(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년07월27일
(11) 등록번호 10-2138315
(24) 등록일자 2020년07월21일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2013-0061688
(22) 출원일자 2013년05월30일
심사청구일자 2018년05월30일
(65) 공개번호 10-2014-0140820
(43) 공개일자 2014년12월10일
(56) 선행기술조사문헌
KR1020120044326 A*
WO2013036011 A2*
A. Menezes 외 2명, Handbook of Applied Cryptography, Chapter.12, CRC Press (1996.)*
KR1020090013270 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
이덕기
서울 서초구 신반포로 32, 2동 108호 (반포동, 주공아파트)
서경주
서울 강남구 영동대로114길 56, 1차 101동 1102호 (삼성동, 삼성래미안)
손중제
경기 용인시 기흥구 동백2로 37, 4106동 603호 (중동, 어은목마을대원칸타빌)
(74) 대리인
윤동열

전체 청구항 수 : 총 20 항 심사관 : 양종필

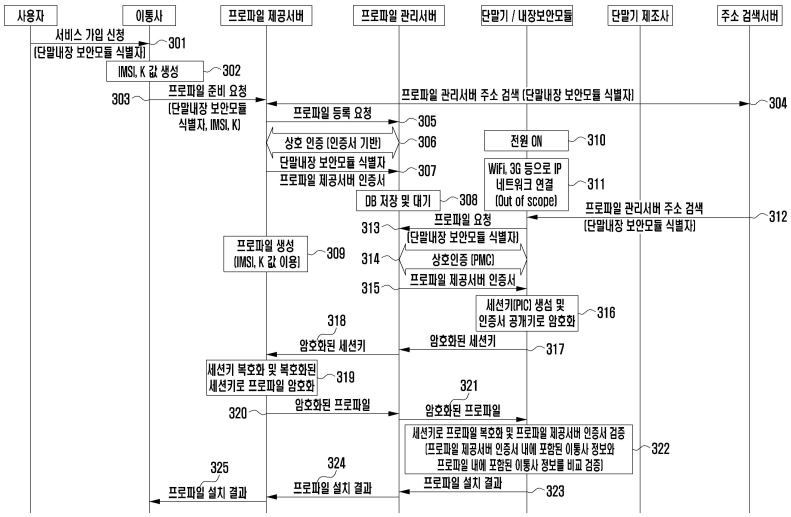
(54) 발명의 명칭 **프로파일 설치를 위한 방법 및 장치**

(57) 요 약

본 발명은 프로파일 설치를 위한 방법 및 장치에 관한 것으로, 더욱 상세하게는 UICC를 대체하여 단말기 내부에 착탈이 불가능하게끔 내장이 되는 보안모듈(Universal Integrated Circuit Card; UICC)에 이동통신 가입자 정보(프로파일)를 원격에서 설치하고 제거하는 등의 관리 방법에 관한 것이다.

이에 따른 본 발명은, 단말 내장 보안 모듈을 포함하는 단말을 위한 서버의 프로파일 설치 방법으로, 상기 단말로부터 상기 단말 내장 보안 모듈의 식별자를 포함하는 프로파일 설치 요청을 수신하는 단계, 상기 설치 요청에 대응하는 암호화된 프로파일을 수신하는 단계 및 상기 단말로 상기 암호화된 프로파일을 전송하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법 및 서버에 관한 것이다.

대 표 도



명 세 서

청구범위

청구항 1

내장 보안 모듈(embedded security module)을 포함하는 단말을 위한 프로파일 관리 서버의 프로파일 설치 방법에 있어서,

프로파일 제공 서버로부터, 디지털 인증서를 포함하며 프로파일 등록을 요청하기 위한 제1 메시지를 수신하는 단계;

상기 단말로부터, 상기 내장 보안 모듈의 식별자를 포함하며 프로파일을 요청하기 위한 제2 메시지를 수신하는 단계;

상기 단말로 상기 디지털 인증서를 전송하는 단계;

상기 단말로부터, 상기 디지털 인증서에 기초하여 암호화된 세션 키를 수신하는 단계;

상기 프로파일 제공 서버로 상기 암호화된 세션 키를 전송하는 단계;

상기 프로파일 제공 서버로부터, 상기 제2 메시지에 대응되며 상기 암호화된 세션 키에 기초하여 생성된 암호화된 프로파일을 수신하는 단계; 및

상기 단말로 상기 암호화된 프로파일을 전송하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 2

제1항에 있어서,

상기 제2 메시지를 수신한 후, 상기 단말과, 아이디/패스워드, 비밀 키 및 상기 디지털 인증서 중 적어도 하나를 이용하여 상호 인증을 수행하는 단계를 더 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 3

제1항에 있어서,

상기 제1 메시지는 상기 내장 보안 모듈의 식별자를 포함하고,

상기 방법은, 상기 프로파일 제공 서버의 식별 정보, 상기 내장 보안 모듈의 식별자 및 상기 디지털 인증서 중 적어도 하나를 포함하는 정보를 저장하는 단계를 더 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 4

제1항에 있어서,

상기 암호화된 세션 키는 상기 디지털 인증서에 포함된 공개 키와 쌍을 이루는 개인 키로 복호화되고,

상기 암호화된 프로파일은 상기 복호화된 세션 키로 암호화되는 것을 특징으로 하는 프로파일 설치 방법.

청구항 5

내장 보안 모듈(embedded security module)을 포함하는 단말을 위한 프로파일 제공 서버의 프로파일 설치 방법에 있어서,

프로파일 관리 서버로, 디지털 인증서를 포함하며 프로파일 등록을 요청하기 위한 제1 메시지를 전송하는 단계;

상기 내장 보안 모듈의 식별자에 대응하는 프로파일을 생성하는 단계;

상기 프로파일 관리 서버로부터, 상기 디지털 인증서에 기초하여 암호화된, 상기 단말의 세션 키를 수신하는 단계;

프로파일을 요청하기 위한 제2 메시지에 응답하여, 상기 암호화된 세션 키에 기초하여 상기 프로파일을 암호화

하는 단계; 및

상기 암호화된 프로파일을 전송하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 6

제5항에 있어서,

상기 프로파일을 암호화하는 단계는,

상기 세션 키를 획득하기 위해 상기 암호화된 세션 키를 복호화하는 단계; 및

상기 세션 키를 이용하여 상기 프로파일을 암호화하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 7

제5항에 있어서,

상기 암호화된 프로파일을 전송하는 단계는,

상기 프로파일에 대한 검증 값(verification value)을 상기 암호화된 프로파일과 함께 전송하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 8

제5항에 있어서,

상기 단말로부터 상기 내장 보안 모듈의 식별자를 수신하는 단계; 및

상기 내장 보안 모듈의 식별자를 더 포함하는 상기 제1 메시지를 전송하는 단계를 더 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 9

제8항에 있어서,

상기 제 1 메시지를 전송하는 단계는,

주소 검색 서버로 상기 내장 보안 모듈의 식별자를 전송하는 단계; 및

상기 주소 검색 서버로부터, 상기 내장 보안 모듈의 식별자에 매핑되는 상기 프로파일 제공 서버의 주소를 수신하는 단계를 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 10

제5항에 있어서,

상기 디지털 인증서에 포함된 공개 키와 쌍을 이루는 개인 키로 상기 암호화된 세션 키를 복호화하는 단계; 및

상기 복호화된 세션 키를 이용하여 상기 프로파일을 암호화하는 단계를 더 포함하는 것을 특징으로 하는 프로파일 설치 방법.

