성 요소가 내재될 수 있음을 의미하는 것이므로, 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것으로 해석되어야 한다. 기술적이거나 과학적인 용어를 포함한 모든 용어들은, 다르게 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 사전에 정의된 용어와 같이 일반적으로 사용되는 용어들은 관련 기술의 문맥 상의 의미와 일치 하는 것으로 해석되어야 하며, 본 발명에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0178] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에

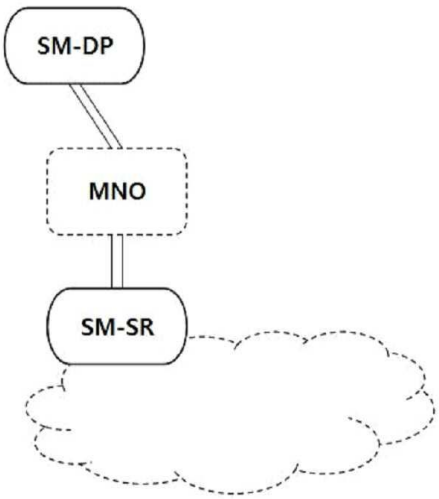
서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시 예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

도면

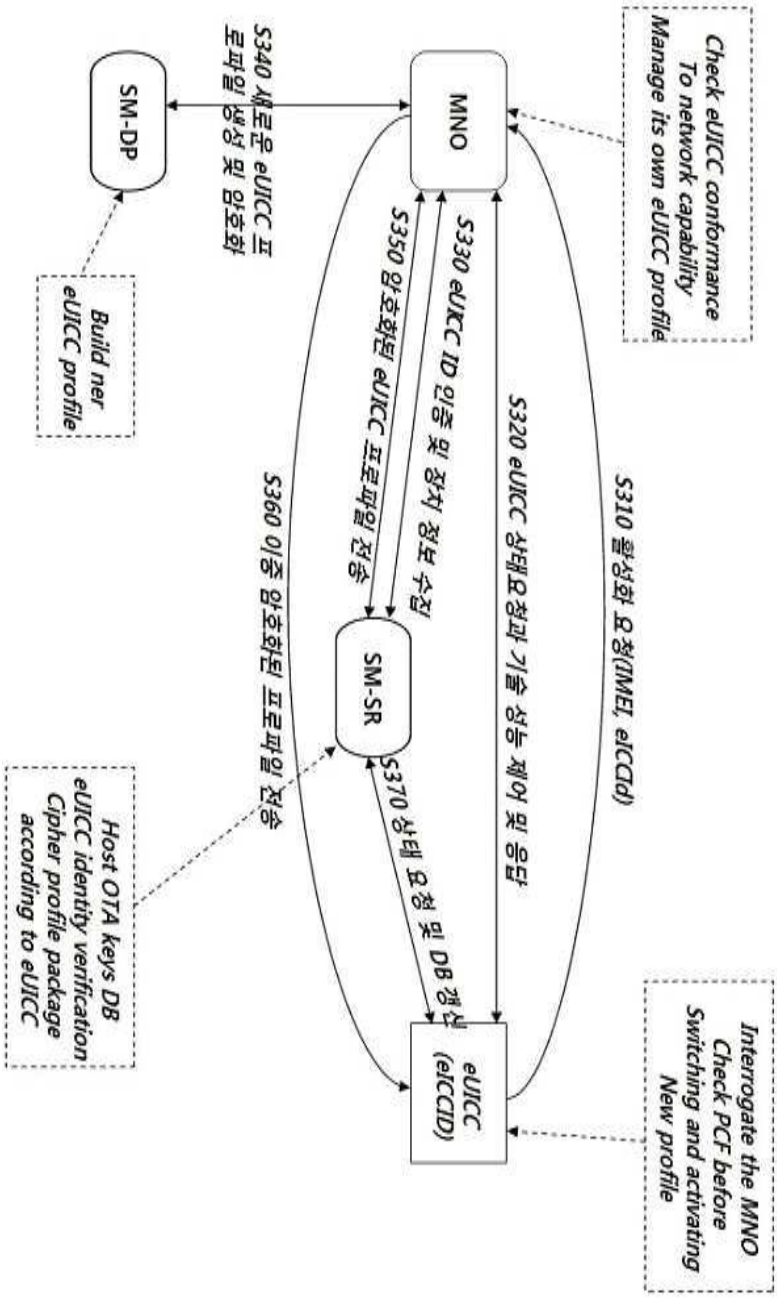
도면1



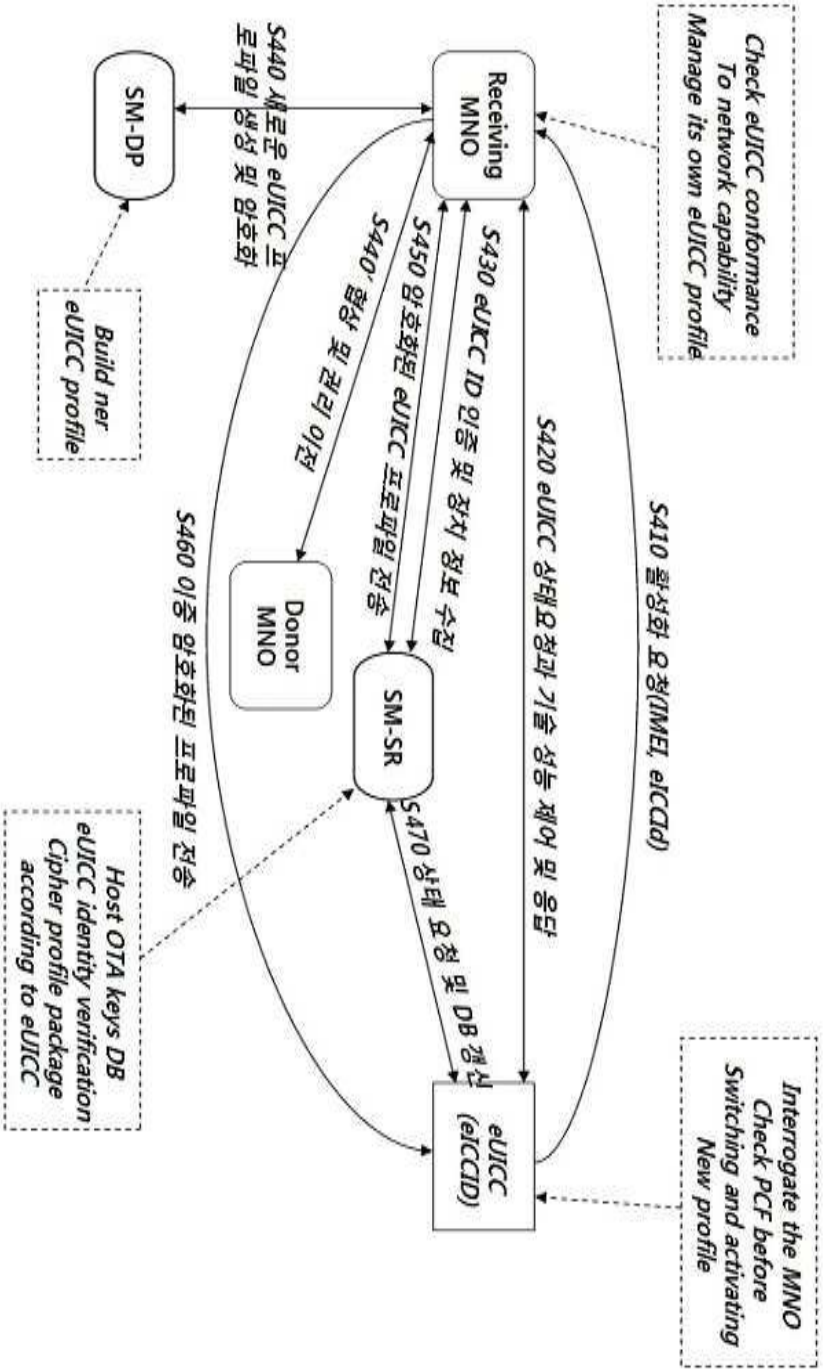
도면2



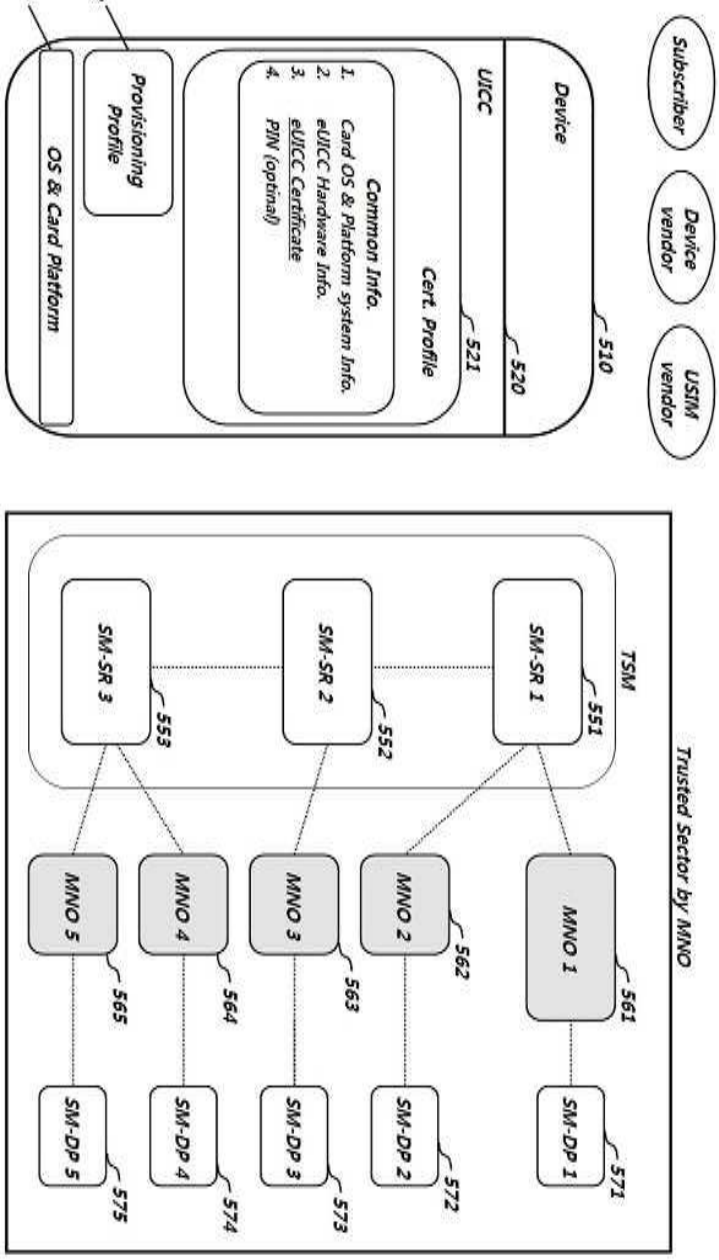
도면3


Check eUICC conformance
To network capability
Manage its own eUICC profile
MNO
SM-DP
S340 새로운 eUICC 프로파일 생성 및 암호화
Build ner eUICC profile
S330 eUICC ID 인증 및 장치 정보 수집
S350 암호화된 eUICC 프로파일 전송
S320 eUICC 상태요청과 기술 성능 제어 및 응답
S310 활성화 요청(IMEI, eICCid)
S360 이중 암호화된 프로파일 전송
SM-SR
S370 상태 요청 및 DB 갱신
eUICC
(eICCID)
Host OTA keys DB
eUICC identity verification
Cipher profile package
according to eUICC
Interrogate the MNO
Check PCF before
Switching and activating
New profile

