(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년04월09일
(11) 등록번호 10-1846995
(24) 등록일자 2018년04월03일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *G06Q 50/00* (2008.03)
H04L 9/30 (2006.01) *H04W 48/18* (2009.01)
(21) 출원번호 10-2011-0067856
(22) 출원일자 2011년07월08일
심사청구일자 2016년07월08일
(65) 공개번호 10-2013-0012220
(43) 공개일자 2013년02월01일
(56) 선행기술조사문헌
KR1020060130312 A*
KR1020080021178 A*
KR1020100087493 A
US20090191857 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 케이티
경기도 성남시 분당구 불정로 90(정자동)
(72) 발명자
이현송
서울특별시 서초구 태봉로 151, KT연구개발센터(우면동)
조수현
서울특별시 서초구 태봉로 151, KT연구개발센터(우면동)
(뒷면에 계속)
(74) 대리인
특허법인이상, 송해모

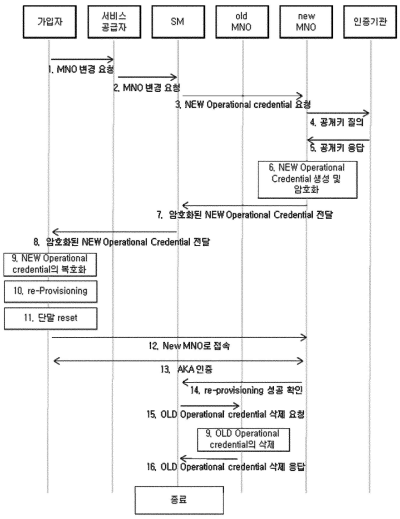
전체 청구항 수 : 총 8 항 심사관 : 이준석

(54) 발명의 명칭 **eUICC를 포함하는 시스템에서 공개키 암호화를 이용한 정보 전송 방법**

(57) 요 약

본 발명은 내장 UICC(eUICC), 인증기관, 가입 관리장치(Subscription Manager; SM), 네트워크 사업자(MNO) 시스템을 포함하는 통신 시스템을 이용한 크레덴셜 정보 전달 방법으로서,MNO 시스템이 해당 eUICC의 공개키를 상기 SM에 질의하여 그에 대한 응답으로 해당 eUICC의 공개키를 수신하고, MNO 시스템은 전달하고자 하는 크레덴셜 정보를 상기 eUICC의 공개키로 암호화하여 상기 SM으로 전송하며, SM은 공개키로 암호화된 크레덴셜 정보를 상기 eUICC로 전송하는 단계를 포함하여 구성

대 표 도 - 도5



(72) 발명자

이성훈

서울특별시 서초구 태봉로 151, KT연구개발센터 (우면동)

홍성표

서울특별시 서초구 태봉로 151, KT연구개발센터 (우면동)

김세훈

서울특별시 서초구 태봉로 151, KT연구개발센터 (우면동)

명 세 서

청구범위

청구항 1

가입관리 시스템(SM: Subscription Manager) 및 통신사업자(MNO: Mobile Network Operator)와 연동하는 단말에 탑재된 내장 UICC(eUICC: embedded Universal IC Card) 크리덴셜 정보 전달 방법으로서,

인증 기관으로부터 발행된 크리덴셜 정보를 수신한 상기 가입관리 시스템 및 상기 통신사업자와 연동하는 단계;

상기 가입관리 시스템으로부터 공개키로 암호화된 크리덴셜 정보를 수신하는 단계;

상기 공개키에 대응되는 개인키로 상기 암호화된 크리덴셜 정보를 복호화하는 단계; 및

복호화된 크리덴셜 정보를 프로비저닝하고 상기 크리덴셜을 활성화하는 단계를 포함하고,

상기 크리덴셜 정보는 eUICC 식별자와 일대일 대응되며 프로비저닝 IMSI(Provisioning International Mobile Subscriber Identity)를 포함하는 초기 크리덴셜 정보; 및

IMSI(International Mobile Subscriber Identity) 및 네트워크 인증키 중 적어도 하나를 포함하는 오퍼레이션 크리덴셜 정보를 포함하고,

상기 초기 크리덴셜 정보는 초기 프로비저닝(initial provisioning)에서 상기 가입관리 시스템에 의한 상기 단말의 인증에 사용되고, 상기 오퍼레이션 크리덴셜 정보는 eUICC에서 사용자 식별을 위해 사용되는, 크리덴셜 정보 전달 방법.

청구항 2

청구항 1에 있어서,

상기 인증기관은 개인키, 공개키, 및 인증서 중 적어도 하나를 발행하는, 크리덴셜 정보 전달 방법.

청구항 3

청구항 1에 있어서,

상기 eUICC가 공개키로 암호화된 크리덴셜 정보를 저장하는 단계를 더 포함하는, 크리덴셜 정보 전달 방법.

청구항 4

삭제

청구항 5

청구항 1에 있어서,

기존 통신사업자에서 새로운 통신사업자로의 변경 요청에 따라, 상기 eUICC가 상기 새로운 통신사업자로부터 암호화된 새로운 오퍼레이션 크리덴셜을 수신하는 단계; 및

상기 eUICC가 상기 새로운 오퍼레이션 크리덴셜을 복호화하여 재-프로비저닝을 수행하는 단계를 더 포함하는, 크리덴셜 정보 전달 방법.