청구항 11

내장 보안 모듈(embedded security module)을 포함하는 단말에 프로파일을 설치하기 위한 프로파일 관리 서버에 있어서,

상기 단말과 데이터 통신을 수행하는 통신부; 및

상기 통신부를 제어하도록 설정된 제어부를 포함하되,

상기 제어부는,

프로파일 제공 서버로부터, 디지털 인증서를 포함하며 프로파일 등록을 요청하기 위한 제1 메시지를 수신하고,
상기 단말로부터 상기 내장 보안 모듈의 식별자를 포함하는 프로파일을 요청하기 위한 제2 메시지를 수신하고,

상기 단말로 상기 디지털 인증서를 전송하고, 상기 단말로부터 상기 디지털 인증서에 기초하여 암호화된 세션 키를 수신하고, 상기 프로파일 제공 서버로 상기 암호화된 세션 키를 전송하고, 상기 프로파일 제공 서버로부터 상기 제2 메시지에 대응되며 상기 암호화된 세션 키에 기초하여 생성된 암호화된 프로파일을 수신하고, 상기 단말로 상기 암호화된 프로파일을 전송하도록 설정된 것을 특징으로 하는 프로파일 관리 서버.

청구항 12

제11항에 있어서, 상기 제어부는,

상기 제2 메시지를 수신한 후, 상기 단말과, 아이디/패스워드, 비밀 키 및 상기 디지털 인증서 중 적어도 하나를 이용하여 상호 인증을 수행하도록 설정된 것을 특징으로 하는 프로파일 관리 서버.

청구항 13

제11항에 있어서,

상기 프로파일 관리 서버는 적어도 하나의 프로파일을 저장하기 위한 저장부를 포함하고,

상기 제어부는,

상기 통신부를 통하여 상기 프로파일 제공 서버로부터 상기 내장 보안 모듈의 식별자를 포함하는 상기 제1 메시지가 수신되면, 상기 프로파일 제공 서버의 식별 정보, 상기 내장 보안 모듈의 식별자 및 상기 디지털 인증서 중 적어도 하나를 포함하는 정보를 상기 저장부에 저장하는 것을 제어하도록 설정된 것을 특징으로 하는 프로파일 관리 서버.

청구항 14

제11항에 있어서,

상기 암호화된 세션 키는 상기 디지털 인증서에 포함된 공개 키와 쌍을 이루는 개인 키로 복호화되고,

상기 암호화된 프로파일은 상기 복호화된 세션 키로 암호화되는 것을 특징으로 하는 프로파일 관리 서버.

청구항 15

내장 보안 모듈(embedded security module)을 포함하는 단말에 프로파일을 설치하기 위한 프로파일 제공 서버에 있어서,

상기 단말과 데이터 통신을 수행하는 통신부;

적어도 하나의 프로파일을 저장하도록 설정된 저장부; 및

제어부를 포함하되,

상기 제어부는,

프로파일 관리 서버로, 디지털 인증서를 포함하며 프로파일 등록을 요청하기 위한 제1 메시지를 전송하도록 상기 통신부를 제어하고,

상기 내장 보안 모듈의 식별자에 대응하는 프로파일을 생성하고,

상기 프로파일 관리 서버로부터, 상기 디지털 인증서에 기초하여 암호화된 상기 단말의 세션 키를 수신하도록 상기 통신부를 제어하고,

프로파일을 요청하기 위한 제2 메시지에 응답하여, 상기 암호화된 세션 키에 기초하여 상기 프로파일을 암호화하고,

상기 암호화된 프로파일을 전송하도록 통신부를 제어하도록 설정되는 것을 특징으로 하는 프로파일 제공 서버.

청구항 16

제15항에 있어서,

상기 제어부는,

상기 통신부를 통하여 상기 디지털 인증서를 이용하여 암호화된 상기 단말의 세션 키가 수신되면, 상기 세션 키를 획득하기 위해 상기 암호화된 세션 키를 복호화하고, 상기 세션 키를 이용하여 상기 프로파일을 암호화하도록 설정된 것을 특징으로 하는 프로파일 제공 서버.

청구항 17

제15항에 있어서,

상기 제어부는,

상기 프로파일에 대한 검증 값(verification value)을 상기 암호화된 프로파일과 함께 전송하도록 상기 통신부를 제어하도록 설정된 것을 특징으로 하는 프로파일 제공 서버.

청구항 18

제15항에 있어서,

상기 제어부는,

상기 단말로부터 상기 내장 보안 모듈의 식별자를 수신하고, 상기 내장 보안 모듈의 식별자를 더 포함하는 상기 제1 메시지를 전송하도록 상기 통신부를 제어하도록 설정된 것을 특징으로 하는 프로파일 제공 서버.

청구항 19

제18항에 있어서,

상기 제어부는,

주소 검색 서버로 상기 내장 보안 모듈의 식별자를 전송하고, 상기 주소 검색 서버로부터, 상기 내장 보안 모듈의 식별자에 매핑되는 상기 프로파일 제공 서버의 주소를 수신하도록 상기 통신부를 제어하도록 설정된 것을 특징으로 하는 프로파일 제공 서버.

청구항 20

제15항에 있어서,

상기 제어부는,

상기 디지털 인증서에 포함 된 공개 키와 쌍을 이루는 개인 키로 상기 암호화된 세션 키를 복호화하고, 상기 복호화된 세션 키를 이용하여 상기 프로파일을 암호화하도록 설정된 것을 특징으로 하는 프로파일 제공 서버.

발명의 설명

기 술 분 야

[0001] 본 발명은 프로파일 설치를 위한 방법 및 장치에 관한 것으로, 더욱 상세하게는 UICC를 대체하여 단말기 내부에 착탈이 불가능하게끔 내장이 되는 보안모듈(Universal Integrated Circuit Card; UICC)에 이동통신 가입자 정보(프로파일)를 원격에서 설치하고 제거하는 등의 관리 방법에 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.