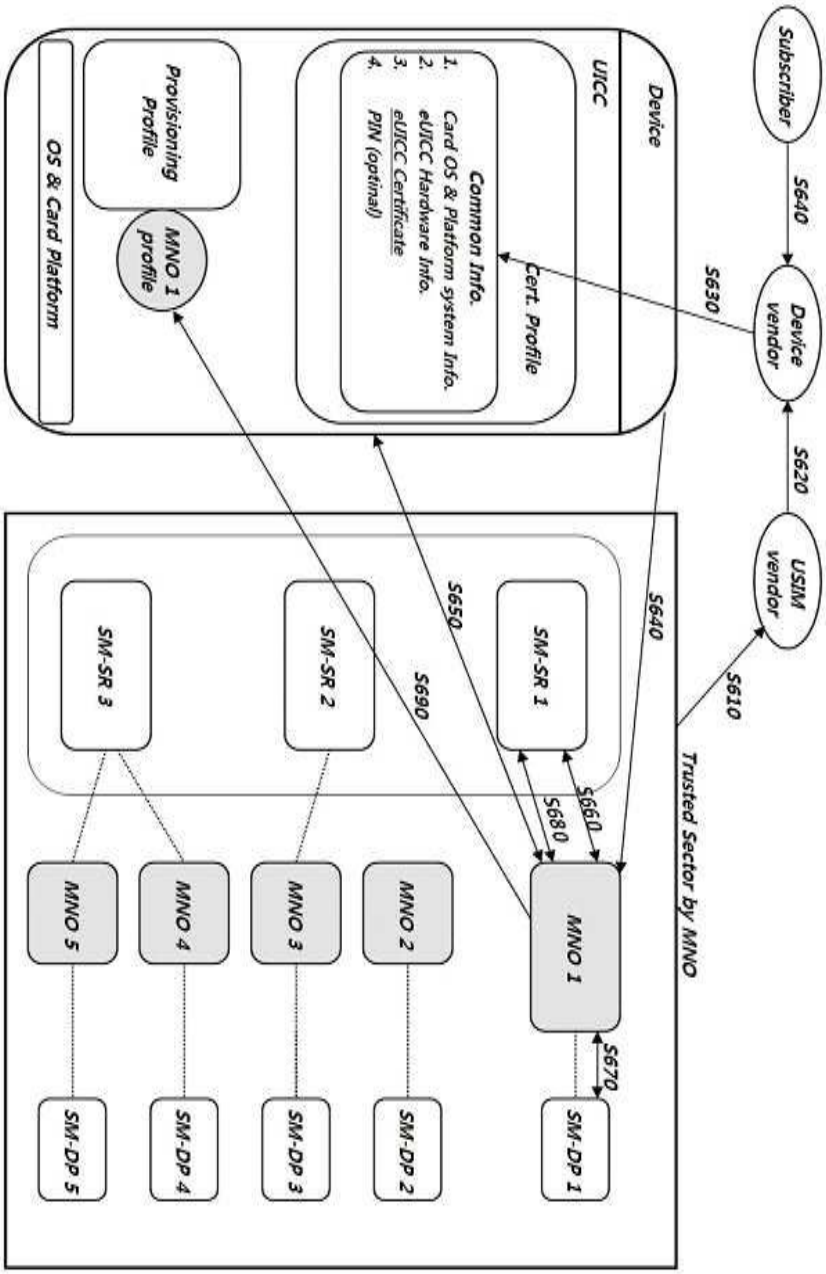
도면4


Check eUICC conformance
To network capability
Manage its own eUICC profile
Receiving MNO
SM-DP
S440 새로운 eUICC 프로파일 생성 및 암호화
Build ner eUICC profile
S420 eUICC 상태요청과 기술 성능 제어 및 응답
S410 활성화 요청(IMEI, eICCId)
S430 eUICC ID 인증 및 장치 정보 수집
S450 암호화된 eUICC 프로파일 전송
S460 이중 암호화된 프로파일 전송
Donor MNO
SM-SR
S470 상태 요청 및 DB 갱신
eUICC (eICCID)
Host OTA keys DB
eUICC identity verification
Cipher profile package according to eUICC
Interrogate the MNO
Check PCF before
Switching and activating
New profile