청구항 6

삭제

청구항 7

가입관리 시스템(SM: Subscription Manager) 및 통신사업자(MNO: Mobile Network Operator)와 연동하는 단말에 탑재된 내장 UICC(eUICC: embedded Universal IC Card)에 있어서,

인증 기관으로부터 발행된 크리덴셜 정보를 수신한 상기 가입관리 시스템 및 상기 통신사업자과 연동하고, 상기 가입관리 시스템으로부터 공개키로 암호화된 크리덴셜 정보를 수신하여 저장하고, 상기 공개키에 대응되는 개인키로 상기 암호화된 크리덴셜 정보를 복호화하며, 복호화된 크리덴셜을 프로비저닝하여 활성화시키고,

상기 크리덴셜 정보는 eUICC 식별자와 일대일 대응되며 프로비저닝 IMSI(Provisioning International Mobile Subscriber Identity)를 포함하는 초기 크리덴셜 정보; 및

IMSI(International Mobile Subscriber Identity) 및 네트워크 인증키 중 적어도 하나를 포함하는 오퍼레이션 크리덴셜 정보를 포함하고,

상기 초기 크리덴셜 정보는 초기 프로비저닝(initial provisioning)에서 상기 가입관리 시스템에 의한 상기 단말의 인증에 사용되고, 상기 오퍼레이션 크리덴셜 정보는 eUICC에서 사용자 식별을 위해 사용되는, eUICC.

청구항 8

청구항 7에 있어서,

상기 인증기관은 개인키, 공개키, 및 인증서 중 적어도 하나를 발행하는, eUICC.

청구항 9

청구항 7에 있어서,

상기 eUICC는 공개키로 암호화된 크리덴셜 정보를 저장하는, eUICC.

청구항 10

삭제

청구항 11

청구항 7에 있어서,

상기 eUICC는 기존 통신사업자에서 새로운 통신사업자로의 변경 요청에 따라, 상기 새로운 통신사업자로부터 암호화된 새로운 오퍼레이션 크리덴셜을 수신하여 복호화하고, 새로운 오퍼레이션 크리덴셜을 이용해 재-프로비저닝을 수행하는, eUICC.

청구항 12

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 본 발명은 내장 UICC(Embedded UICC ; 이하 'eUICC'라고도 칭함)가 사용되는 환경에서 공개키 암호화 방법을 이용한 eUICC의 발주/판매/프로비저닝(Provisioning)/MNO변경/해지 등을 위한 방법, 장치 및 시스템에 관한 것이다.

배 경 기 술

[0002] UICC(Universal Integrated Circuit Card)는 가입자 인증/식별/보안을 위한 이동통신의 핵심기술로서, UMTS 네트워크에서 안정적으로 사용되고 있다. MNO는 고유의 보안정보로서의 크레덴셜(credential; IMSI, Ki, OPC 등)을 UICC에 삽입하여 가입자에 대한 네트워크 인증을 하고 통신 및 부가서비스를 제공하고 있다.

현재 표준화된 UICC 물리적 형태 (단말과의 결합형태, 크기, 무게 등)는 M2M(Machine-to-Machine) 환경에 적합하지 않다. 예를 들어 M2M 의료와 같은 특수한 영역에서는 아주 작은 크기, 무게의 물리적 형태가 요구된다. 또한, 사물중심의 운용환경은 사람중심으로 표준화된 환경보다 더 높은 내구성을 요구한다. 다수의 단말이 원격지에 위치해 있으므로 UICC의 도난/훼손의 우려가 높다.

또한, 통신 사업자, 즉 MNO(Mobile Network Operator)가 결정되지 않은 상태에서 출시된 M2M 단말의 경우, 초기 원격 개통이 불가능하다. 기존의 핸드셋이 MNO가 미리 정해져서 단말이 출시되는 것에 반해, M2M은 단말이 만들어진 후, 사용자의 선택에 의해 MNO가 결정될 수 있다. 즉, MNO가 결정되지 않은 상태에서 M2M 단말이 생산된다. 예를 들어 자동차의 경우, UICC이 MNO가 결정되지 않은 채, M2M 단말에 내장(embedded) 형태로 설치되어 생산될 수 있다. 따라서 가입자는 자동차 구매 후 MNO와 초기 원격 개통을 해야 한다. 이와 같은 경우 기존 UICC은 초기 원격 개통이 불가능하다.

또한, MNO 변경에 많은 비용이 소요된다. 현재 UICC 환경에서 MNO와의 계약이 만료되고, 가입자가 새로운 MNO와의 계약을 원한다면, 일일이 UICC 카드를 교체해야만 한다. 다수의 M2M 단말에 대한 위와 같은 방법의 MNO 변경은 높은 비용을 발생시킨다.

[0003] 삭제

[0004] 삭제

[0005] 삭제

발명의 내용

해결하려는 과제

[0006] 상기한 문제점을 해결하기 위해 내장 SIM(Subscriber Identity Module)은 단말에 물리적으로 고정되어(embedded) 착탈이 불가능하고 원격 프로비저닝(Provisioning)이 가능한 기술이어야 한다.

본 발명은 eUICC가 사용되는 환경에서 공개키 암호화 방법을 이용한 eUICC의 발주/판매/프로비저닝(Provisioning)/MNO변경/해지 등의 절차에 관한 것이다.