[0003] UICC는 GSM, WCDMA, LTE 등과 같은 이동통신 네트워크에 접속 시 가입자 인증 및 트래픽 보안 키 생성을 수행하여 안전한 이동통신 이용을 가능케 한다.

[0004] UICC에는 가입자가 접속하는 이동통신 네트워크의 종류에 따라 SIM, USIM, ISIM 등의 통신 애플리케이션이 탑재된다. 또한, UICC는 전자지갑, 티켓팅, 전자여권 등과 같은 다양한 응용 애플리케이션의 탑재를 위한 상위 레벨의 보안 기능을 제공한다.

[0005] 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 애플리케이션 및 IMSI, K 값)가 사전 탑재되어 출고된다. 제조된 UICC 카드는 해당 이동통신 사업자가 납품받아 가입자에게 제공하며, 필요한 경우, OTA(Over The Air) 등의 기술을 활용하여 UICC 내 애플리케이션의 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.

발명의 내용

해결하려는 과제

[0006] 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.

[0007] Nano SIM보다 더 작은 크기의 UICC카드는 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 예상된다.

[0008] 또한, 지능형 가전제품, 전기/수도 미터기, CCTV 카메라 등 다양한 설치 환경에서 사람의 직접적인 조작 없이 이동통신 데이터망 접속을 수행하는M2M(Machine-to-Machine) 기기에는 착탈형 UICC 카드가 적합하지 않은 상황이다.

[0009] 이러한 문제점을 해결하기 위해, UICC와 유사한 기능을 수행하는 보안 모듈을 이동통신 단말기 제조 시 단말기에 내장하여, 종래의 착탈식 UICC를 대체하기 위한 요구사항이 대두하고 있다. 이러한 보안 모듈은 단말기 제조 시 단말기 내부에 장착되어 착탈이 불가능하므로, 단말기 제조 시 USIM의 IMSI, K와 같은 특정 이동통신 사업자의 네트워크 접속인증 정보를 사전 탑재하기가 불가능하며, 해당 단말을 구입한 사용자가 특정 이동통신 사업자에 가입을 한 이후에 이러한 인증정보의 설정이 가능하다.

[0010] 또한, 특정 이동통신 사업자 전용으로 제조 및 유통되던 종래의 UICC 카드와 달리, 새롭게 도입되는 단말 내장 보안 모듈은 해당 단말기를 구입한 사용자가 특정 이동통신 사업자로 가입 및 해지, 또는 다른 사업자로 가입 변경 등을 수행함에 따라 다양한 이동통신 사업자의 인증정보를 안전하고 유연하게 설치 및 관리할 수 있어야 한다.

[0011] 따라서, 본 발명은, 종래의 착탈식 UICC 카드를 대체하는 단말 내장 보안 모듈에 다양한 이동통신 사업자의 UICC 정보를 네트워크를 통해 원격에서 설치할 수 있는 안전한 방법을 제공하고자 한다.

과제의 해결 수단

[0012] 본 발명에 따른 프로파일 설치 방법은, 단말 내장 보안 모듈을 포함하는 단말을 위한 서버의 프로파일 설치 방법으로, 상기 단말로부터 상기 단말 내장 보안 모듈의 식별자를 포함하는 프로파일 설치 요청을 수신하는 단계, 상기 설치 요청에 대응하는 암호화된 프로파일을 수신하는 단계 및 상기 단말로 상기 암호화된 프로파일을 전송하는 단계를 포함하는 것을 특징으로 한다.

[0013] 또한, 본 발명에 따른 프로파일 설치 방법은, 단말 내장 보안 모듈을 포함하는 단말을 위한 서버의 프로파일 설치 방법으로, 상기 단말 내장 보안 모듈의 식별자에 대응하는 프로파일을 생성하는 단계, 상기 단말의 프로파일 설치 요청에 대응하여, 상기 프로파일을 암호화하는 단계 및 상기 암호화된 프로파일을 전송하는 단계를 포함하는 것을 특징으로 한다.

[0014] 또한, 본 발명에 따른 서버는, 단말 내장 보안 모듈을 포함하는 단말에 프로파일을 설치하기 위한 서버로, 상기 단말과 데이터 통신을 수행하는 통신부 및 상기 통신부를 통하여 상기 단말로부터 상기 단말 내장 보안 모듈의 식별자를 포함하는 프로파일 설치 요청을 수신하면, 상기 설치 요청에 대응하는 암호화된 프로파일을 수신하고, 상기 단말로 상기 암호화된 프로파일을 전송하도록 상기 통신부를 제어하는 제어부를 포함하는 것을 특징으로

한다.

[0015] 또한, 본 발명에 따른 서버는, 단말 내장 보안 모듈을 포함하는 단말에 프로파일을 설치하기 위한 서버로, 상기 단말과 데이터 통신을 수행하는 통신부, 상기 단말 내장 보안 모듈의 식별자에 대응하는 프로파일을 저장하는 저장부 및 상기 단말의 프로파일 설치 요청에 대응하여, 상기 프로파일을 암호화하고, 상기 암호화된 프로파일을 전송하도록 상기 통신부를 제어하는 제어부를 포함하는 것을 특징으로 한다.

발명의 효과

[0016] 본 발명의 바람직한 실시 예에 따르면 사용자가 구입한 이동통신 단말기의 내장 보안모듈에 이동통신사의 기존 UICC카드 정보에 해당하는 프로파일을 통신 네트워크를 통해 안전하게 전달, 설치할 수 있다. 또한, 본 발명의 실시 예에 따르면 특정 단말기의 내장 보안모듈에 대한 전체적인 관리를 담당하는 프로파일 관리 서버와, 특정 이동통신사와 연계하여 UICC 프로파일을 생성하는 프로파일 제공 서버의 역할을 분리하고, 프로파일 제공 서버에서 제공하는 디지털 인증서를 사용하여 세션 키의 암호화 및 프로파일 검증을 수행함으로써, 프로파일 제공 서버와 단말기 사이에 위치한 프로파일 관리 서버에 프로파일의 내용을 노출하지 않고 단말내장 보안모듈까지 암호화된 프로파일을 안전하게 전달할 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명에 따른 프로파일 설치 방법을 간략히 나타낸 순서도이다.

도 2는 본 발명에 따른 프로파일 설치 방법이 적용되는 통신 시스템의 구조를 나타낸 도면이다.

도 3은 본 발명에 따른 프로파일 설치 방법이 적용되는 통신 시스템의 주요 장치에 대한 구성을 나타낸 도면이다.