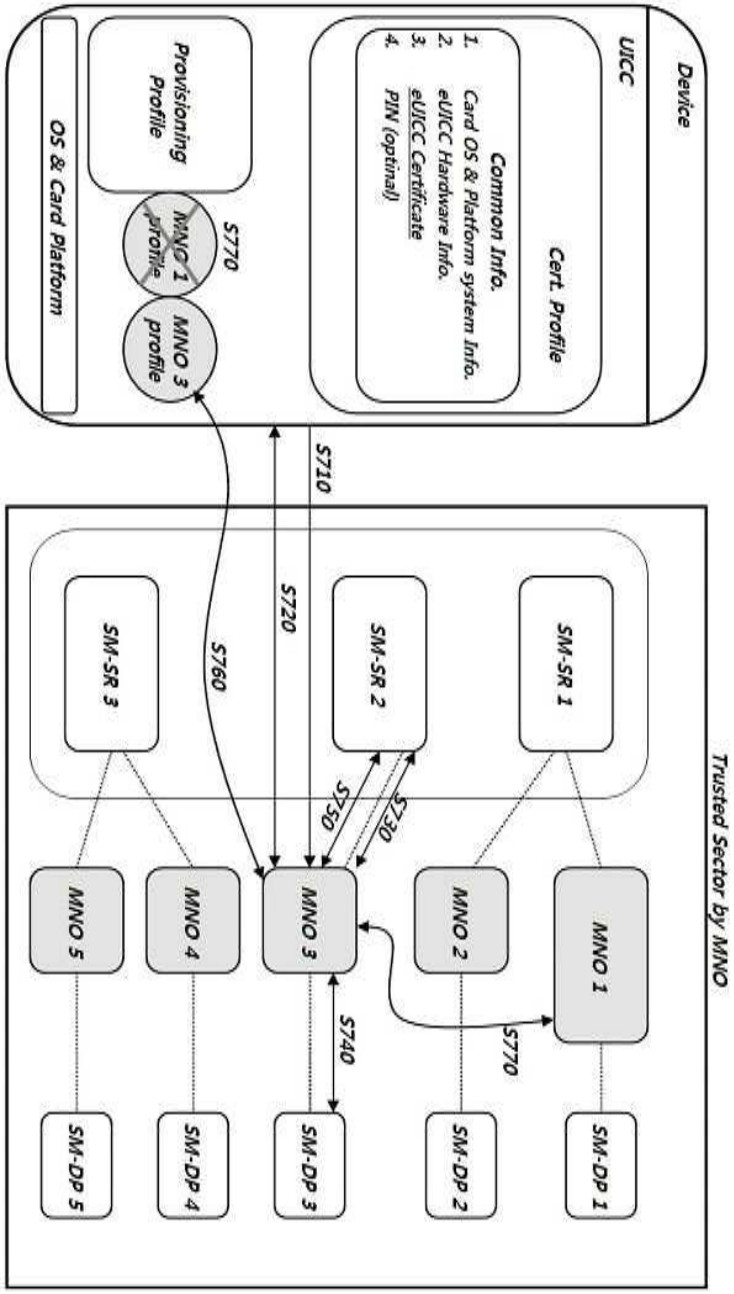
도면5


Subscriber
Device vendor
USIM vendor
Device
510
UICC
520
Cert. Profile
521
Common Info.
1. Card OS & Platform system Info.
2. eUICC Hardware Info.
3. eUICC Certificate
4. PIN (optinal)
Provisioning Profile
522
OS & Card Platform
523
Trusted Sector by MNO
TSM
SM-SR 1
551
SM-SR 2
552
SM-SR 3
553
MNO 1
561
MNO 2
562
MNO 3
563
MNO 4
564
MNO 5
565
SM-DP 1
571
SM-DP 2
572
SM-DP 3
573
SM-DP 4
574
SM-DP 5
575