과제의 해결 수단

[0007] 본 발명에 의하면, 내장 UICC(eUICC), 인증기관, 가입 관리장치(Subscription Manager; SM), 네트워크 사업자(MNO) 시스템을 포함하는 통신 시스템을 이용한 크레덴셜 정보 전달 방법으로서, 상기 MNO 시스템이 해당 eUICC의 공개키를 상기 인증기관에 질의하여 그에 대한 응답으로 해당 eUICC의 공개키를 수신하는 단계와, 상기 MNO 시스템은 전달하고자 하는 크레덴셜 정보를 상기 eUICC의 공개키로 암호화하여 상기 SM으로 전송하는 단계와, 상기 SM은 공개키로 암호화된 크레덴셜 정보를 상기 eUICC로 전송하는 단계를 포함하는 크레덴셜 정보 전달 방법을 제공한다.

발명의 효과

[0008] 본 발명에 의하면, Embedded UICC가 사용되는 환경에서 MVNO 형태의 SM은 초기 프로비저닝(Initial provisioning) 및 사업자 변경을 가능하게 한다. 즉, SM은 eUICC_ID와 그것에 일대일 대응되는 초기 크레덴셜(Initial credential)을 발행하고 PIMSI(Provisioning IMSI), Ki, Opc를 발행/관리/인증 하는 일종의 MVNO기능을 수행한다. PIMSI의 발행을 위해 SM은 고유의 MNC(Mobile Network Code)를 ITU로 부터 할당 받아 번호자원을 관리하고, 향후 초기 개통시 AKA (Authentication and Key Agreement)절차를 통해 단말을 인증한다.

M2M 단말은 SM 접속을 위한 공통의 정보(initial credential)만 가지고 있으면 되기 때문에, 특정 MNO에 종속되어 생산되는 기존 M2M 단말 생산구조보다 훨씬 개방적이다. 따라서 M2M 단말의 대량생산으로 인한 단가 하락의 효과를 기대할 수 있다.

또한 SM을 통한 MNO 크레덴셜(credential) 전송시 발생할 수 있는 보안 문제를 해결하기 위해, 공개키 암호화 방법을 사용하여 MNO 주요정보(credential, application등)의 노출을 막을 수 있다. MNO는 공개키를 통해 MNO 주요정보를 암호화하여 전송하면 단말은 개인키를 통해 해당정보를 복호화하는 PKI 알고리즘을 사용한다. 따라서 사용자와 MNO를 제외한 모든 구성원은 암호화된 MNO의 주요정보의 열람, 수정, 복제 등이 불가능하다. 이러

한 프로세스는 MNO 주요정보에 대한 보안문제를 해결할 뿐만 아니라, SM의 역할을 단순히 MNO 주요정보의 전달자로 한정하기 때문에, MNO는 UICC의 각종 사업에 대한 주도권을 유지하고 기존망에 있는 기능을 그대로 사용하는 것을 가능하게 한다.

[0009] 삭제

[0010] 삭제

도면의 간단한 설명

도 1은 본 발명의 실시예에 따른 전체 시스템 구조 및 개략적인 연동 관계를 도시한다.

도 2는 본 발명에 의한 단말의 발주 및 공급 과정의 신호 흐름을 도시한다.

도 3은 본 발명에 의한 단말의 판매와 Subscription 과정의 신호 흐름을 도시한다.

도 4는 본 발명에 의한 초기 프로비저닝(initial Provisioning) 과정의 신호 흐름을 도시한다.

도 5는 본 발명에 의한 통신 사업자 변경 과정의 신호 흐름을 도시한다.

도 6은 본 발명에 의한 서비스 해지 과정의 신호 흐름을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0012] 도 1 과 같이, 본 발명에 의한 전체 시스템은 아래와 같은 구성요소로 이루어져 있으나 그에 한정되는 것은 아니며, 필요한 경우 일부가 삭제되거나 통합 구현될 수 있다.

도 1과 같이 본 발명에 의한 전체 시스템은 eUICC 제조사, 단말 제조사, MNO (Mobile Network Operator)인 이동통신사, 서비스 공급자, 사용자 단말, 프로비저닝 네트워크, 인증기관 및 SM 등으로 구성된다.

서비스 공급자는 M2M 단말을 발주하고 M2M 서비스를 고객에게 제공하는 회사로서, 서비스공급자는 MNO가 될 수 있다.

프로비저닝 네트워크는 초기 (initial) 프로비저닝을 위해 사용되는 임시 네트워크(예: 이동통신망 or 인터넷)를 의미한다.

인증기관은 본 발명에 의한 공개키 방식(PKI; Public Key Infrastructure)의 인증을 위해, 개인키, 공개키, 인증서를 발행하는 기관을 의미한다.

SM (Subscription Manager)은 eUICC를 관리하는 기능을 하는 엔터티로서, 기존 모바일 네트워크 구성원 (MNO, 서비스 공급자, eUICC 제조사, 단말 제조사 등) 내에서 구현되거나, 별도의 제3 주체로 구현될 수 있다.

도 2와 같이, 본 발명에 의한 M2M 단말의 발주 및 공급 과정은 다음과 같다.

① 서비스 공급자는 M2M 단말을 단말제조사로 요청한다.

② 단말 제조사는 SM에게 eUICC 발주를 요청한다.

③ 단말 제조사는 M2M 단말을 생산한다.

④ SM은 eUICC_ID와 그것에 일대일 대응되는 초기 크레덴셜(Initial credential)을 발행한다. 이때 SM은 PIMSI(Provisioning IMSI), Ki, Opc를 발행/관리/인증 하는 일종의 MVNO 기능을 수행한다. 즉, PIMSI의 발행을 위해 SM은 고유의 MNC(Mobile Network Code)를 ITU로 부터 할당 받아 번호자원을 관리 할 수 있고, 향후 초기 프로비저닝시 AKA (Authentication and Key Agreement)절차를 통해 단말을 인증한다.