도 4는 본 발명에 따른 프로파일 설치 방법을 구체적으로 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 본 발명은 이동통신 단말기, 단말내장 보안모듈, 프로파일 제공 서버, 프로파일 관리 서버, 그리고 옵션 사항인 주소 검색 서버로 구성된다. 단말내장 보안모듈 내에 설치되는 프로파일은 기존 UICC 카드에 저장되는 하나 또는 복수 개의 애플리케이션 및 가입자 인증정보, 전화번호부 등의 데이터 정보를 총칭한다.

[0019] 프로파일 제공 서버는 이동통신사에 의해 직접 운영되거나, 또는 이동통신사와 완전한 신뢰 관계에 있는 다른 업체에 의해 운영될 수 있다. 비즈니스 및 계약 관계에 따라, 프로파일 제공서 버는 하나 또는 복수 개의 이동통신사를 위한 서비스를 제공할 수 있다. 프로파일 제공 서버는 해당 이동통신사에 가입하는 가입자를 위한 프로파일의 생성 및 암호화, 그리고 암호화된 프로파일을 프로파일 관리 서버로 전달하는 역할을 수행한다.

[0020] 프로파일 관리 서버는 특정한 단말내장 보안모듈에 대한 프로파일 관리를 수행하는 서버로서, 프로파일 제공 서버로부터 전달받은 암호화된 프로파일을 해당 단말내장 보안모듈로 안전하게 전송한다. 프로파일 관리 서버는 보안모듈 내에서 프로파일의 복호화 및 설치가 완료된 이후에는 프로파일의 활성화, 비활성화, 제거 등의 프로파일 관리 역할을 수행한다.

[0021] 하나의 단말내장 보안모듈에는 하나 또는 복수 개의 프로파일들이 설치될 수 있으며, 단말기가 이동통신 네트워크에 접속 시에는 설치된 프로파일들 중 하나가 선택되어 사용된다.

[0022] - 용어의 정의-

[0023] 이동통신 단말기: Mobile Device

[0024] 단말내장 보안모듈: eSE(embedded Secure Element. eUICC는 eSE의 한 종류임)

[0025] 프로파일 관리 서버: Profile Manager 프로파일 제공 서버: Profile Provider 주소 검색 서버: Address Resolution Server

[0026] 프로파일 관리용 인증정보: PMC(Profile Management Credentials)

[0027] 프로파일 관리용 사용자 인증정보: PMUC(Profile Management User Credentials)

[0028] 프로파일 제공용 인증정보: PIC(Profile Installer Credentials)

[0029] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시 예에 대한 동작 원리를 상세히 설명한다.

[0030] 도 1은 본 발명에 따른 프로파일 설치 방법을 간략히 나타낸 순서도이다. 구체적으로, 도 1은 가입자가 이동통신사에 서비스 가입을 요청한 후 단말기의 보안모듈에 UICC 프로파일이 설치되기까지의 과정을 나타낸다.

[0031] 단계 102에서, 사용자는 이동통신사에 이동통신 서비스에 대한 가입을 신청한다. 서비스 가입을 위하여 이동통신 단말기에 구비되는 단말 내장 보안모듈에는 전 세계적으로 유일한 값을 가지는 고유한 식별자가 할당될 수 있다. 본 발명의 실시 예에 따르면, 서비스 가입 요청 시, 단말 내장 보안 모듈의 식별자가 요구될 수 있다. 따라서, 서비스 가입을 신청하는 사용자가 식별자 값을 쉽게 알아낼 수 있도록 다양한 방법이 지원될 수 있다.

[0032] 예를 들어 단말내장 보안모듈 내 메모리에 저장되는 식별자 값은 단말기 화면의 메뉴 선택에 의하여 사용자가 용이하게 확인 가능하도록 표시될 수 있다. 또는 단말 내장 보안 모듈의 식별자는 단말기 전원을 켜지 않고도 값을 읽을 수 있게끔 외부 스티커 라벨에 단말기 시리얼 번호와 함께 프린트될 수 있다.

[0033] 본 발명의 실시 예에 따르면 단말내장 보안모듈의 식별자 값은 이동통신 서비스 가입 신청 시 이동통신사에 전달되어야 한다. 식별자를 이동통신사에 제공하는 방법에는, 가입자가 이동통신사의 온라인 가입 신청 화면에서 식별자 값을 직접 입력하는 방법, 단말기가 자신의 보안모듈 식별자 값을 네트워크 프로토콜을 통해 이동통신사의 서버로 전달하는 방법, 오프라인 대리점에서 서비스 가입 시 단말기 라벨을 바코드 리더기로 읽어서 이동통신사 서버에 입력하는 방법 등이 있을 수 있다.

[0034] 또한, 서비스 가입 요청 시, 프로파일 관리용 사용자 인증정보(PMUC)가 요구될 수 있다. 따라서, 서비스 가입을 신청하는 사용자가 이 PMUC 값도 쉽게 알아낼 수 있는 방법이 필요하며, 상기 단말내장 보안모듈 식별자와 동일한 방법이 사용자에게 제공될 수 있다.

[0035] 또한, 상기 프로파일 관리용 사용자 인증정보는, 좀더 안전한 보안을 위해, 사용자가 원하는 값으로 변경되어 단말내장 보안모듈에 업데이트 될 수 있다.

[0036] 서비스 가입 요청 시 사용자가 단말내장 보안모듈 식별자와 함께 이동통신사에 전달한 상기 프로파일 관리용 사용자 인증정보는, 프로파일 설치 시에 단말내장 보안모듈에 저장되어 있는 값과 비교 검증되어, 검증에 실패하면 프로파일 설치를 중단하는 데 이용될 수 있다. 이를 통해, 상기 프로파일 관리용 사용자 인증정보를 알고 있는 적법한 사람만이 상기 단말내장 보안모듈로 프로파일이 설치되도록 이동통신사에 요청할 수 있는, 사용자 레벨의 보안 메커니즘을 제공한다.

[0037] 단계 103에서, 가입 신청을 받은 이동통신사는 해당 단말기의 내장 보안모듈에 가입자를 위한 프로파일이 설치될 수 있도록 프로파일 제공 서버와 프로파일 관리 서버를 활용하여 프로파일 설치를 준비한다.

[0038] 구체적으로, 프로파일 제공 서버는 통신 네트워크를 통해 프로파일 관리 서버에 접속하여, 프로파일이 설치될 대상 단말기의 내장 보안모듈 식별자 값을 프로파일 관리 서버에 등록한다. 이때 프로파일 제공 서버는 단말내장 보안모듈 식별자와 함께, 디지털 인증서를 프로파일 관리 서버에 전달할 수 있다. 함께 전달된 디지털 인증서는 추후 단말내장 보안모듈에 의해 생성되는 세션 키의 암호화 (단계 104), 그리고 최종적으로 단말내장 보안모듈로 전송되는 프로파일에 대한 검증 시에 사용될 수 있다 (단계 106).