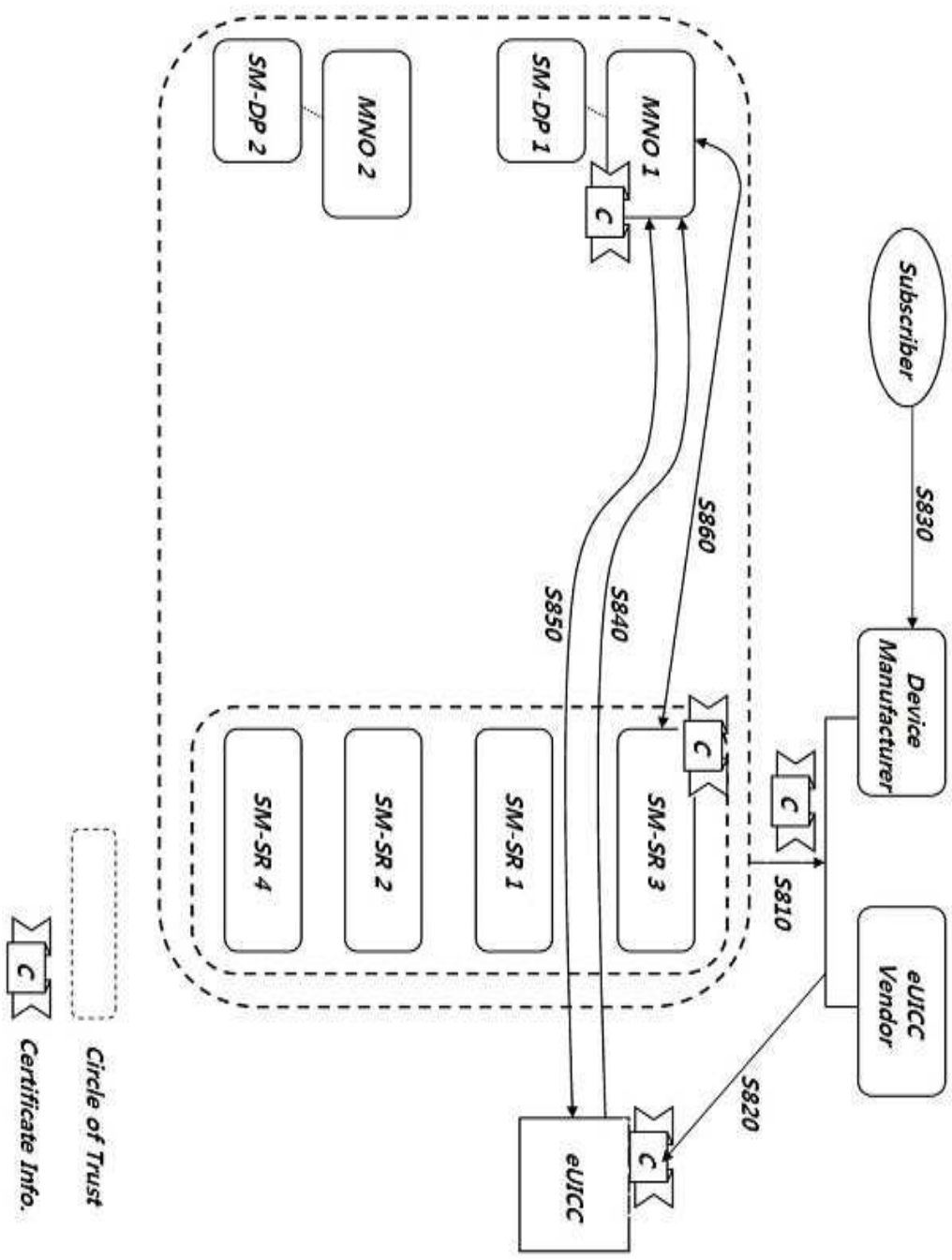
도면6


Subscriber
S640
Device vendor
S630
S620
USIM vendor
S610
Device
UICC
Common Info.
1. Card OS & Platform system Info.
2. eUICC Hardware Info.
3. eUICC Certificate
4. PIN (optinal)
Cert. Profile
Provisioning Profile
MNO 1 profile
OS & Card Platform
S640
S650
S690
SM-SR 1
SM-SR 2
SM-SR 3
S660
S680
MNO 1
MNO 2
MNO 3
MNO 4
MNO 5
S670
SM-DP 1
SM-DP 2
SM-DP 3
SM-DP 4
SM-DP 5
Trusted Sector by MNO