본 발명에 의한 초기 크레덴셜(Initial credential) 주요 파라미터 정보는 다음과 같을 수 있다.

- PIMSI 예: 450771234567890) 450=MCC(한국), 77=MNC(ITU가 SM에 할당한 MNC code), 1234567890=MSIN(SM 고유의 번호자원)

- 네트워크 인증키(Ki/OPC)

eUICC_ID는 eUICC를 식별할 수 있는 유일한 ID이다.

⑤ SM은 eUICC 제조사로 eUICC_ID와 초기 크레덴셜을 보내고 eUICC 생산을 요청한다.

⑥ eUICC 제조사는 UICC_ID 해당하는 PKI 인증데이터를 인증기관으로 발행 요청한다.

⑦ 인증기관은 PKI 인증데이터(개인키, 공개키, 인증서)를 발행한다.

⑧ 인증기관은 PKI 인증데이터를 전송한다.

⑨ eUICC 제조사는 ④와 ⑦의 정보를 포함하는 eUICC를 생산한다. (pre-provision)

⑩ eUICC 제조사는 단말 제조사에 eUICC를 납품한다.

⑪ 단말제조사는 생산된 M2M 단말에 eUICC를 내장(embedding) 시킨다.

⑫ 단말제조사는 서비스 공급자에게 단말을 납품한다.

도 3과 같이, 본 발명에 의한 M2M 단말의 판매와 가입(Subscription) 과정은 다음과 같다.

① 서비스 공급자는 M2M 단말을 가입자에게 판매한다. 이때 서비스 공급자와 가입자는 가입(Subscription) 관계를 맺는다. (M2M단말이 향후 사용할 MNO 정보를 포함)

② 서비스 공급자는 판매된 eUICC ID에 해당하는 가입(Subscription)정보를 SM에 전달한다.

③ SM은 eUICC ID에 해당하는 가입 정보를 저장한다. (향후 Initial provisioning시 사용)

도 4와 같이, 본 발명에 의한 초기 프로비저닝(initial Provisioning) 과정은 다음과 같다.

① 가입자가 M2M 단말의 사용을 위해 전원을 켠다.

② eUICC는 프로비저닝 네트워크를 통해 PIMSI를 사용하여 SM에 접속한다. (모든 MNO는 PIMSI(MNC)의 라우팅 정보를 가지고 있다.)

이 때, 프로비저닝 네트워크는 초기 프로비저닝(Initial provisioning)을 위해 임시적으로 사용하는 네트워크로 어떤 MNO망도 대상이 될 수 있다.

③ eUICC와 단말은 초기 크레덴셜(Initial credential)을 통해 AKA인증을 수행한다.

④ SM은 2)에서 얻은 가입(Subscription) 정보에 있는 MNO에게 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)을 요청한다.

이 때, 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)는 현 UICC에서 사용하는 사용자 인증/식별을 위한 데이터로서, 다음과 같은 정보를 포함할 수 있다.

- IMSI : 일 예로서 450081234567890) 450=MCC(한국), 08=KT(ITU가 MNO에 할당한 MNC code), 1234567890=MSIN(KT 고유의 번호자원)

- 네트워크 인증키(Ki/OPC)

⑤ MNO는 인증기관으로 eUICC_ID에 해당하는 공개키를 질의한다.

⑥ 인증기관은 MNO에게 eUICC_ID의 공개키를 알려준다.

⑦ MNO는 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)을 생성하고 eUICC에 대한 공개키로 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)를 암호화 한다. (개인키를 가지고 있는 eUICC만이 암호화를 해독할 수 있다.)

⑧ MNO는 암호화된 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)을 SM에 전달한다.

⑨ SM은 프로비저닝 네트워크를 통해 암호화된 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)을 eUICC에 전달한다.

⑩ eUICC는 개인키를 통해 암호화된 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)을 해독한다.

⑪ eUICC는 해독된 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)을 프로비저닝

(provisioning) 한다.

⑫ eUICC는 단말을 리셋시키고, eUICC는 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)을 활성화한다.

⑬ eUICC는 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)의 IMSI정보를 이용해 MNO로 접속한다.

⑭ eUICC와 단말은 오퍼레이션 크레덴셜 또는 동작 크레덴셜(Operational Credential)을 통해 AKA인증을 수행한다.

⑮ MNO는 초기 프로비저닝(Initial provisioning) 성공확인 메시지를 SM으로 보낸다.

도 5와 같이, 본 발명에 의한 MNO 변경 과정은 다음과 같다.

① 가입자는 서비스 공급자로 MNO 변경 요청을 한다.

② 서비스 공급자는 SM으로 MNO 변경 요청을 한다.

③ SM은 새로운 MNO(New MNO, 즉 변경후 MNO)에게 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)의 발급을 요청한다.

④ New MNO는 인증기관으로 eUICC_ID에 해당하는 공개키를 질의한다.

⑤ 인증기관은 new MNO에게 eUICC_ID의 공개키를 알려준다.

⑥ new MNO는 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)을 생성하고 eUICC에 대한 공개키로 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)를 암호화한다. (개인키를 가지고 있는 eUICC만이 암호화를 해독할 수 있다.)

⑦ new MNO는 암호화된 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)을 SM에 전달한다.

⑧ SM은 old MNO 네트워크를 통해 암호화된 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)을 eUICC에 전달한다.

⑨ eUICC는 개인키를 통해 암호화된 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)을 해독한다.