[0039] 프로파일 제공 서버는 가입이 요청된 단말기의 내장 보안모듈에 대한 관리를 수행하는 프로파일 관리 서버에 접속하기 위해 해당 프로파일 관리 서버의 주소를 알아내야 한다.

[0040] 일 실시 예에서, 프로파일 관리 서버의 주소 또는 식별자 값은 가입 신청 시 단말내장 보안모듈의 식별자와 함께 프로파일 제공 서버로 전달될 수 있다.

[0041] 다른 실시 예에서, 프로파일 제공 서버는 단말내장 보안모듈 식별자를 활용하여 해당 단말기의 내장 보안모듈에 대한 프로파일 관리를 담당하는 프로파일 관리 서버의 주소를 알아낼 수 있다. 식별자를 활용하여 프로파일 관리 서버의 주소를 알아내는 방법에는, 단말내장 보안모듈 식별자와 프로파일 관리 서버의 매핑 관계를 프로파일 제공 서버 내에서 테이블로 관리하는 방법, 또는 단말내장 보안모듈 식별자를 키 값으로 이용하여 외부 서버에 프로파일 관리 서버의 주소를 질의하고 외부 서버로부터 주소를 획득하는 방법 등이 사용될 수 있다. 외부서버

를 사용하는 방법의 일례로는 DNS 서버에 FQDN(Fully Qualified Domain Name) 형태로 구성된 단말내장 보안모듈의 식별자를 프로파일 관리 서버의 IP주소와 매핑하여 등록하고, DNS 서버를 상기 외부서버로 활용하는 방법이 사용될 수 있다. 또 다른 예로는 식별자를 전화번호와 같은 숫자로 구성하고, 프로파일 관리 서버의 주소는 IP주소 또는 URL과 같은 형태로 구성하여 ENUM 서버에 둘 간의 매핑 관계를 저장하고, ENUM 서버를 상기 외부서버로 활용하는 방법이 사용될 수 있다. 또 다른 예로는 단말내장 보안모듈 식별자와 프로파일 관리 서버의 매핑 관계를 전담하는 새로운 네트워크 엔티티를 정의하여, 상기 외부서버로 활용할 수 있다.

[0042] 프로파일 제공 서버에서 프로파일 관리 서버로 접속하여 보안모듈 식별자 값을 등록할 때, 서버 상호 간 또는 일방향으로 인증이 수행될 수 있으며, 인증 방식은 아이디/패스워드 기반의 인증, 공유 비밀 키를 이용한 인증, 또는 디지털 인증서를 이용한 인증방식 등이 사용될 수 있다.

[0043] 인증과정이 성공적으로 완료되고 프로파일 관리 서버에 단말내장 보안모듈 식별자 등록이 완료되면, 프로파일 관리 서버는 등록을 요청한 프로파일 제공 서버의 주소 또는 식별자, 그리고 단말내장 보안모듈 식별자를 포함한 정보를 데이터베이스에 저장하여, 추후 실행될 프로파일 설치 작업을 대기한다.

[0044] 또한, 프로파일 제공 서버는 상기 정보 이외에, 설치될 프로파일도 미리 생성하여 프로파일 관리 서버에 전달하여 데이터베이스에 저장해 놓을 수 있다.

[0045] 단계 104에서, 프로파일 관리 서버와 이동통신 단말기 간에 프로파일 설치요청이 전달된다. 설치요청 메시지는 프로파일 관리 서버에서 생성되어 이동통신 단말기로 전달되거나, 아니면 이동통신 단말기에서 생성되어 프로파일 관리 서버로 전달될 수 있다.

[0046] 프로파일 관리 서버에서 이동통신 단말기로 설치요청 메시지를 전송할 때, 프로파일 관리 서버가 이동통신 단말기에 접속하기 위한 IP주소/Port번호 또는 WAP Push 메시지를 전송할 전화번호를 모르거나, 또는 이동통신 단말기의 전원이 꺼져 있는 등의 이유로 단말기에 접속이 불가능한 경우, 프로파일 관리 서버는 해당 프로파일의 설치를 위한 정보를 내부 데이터베이스에 저장하여, 추후 이동통신 단말기로부터 설치요청 메시지를 수신했을 때 상기 정보를 활용하여 설치를 진행할 수 있다. 또는 프로파일 관리 서버는 이동통신 단말기로 접속이 가능해 질 때까지 주기적으로 설치요청 메시지 전송을 시도할 수도 있다.

[0047] 이동통신 단말기 전원이 켜지거나 또는 사용자의 명시적인 단말기 조작에 의해 새로운 프로파일 설치를 요청하는 경우 이동통신 단말기는 프로파일 관리 서버로 프로파일 설치요청 메시지를 전송할 수 있다. 이때 프로파일 관리 서버의 데이터 베이스에 프로파일 제공 서버로부터 전달받은 해당 프로파일에 설치에 대한 정보가 기 저장되어 있는 경우 프로파일 관리 서버는 바로 프로파일 설치를 진행할 수 있다(도 4에 설명된 실시 예). 만약 그렇지 않은 경우, 프로파일 관리 서버는 설치를 요청하는 이동통신 단말기의 IP주소, Port 번호 및 단말내장 보안모듈 식별자 값을 내부 데이터베이스에 저장하고 대기할 수 있다. 이 경우 프로파일 관리 서버는, 추후 상기 이동통신 단말기에 대한 프로파일 설치요청이 전달되는 시점에 상기 데이터베이스에 저장된 이동통신 단말기 정보를 이용하여 이동통신 단말기에 접속하고 프로파일 설치를 진행할 수 있다. 또는, 이동통신 단말기로부터 프로파일 설치요청 메시지를 수신한 프로파일 관리 서버는 내부 데이터베이스에 해당 프로파일 설치에 대한 정보가 저장되어 있지 않은 경우, 프로파일 제공 서버에 역으로 접속하여 상기 이동통신 단말기에 대한 프로파일 제공을 요청하고 프로파일 설치를 진행할 수도 있다.