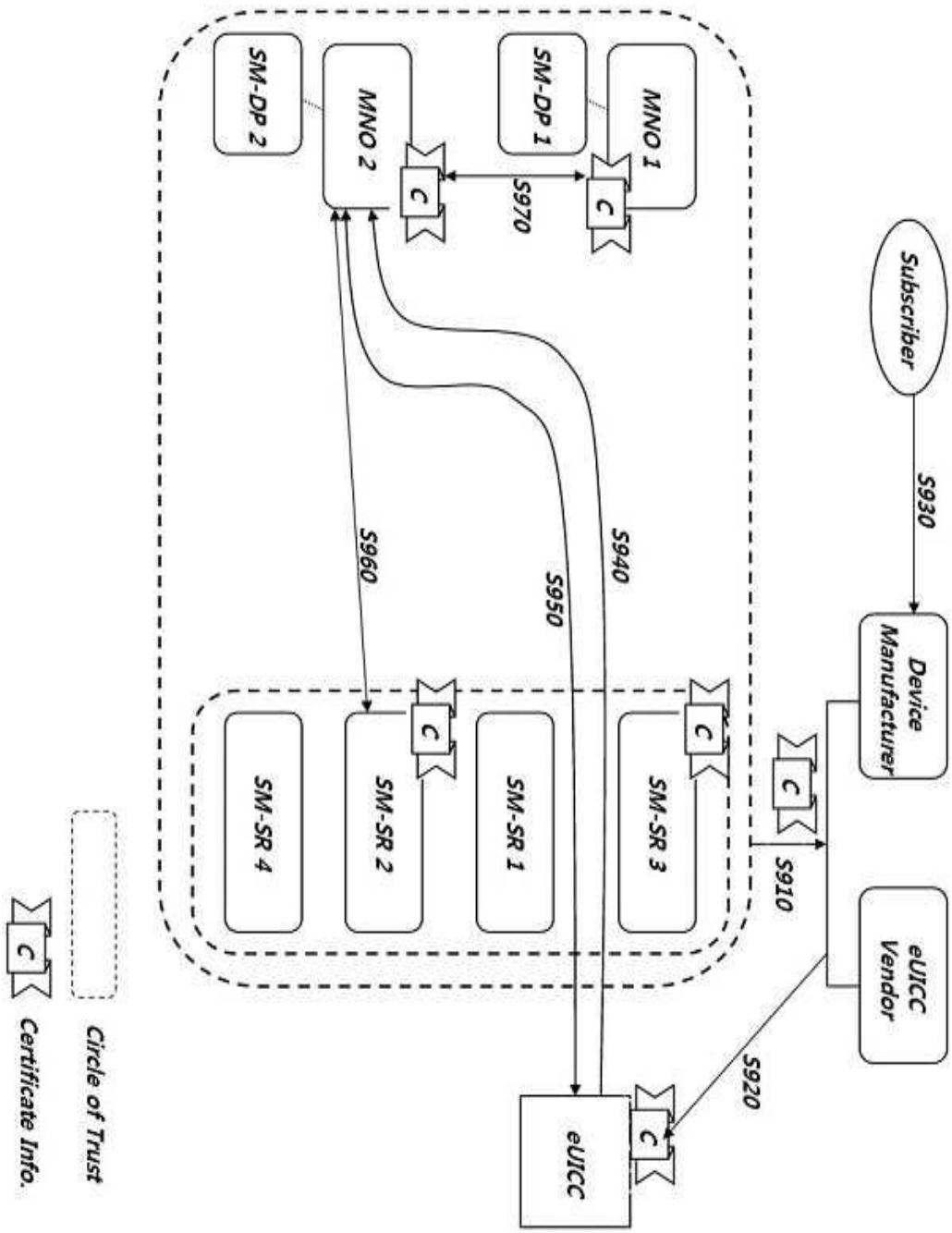
도면7


Device
UICC
Cert. Profile
Common Info.
1. Card OS & Platform system Info.
2. eUICC Hardware Info.
3. eUICC Certificate
4. PIN (optinal)
Provisioning Profile
MNO 1 profile
MNO 3 profile
S770
OS & Card Platform
S710
S720
S760
SM-SR 3
SM-SR 2
SM-SR 1
S750
S730
Trusted Sector by MNO
MNO 5
MNO 4
MNO 3
MNO 2
MNO 1
S740
S770
SM-DP 5
SM-DP 4
SM-DP 3
SM-DP 2
SM-DP 1

도면8


Subscriber
S830
Device Manufacturer
S810
eUICC Vendor
S820
eUICC
S860
S840
S850
MNO 1
SM-DP 1
MNO 2
SM-DP 2
SM-SR 3
SM-SR 1
SM-SR 2
SM-SR 4
Circle of Trust
Certificate Info.

도면9


Subscriber
S930
Device Manufacturer
S910
eUICC Vendor
S920
eUICC
SM-DP 2
MNO 2
SM-DP 1
MNO 1
S970
S960
S950
S940
SM-SR 4
SM-SR 2
SM-SR 1
SM-SR 3
Circle of Trust
Certificate Info.