⑩ eUICC는 해독된 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)으로 재프로비저닝(re-provisioning) 한다.

이 때, 재프로비저닝(re-provisioning)은 MNO를 변경하기 위해 new MNO의 크레덴셜로 eUICC를 활성화하는 절차이다. eUICC 내부구조 구현방식에 따라, 종전의 MNO, 즉 도너(Donor) MNO의 오퍼레이션 크레덴셜을 삭제하고 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)을 덮어쓰는 방식과 기존 크레덴셜을 비활성화 시키고 새로운 크레덴셜을 활성화 하는 방법 등이 사용될 수 있다.

⑪ eUICC는 단말을 리셋시키고, eUICC는 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)을 활성화한다.

⑫ eUICC는 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)의 IMSI정보를 이용해 새로운 MNO로 접속한다.

⑬ eUICC와 단말은 새로운 오퍼레이션 크레덴셜 또는 동작 크레덴셜(NEW Operational Credential)을 통해 AKA인증을 수행한다.

⑭ MNO는 재프로비저닝(re-provisioning) 성공확인 메시지를 SM으로 보낸다.

⑮ SM은 기존 MNO로 기존 오퍼레이션 크레덴셜(OLD Operational credential)의 삭제를 요청한다.

16) 기존 MNO는 기존 오퍼레이션 크레덴셜(OLD Operational credential)을 삭제한다.

17) 기존 MNO는 SM으로 기존 오퍼레이션 크레덴셜(OLD Operational credential) 삭제를 응답한다.

도 6과 같이, 본 발명에 의한 M2M 서비스 해지 과정은 다음과 같다.

① 가입자는 서비스 공급자에게 서비스 해지를 요청한다.

② 서비스 공급자는 SM에게 서비스 해지를 요청한다.

③ SM은 MNO 네트워크를 통해 eUICC로 접속하고 eUICC 초기화를 요청한다.

④ eUICC는 eUICC 생산단계로 초기화 된다.(pre-provision단계: eUICC_ID와 initial credential이 존재하는 단계).

⑤ eUICC는 프로비저닝 네트워크를 통해 SM으로 접속하고 eUICC 초기화 완료를 응답한다.

⑥ SM은 MNO로 오퍼레이션 크레덴셜(Operational credential)의 삭제를 요청한다.

⑦ MNO는 오퍼레이션 크레덴셜(Operational credential)을 삭제한다.

⑧ MNO는 SM으로 오퍼레이션 크레덴셜(Operational credential) 삭제를 응답한다.

본 발명에 의하면, eUICC가 사용되는 환경에서 MVNO 형태의 SM은 초기 프로비저닝(Initial provisioning) 및 사업자 변경을 가능하게 한다. 즉, SM은 eUICC_ID와 그것에 일대일 대응되는 초기 크레덴셜을 발행하고 PIMSI(Provisioning IMSI), Ki, Opc를 발행/관리/인증 하는 일종의 MVNO기능을 수행한다. PIMSI의 발행을 위해 SM은 고유의 MNC(Mobile Network Code)를 ITU로 부터 할당 받아 번호자원을 관리하고, 향후 initial provision시 AKA (Authentication and Key Agreement)절차를 통해 단말을 인증한다.

M2M 단말은 SM 접속을 위한 공통의 정보(initial credential)만 가지고 있으면 되기 때문에, 특정 MNO에 종속되어 생산되는 기존 M2M 단말 생산구조보다 훨씬 개방적이다. 따라서 M2M 단말의 대량생산으로 인한 단가 하락의 효과를 기대할 수 있다.

또한 SM을 통한 MNO 크레덴셜 전송시 발생할 수 있는 보안 문제를 해결하기 위해, 공개키 암호화 방법을 사용하여 MNO 주요정보(credential, application등)의 노출을 막을 수 있다. MNO는 공개키를 통해 MNO 주요정보를 암호화 하여 전송하면 단말은 개인키를 통해 해당정보를 복호화하는 PKI 알고리즘을 사용한다. 따라서 사용자와 MNO를 제외한 모든 구성원은 암호화된 MNO의 주요정보의 열람, 수정, 복제 등이 불가능하다. 이러한 프로세스는 MNO 주요정보에 대한 보안문제를 해결할 뿐만 아니라, SM의 역할을 단순히 MNO 주요정보의 전달자로 한정하기 때문에, MNO는 UICC의 각종 사업에 대한 주도권을 유지하고 기존망에 있는 기능을 그대로 사용하는 것을 가능하게 한다.