[0048] 프로파일 관리 서버가 프로파일 제공 서버로 접속을 시도하는 경우, 프로파일 관리 서버는 프로파일 제공 서버의 접속주소 정보를 알고 있어야 한다. 이를 위해, 프로파일 관리 서버는 이동통신 단말기로부터 프로파일 설치요청 메시지 수신 시 MCC+MNC와 같은 이동통신사 정보를 함께 전달받고, 상기 이동통신사 정보로부터 프로파일 제공 서버의 주소를 알아낼 수 있다. 상기 프로파일 제공 서버의 주소를 알아내는 방법으로는, 이동통신사 정보와 프로파일 제공 서버 주소의 매핑 관계를 프로파일 관리 서버의 데이터베이스 내에 관리하는 방법이 사용될 수 있다. 또는, 프로파일 관리 서버가 이동통신사 정보를 가지고 주소 검색 서버에 질의하여, 프로파일 제공 서버의 주소를 획득하는 방법이 사용될 수 있다.

[0049] 설치요청 메시지 전달 후 프로파일 관리 서버와 이동통신 단말기 간 상호인증 또는 일 방향 인증이 수행될 수 있다. 상기 과정에서 인증 방식은 사용자 아이디와 패스워드를 이용한 인증, 공유 비밀 키를 이용한 인증, 또는 디지털 인증서를 이용한 인증방식 등이 사용될 수 있다.

[0050] 인증 과정이 완료된 후, 프로파일 관리 서버는 단계 103에서 수신한 디지털 인증서를 단말기에 전달한다. 인증서를 전달받은 단말내장 보안모듈은 단계 105에서 프로파일을 암호화하기 위한 세션 키를 생성하고, 디지털 인증서 내에 포함된 공개키로 세션 키를 암호화한다. 또한, 단말 내장 보안 모듈은 암호화된 세션 키를 프로파일

관리 서버에 전달한다. 추가로, 단말내장 보안모듈은, 추후 단계 106에서의 사용을 위해, 상기 세션 키와 상기 디지털 인증서를 내부 메모리에 저장한다.

[0051] 암호화된 세션 키를 수신한 프로파일 관리 서버는 상기 세션 키를 암호화된 상태 그대로 프로파일 제공 서버에 전달한다.

[0052] 단계 105에서, 프로파일 제공 서버는 디지털 인증서에 포함된 공개 키와 한 쌍을 이루는 개인 키를 사용하여 암호화된 세션 키를 복호화한다. 또한, 프로파일 제공 서버는 복호화된 세션 키를 이용하여 프로파일을 암호화한 후, 암호화된 프로파일을 프로파일 관리 서버로 전달한다. 이때 암호화된 프로파일과 함께, 프로파일에 대한 송신자 인증과 메시지 무결성 검증을 위한 프로파일 검증 값이 전달될 수 있다.

[0053] 프로파일 검증 값은 상기 복호화된 세션 키와 상기 프로파일을 연접하여 SHA 1과 같은 해쉬 함수를 적용함으로써 생성될 수 있다. 또는 프로파일 검증 값은 상기 복호화된 세션 키와 상기 프로파일을 HMAC-SHA1 등의 함수에 적용함으로써 생성될 수 있다. 또 다른 방법으로는 프로파일 검증 값은 상기 디지털 인증서의 개인키로 상기 프로파일에 대해 SHA1withRSA와 같은 전자서명을 수행함으로써 생성될 수 있다.

[0054] 프로파일 관리 서버는 전달받은 암호화된 프로파일 및 프로파일 검증 값을 단말기로 전송한다.

[0055] 단계 106에서, 단말내장 보안모듈은 암호화된 프로파일을 단계 104에서 저장했던 세션 키를 이용하여 복호화한다. 그리고 단말내장 보안 모듈은 암호화된 프로파일과 함께 전달받은 검증 값을 상기 세션 키 또는 상기 디지털 인증서의 공개 키를 사용하여 검증한다.

[0056] 검증 값의 검증이 실패하면 단말내장 보안모듈은 프로파일 설치 과정을 중단하고 프로파일 관리 서버로 실패 메시지를 전달한다.

[0057] 반대로, 검증 값의 검증이 성공하면 단말내장 보안 모듈은 상기 디지털 인증서에 대한 검증을 수행한다.

[0058] 상기 디지털 인증서의 정당성 검증을 위해, 상기 단말내장 보안모듈은 디지털 인증서 내에 포함된 특정 정보와, 복호화 및 검증이 완료된 상기 프로파일 내에 포함된 특정 정보가 일치하는지 확인한다.

[0059] 한편, 상기 특정 정보의 예로 이동통신사 정보가 이용될 수 있다. 예를 들어 프로파일 내에 포함된 USIM 애플리케이션의 IMSI 값은 MCC, MNC, MSIN 정보를 포함하고 있으며, 단말내장 보안 모듈은 MCC와 MNC 값을 이용하여 이동통신사 정보를 확인할 수 있다. 또는 프로파일 내의 다른 파일 또는 필드에 이동통신사 정보가 포함될 수 있으며, 단말내장 보안 모듈은 이를 정당성 검증에 이용할 수 있다.

[0060] 상기 디지털 인증서의 정당성 검증을 위해, 상기 디지털 인증서 내에도 이동통신사 정보가 포함될 수 있다. 예를 들어 디지털 인증서의 DN(Distinguished Name) 필드 또는 다른 확장 필드에 이동통신사 정보가 포함될 수 있다. 디지털 인증서 내에 포함된 정보는 인증서를 발행한 인증기관에 의해 서명되어 있어 제 3자에 의해 수정 및 변경이 불가능하므로, 단말내장 보안모듈은 인증서 내에 포함된 이동통신사 정보와, 프로파일 내에 포함된 이동통신사 정보의 비교를 통해 해당 프로파일이 정당한 인증서를 통해 암호화 처리가 된 것임을 검증할 수 있다. 이동통신사 정보는, 프로파일 제공 서버가 전달한 정당한 인증서가, 통신 경로 중간에 있는 누군가에 의해 정당하지 않은 인증서로 교체되어 단말로 전송되는 Man-in-the-middle 보안 공격을 방지하기 위해 사용될 수 있다.

[0061] 단계 104에서, 프로파일 관리 서버는 단계 103에서 수신한 프로파일 제공 서버의 인증서 대신 자기 자신의 인증서 또는 제 3의 인증서를 단말기에 전달할 수 있다. 이렇게 되면 단말 내장 보안 모듈은 단말내장 보안모듈이 생성한 세션 키를 프로파일 관리 서버가 중간에서 바꿔치기한 부정한 인증서의 공개키로 암호화하게 된다. 부정한 공개 키로 암호화된 세션 키가 프로파일 관리 서버로 전달되면, 프로파일 관리 서버는 부정하게 전달된 인증서의 개인키로 상기 세션 키를 복호화할 수 있으며, 단계 105에서 전달되는 암호화된 프로파일을 상기 복호화된 세션 키를 이용하여 복호화하여 가로챌 수 있다.