[0013] 삭제

[0014] 삭제

[0015] 삭제

[0016] 삭제

[0017] 삭제

[0018] 삭제

[0019] 삭제

[0020] 삭제

[0021] 삭제

[0022] 삭제

[0023] 삭제

[0024] 삭제

[0025] 삭제

[0026] 삭제

[0027] 삭제

[0028] 삭제

[0029] 삭제

[0030] 삭제

[0031] 삭제

[0032] 삭제

[0033] 삭제

[0034] 삭제

[0035] 삭제

[0036] 삭제

[0037] 삭제

[0038] 삭제

[0039] 삭제

[0040] 삭제

[0041] 삭제

[0042] 삭제

[0043] 삭제

[0044] 삭제

[0045] 삭제

[0046] 삭제

[0047] 삭제

[0048] 삭제

[0049] 삭제

[0050] 삭제

[0051] 삭제

[0052] 삭제

[0053] 삭제

[0054] 삭제

[0055] 삭제

[0056] 삭제

[0057] 삭제

[0058] 삭제

[0059] 삭제

[0060] 삭제

[0061] 삭제

[0062] 삭제

[0063] 삭제

[0064] 삭제

[0065] 삭제

[0066] 삭제

[0067] 삭제

[0068] 삭제

[0069] 삭제

[0070] 삭제

[0071] 삭제

[0072] 삭제

[0073] 삭제

[0074] 삭제

[0075] 삭제

[0076] 삭제

[0077] 삭제

[0078] 삭제

[0079] 삭제

[0080] 삭제

[0081] 삭제

[0082] 삭제

[0083] 삭제

[0084] 삭제

[0085] 삭제

[0086] 삭제

[0087] 삭제

[0088] 삭제

[0089] 삭제

[0090] 삭제

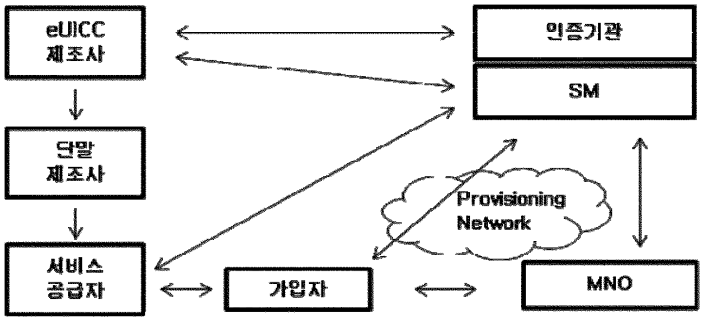
[0091] 삭제

[0092] 삭제

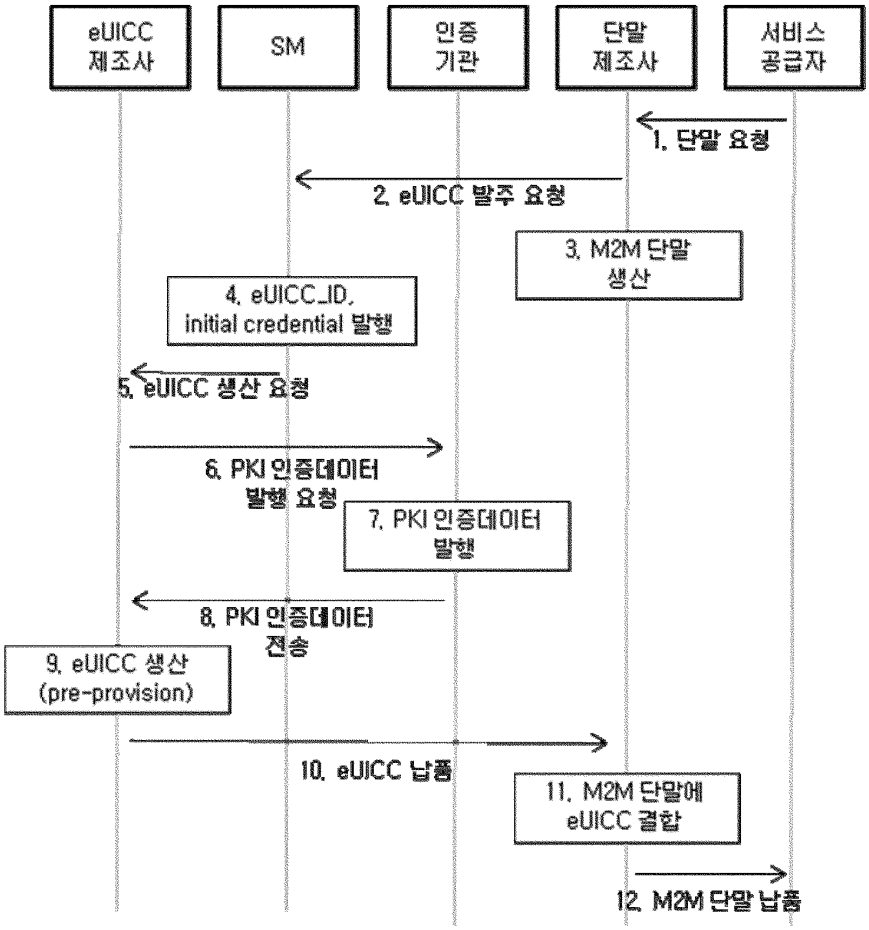
[0093] 삭제

도면

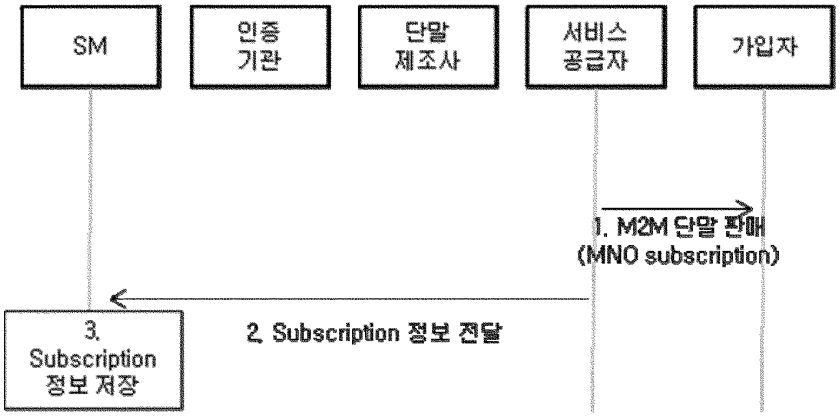
도면1



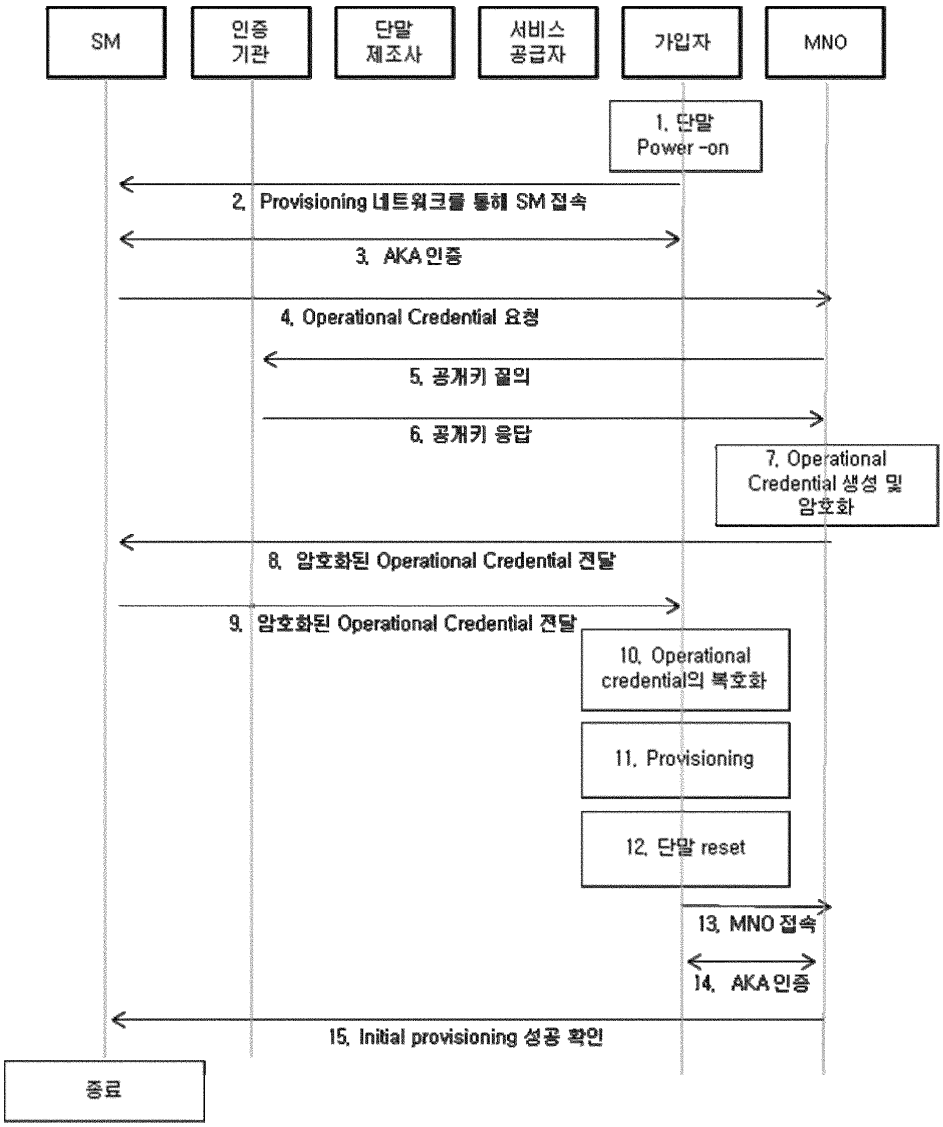
도면2



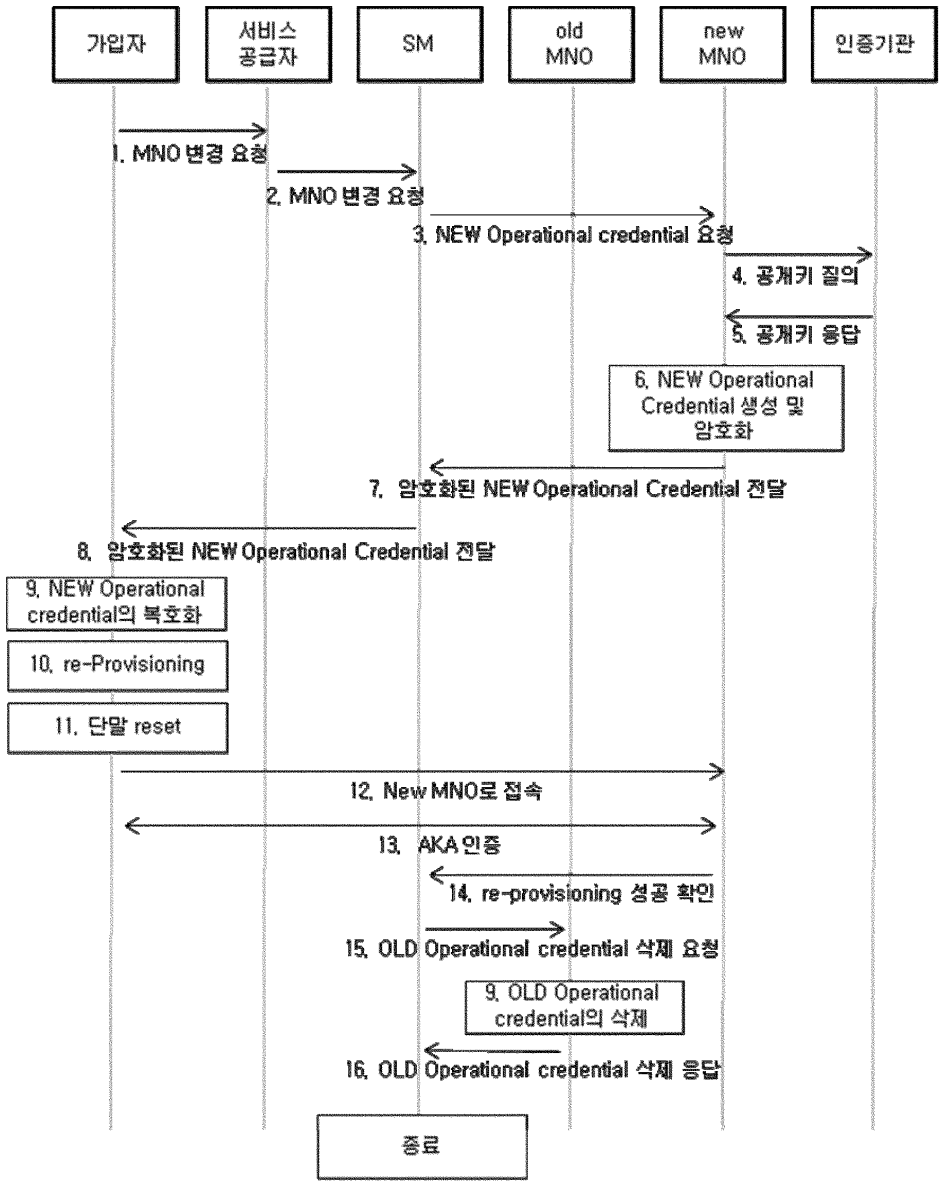
도면3


SM
인증 기관
단말 제조사
서비스 공급자
가입자
1. M2M 단말 판매 (MNO subscription)
2. Subscription 정보 전달
3. Subscription 정보 저장

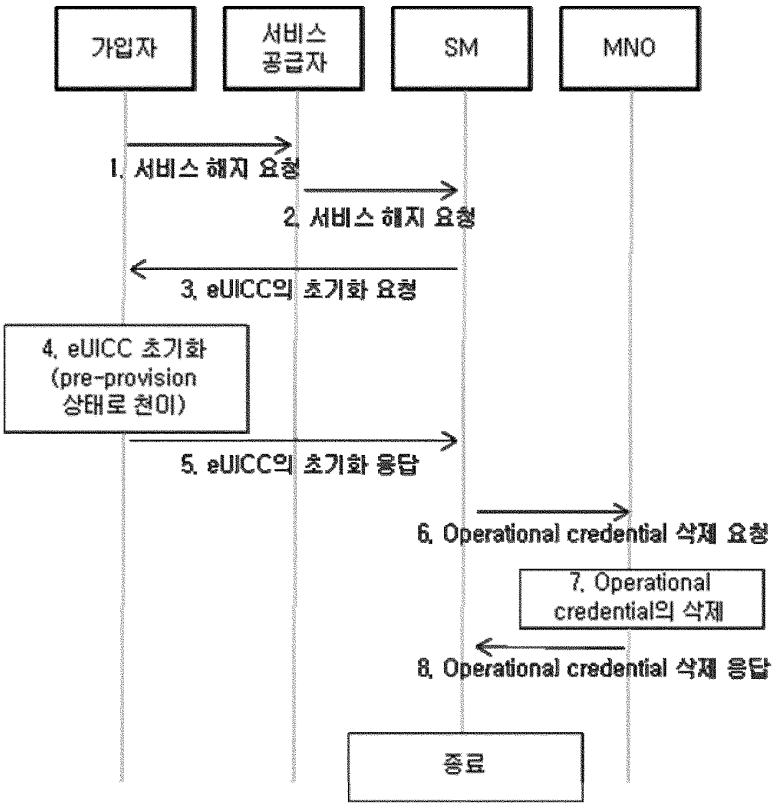
도면4


SM
인증 기관
단말 제조사
서비스 공급자
가입자
MNO
1. 단말 Power -on
2. Provisioning 네트워크를 통해 SM 접속
3. AKA 인증
4. Operational Credential 요청
5. 공개키 꾸의
6. 공개키 응답
7. Operational Credential 생성 및 암호화
8. 암호화된 Operational Credential 전달
9. 암호화된 Operational Credential 전달
10. Operational credential의 복호화
11. Provisioning
12. 단말 reset
13. MNO 접속
14. AKA 인증
15. Initial provisioning 성공 확인
종료

도면5


가입자
서비스 공급자
SM
old MNO
new MNO
인증기관
1. MNO 변경 요청
2. MNO 변경 요청
3. NEW Operational credential 요청
4. 공개키 질의
5. 공개키 응답
6. NEW Operational Credential 생성 및 암호화
7. 암호화된 NEW Operational Credential 전달
8. 암호화된 NEW Operational Credential 전달
9. NEW Operational credential의 복호화
10. re-Provisioning
11. 단말 reset
12. New MNO로 접속
13. AKA 인증
14. re-provisioning 성공 확인
15. OLD Operational credential 삭제 요청
9. OLD Operational credential의 삭제
16. OLD Operational credential 삭제 응답
종료

도면6


가입자
서비스 공급자
SM
MNO
1. 서비스 해지 요청
2. 서비스 해지 요청
3. eUICC의 초기화 요청
4. eUICC 초기화 (pre-provision 상태로 천이)
5. eUICC의 초기화 응답
6. Operational credential 삭제 요청
7. Operational credential의 삭제
8. Operational credential 삭제 응답
종료