[0062] 하지만, 디지털 인증서에 이동통신사 정보가 포함되면, 단계 106에서 단말내장 보안모듈은 인증서에 포함된 이동통신사 정보를 프로파일 내에 포함된 이동통신사 정보와 비교 검증할 수 있고, 검증에 실패 시 프로파일을 삭제하고 에러 처리를 하여(단계 108), 중간에서 가로챈 프로파일을 프로파일 관리 서버가 이용할 수 없도록 함으로써, Man-in-the-middle 공격을 방지할 수 있다.

[0063] 디지털 인증서의 검증이 실패하면 단말내장 보안모듈은 프로파일 설치 과정을 중단하고 프로파일 관리 서버로 실패 메시지를 전달한다.

[0064] 반면, 상기 이동통신사 정보의 비교 검증을 포함한 디지털 인증서의 검증이 성공하면, 단말내장 보안모듈은 단

계 107에서 해당 프로파일을 내부 메모리에 저장 및 설치하여 이동통신 서비스에 사용될 수 있는 상태로 만들 수 있다.

[0065] 도 2는 본 발명에 따른 프로파일 설치 방법이 적용되는 통신 시스템의 구조를 나타낸 도면이다.

[0066] 도 2를 참조하면, 통신 시스템은 단말기 제조사(210), 단말기(220), 이동통신사(230), 프로파일 제공 서버(240), 인증서 발급기관(250), 주소 검색 서버(260), 프로파일 관리 서버(270)를 포함하여 구성될 수 있다.

[0067] 단말기 제조사(210)는 단말기(220)를 제조하여 판매한다. 단말기 제조사(210)는 단말기(220) 내에 내장 보안 모듈(221)을 실장하여 제조할 수 있다. 단말 내장 보안 모듈(221)은 고유의 식별자를 가질 수 있으며, 단말기 제조사(210)는 단말기(220)에 물리적으로 또는 소프트웨어적으로 단말 내장 보안 모듈(221)의 식별자를 표기할 수 있다.

[0068] 단말기(220)는 내장 보안 모듈(221)에 저장된 프로파일을 이용하여 프로파일에 대응하는 이동통신 망의 통신망을 통해 데이터 통신을 수행한다. 단말기(220)는 사용자의 요청 또는 단말기 제조사(210)의 요청에 따라 프로파일을 설치하기 위한 동작을 수행할 수 있다. 구체적으로, 단말기(220)는 프로파일 관리 서버(270)로 단말 내장 보안 모듈(221)의 식별자를 포함하여 프로파일 요청을 전송할 수 있다. 이때, 단말기(220)는 프로파일 관리 서버(270)와 인증을 수행할 수 있다. 프로파일 관리 서버(270)로부터 디지털 인증서가 수신되면, 단말기(220)는 세션 키를 생성하여 디지털 인증서의 공개 키로 암호화하고 이를 프로파일 관리 서버(270)로 전송한다. 이후, 프로파일 관리 서버(270)로부터 암호화된 프로파일이 전송되면, 단말기(220)는 세션 키로 프로파일을 복호화하고 단말내장 보안 모듈(221)에 설치한다.

[0069] 본 발명의 통신 시스템에는 적어도 하나의 이동통신사(230a, 230b, 230c)가 존재할 수 있다. 이동통신사(230a, 230b, 230c)는 단말기(220)에 통신 서비스를 제공한다. 이동통신사(230a, 230b, 230c)는 프로파일 제공 서버(240a, 240b, 240c)를 운영할 수 있으며, 단말기(220) 사용자가 서비스 가입을 신청하면, 프로파일 제공 서버(240a, 240b, 240c)를 이용하여, 단말기(220)의 프로파일 설치를 도울 수 있다.

[0070] 적어도 하나의 이동통신사(230a, 230b, 230c) 각각은 별개의 프로파일 제공 서버(240a, 240b, 240c)를 운영할 수 있다. 또는, 신뢰할 수 있는 계약 관계에 의해 하나의 프로파일 제공 서버가 복수의 이동통신사를 위한 서비스를 제공할 수 있다. 프로파일 제공 서버(240a, 240b, 240c)는 이동통신사(230a, 230b, 230c)로부터 프로파일 준비 요청이 수신되면, 해당 단말기(220)에 대응하는 프로파일 관리 서버(270)로 프로파일 등록을 요청한다. 이때, 단말기(220)에 대응하는 프로파일 관리 서버(270)의 주소는 주소 검색 서버(260)로부터 획득될 수 있다. 프로파일 제공 서버(240a, 240b, 240c)는 프로파일 관리 서버(270)와 상호인증을 수행할 수 있으며, 프로파일 관리 서버(270)로 단말기(220)의 내장 보안모듈 식별자와 디지털 인증서를 전달할 수 있다. 이후에, 프로파일 제공 서버(240a, 240b, 240c)는 프로파일을 생성 및 관리하고, 단말기(220)의 암호화된 세션 키가 수신되면, 디지털 인증서의 공개 키와 쌍을 이루는 개인 키로 세션 키를 복호화하여 획득한다. 또한, 프로파일 제공 서버(240a, 240b, 240c)는 획득한 세션 키를 이용하여 프로파일을 암호화하고 암호화된 프로파일을 프로파일 관리 서버(270)로 전달하여 단말기(220)가 프로파일을 획득할 수 있도록 한다.

[0071] 인증서 발급 기관(250)은 단말기(220)의 프로파일 설치를 위하여 디지털 인증서를 발급할 수 있다. 인증서 발급 기관(250)은 공인된 디지털 인증서를 프로파일 제공 서버(240a, 240b, 240c)로 제공할 수 있다.

[0072] 주소 검색 서버(260)는 프로파일 제공 서버(240a, 240b, 240c)가 특정 단말기(220)에 대응하는 프로파일 관리 서버(270)의 주소 또는 식별자를 검색할 수 있도록 한다. 주소 검색 서버(260)는 FQDN(Fully Qualified Domain Name) 형태로 구성된 단말내장 보안모듈의 식별자를 프로파일 관리 서버의 IP주소와 매핑하여 등록할 수 있다. 또는, 주소 검색 서버(260)는 식별자를 전화번호와 같은 숫자로 구성하고, 프로파일 관리 서버의 주소는 IP주소 또는 URL과 같은 형태로 구성하여 ENUM 서버에 둘 간의 매핑 관계를 저장할 수 있다. 이때, 주소 검색 서버(260)는 DNS 서버 또는 ENUM 서버일 수 있다.

[0073] 프로파일 관리 서버(270)는 프로파일 제공 서버(240a, 240b, 240c)로부터 프로파일 등록 요청이 수신되면, 등록 요청에 포함된 단말 내장 보안 모듈(221)의 식별자와 디지털 인증서를 저장할 수 있다. 또한, 프로파일 관리 서버(270)는 단말기(220)로부터 프로파일 설치 요청이 전달되면, 단말기(220)와 상호인증을 수행한 후, 단말기(220)로 디지털 인증서를 전송한다. 또한, 프로파일 관리 서버(270)는 단말기(220)로부터 수신된 암호화된 세션 키를 프로파일 제공 서버(240a, 240b, 240c)로 전달하고, 프로파일 제공 서버(240a, 240b, 240c)로부터 수신된

암호화된 프로파일을 단말기(220)로 전달한다.

[0074] 도 2에 도시된 구성 요소들이 모두 필수 구성 요소는 아니어서, 도 2에 도시된 것보다 더 많거나 적은 구성 요소에 의하여 통신 시스템이 구성될 수 있다.

[0075] 도 3은 본 발명에 따른 프로파일 설치 방법이 적용되는 통신 시스템의 주요 장치에 대한 구성을 나타낸 도면이다. 구체적으로, 도 3은 단말기(220), 프로파일 관리 서버(270) 및 프로파일 제공 서버(240)의 구성을 나타내었다.

[0076] 단말기(220)는 내장 보안 모듈(221), 제어부(222), 통신부(233)를 포함하여 구성될 수 있다.

[0077] 내장 보안 모듈(221)은 프로파일 설치 및 관리에 필요한 인증 정보를 저장하며, 하나 이상의 프로파일이 설치되어 저장될 수 있다. 인증정보는 프로파일 관리 서버(270)와의 인증을 위한 정보를 포함할 수 있다. 또한, 인증정보는 프로파일 제공 서버(240)와의 인증을 위한 정보를 포함할 수 있다. 또한, 인증 정보는 사용자의 인증을 위한 정보를 포함할 수 있다.

[0078] 단말 내장 보안 모듈(221)은 본 발명에 따른 프로파일 설치 동작을 수행할 수 있으며, 이를 위하여 별도의 제어부를 포함할 수 있다.

[0079] 제어부(222)는 내장 보안 모듈(221)에 프로파일을 설치하기 위한 동작을 수행한다. 제어부(222)는 단말 내장 보안 모듈(221)과 일체형으로 구성되거나 별개로 구성될 수 있다.

[0080] 구체적으로, 제어부(222)는 내장 보안 모듈(221)의 식별자를 포함하는 프로파일 설치 요청, 암호화된 세션 키 등을 서버로 전송하도록 통신부(223)를 제어한다. 또한, 제어부(222)는 디지털 인증서의 공개 키를 이용하여 세션 키를 암호화하거나, 수신된 암호화된 프로파일을 복호화할 수 있다.

[0081] 통신부(223)는 서버와 데이터 통신을 수행할 수 있다.

[0082] 프로파일 관리 서버(270)는 통신부(271), 제어부(272), 저장부(273)를 포함하여 구성될 수 있다.

[0083] 통신부(271)는 단말기(220) 또는 프로파일 제공 서버(240)와 데이터 통신을 수행한다.

[0084] 제어부(272)는 단말기(220)로부터 단말 내장 보안 모듈(221)의 식별자를 포함하는 프로파일 설치 요청이 수신되면, 프로파일 제공 서버(240)로부터 암호화된 프로파일을 수신하여 단말기(220)로 전송한다. 또한, 제어부(272)는 단말기(220)로 디지털 인증서를 전송하고, 단말기(220)로부터 암호화된 세션 키를 수신하여 프로파일 제공 서버(240)로 전달한다. 또한, 제어부(272)는 단말기(220)와 상호 인증을 위한 동작을 수행할 수 있다.

[0085] 저장부(273)는 단말 내장 보안 모듈(221)의 식별자, 프로파일, 디지털 인증서를 임시 또는 영구적으로 저장할 수 있다.

[0086] 프로파일 제공 서버(240)는 통신부(241), 제어부(242), 저장부(243)를 포함하여 구성될 수 있다.

[0087] 통신부(241)는 단말기(220) 또는 프로파일 관리 서버(270)와 데이터 통신을 수행한다.

[0088] 제어부(242)는 단말기(220)의 프로파일 설치 요청에 대응하여, 프로파일을 암호화하고, 암호화된 프로파일을 프로파일 관리 서버(270)로 전송한다. 또한, 제어부(242)는 암호화된 단말기(220)의 세션 키가 전송되면, 세션 키를 복호화하여 획득하고, 세션 키를 이용하여 프로파일을 암호화한다. 이때, 제어부(242)는 프로파일에 대한 검증 값을 암호화된 프로파일과 함께 프로파일 관리 서버(270)로 전송할 수 있다.

[0089] 저장부(243)는 하나 이상의 프로파일 및 디지털 인증서를 저장할 수 있다.

[0090] 도 4는 본 발명에 따른 프로파일 설치 방법을 구체적으로 나타낸 흐름도이다.

[0091] 도 4의 실시 예에서, 프로파일 제공 서버는 이동통신사 정보를 포함하는 디지털 인증서를 발급받은 상태이며, 프로파일 관리 서버 역시 디지털 인증서를 발급받은 상태이다. 단말기 제조사는 내장보안 모듈을 포함하는 단말기를 제조, 판매할 수 있다. 이때, 단말기 제조사는 프로파일 관리용 인증 정보(PMC: 예를 들어, 128bit 인증키) 및 내장 보안 모듈 식별자를 단말기에 포함하여 제조할 수 있다. 단말기 제조사는 단말내장 보안 모듈 식별자 및 PMC 인증 정보를 프로파일 관리 서버로 전달할 수 있고, 단말내장 보안 모듈 식별자와 프로파일 관리 서

버의 매핑 관계를 주소 검색 서버에 제공할 수 있다.

[0092] 사용자가 단말기를 구입하면, 사용자는 이동통신사로 서비스 가입을 신청하게 된다(301). 이때, 서비스 가입을 위하여 이동통신 단말기에 구비되는 단말 내장 보안모듈에는 전 세계적으로 유일한 값을 가지는 고유한 식별자가 할당될 수 있다. 본 발명의 실시 예에 따르면, 서비스 가입 요청 시, 단말 내장 보안 모듈의 식별자가 요구될 수 있다. 따라서, 서비스 가입을 신청하는 사용자가 식별자 값을 쉽게 알아낼 수 있도록 다양한 방법이 지원될 수 있다.

[0093] 예를 들어 단말내장 보안모듈 내 메모리에 저장되는 식별자 값은 단말기 화면의 메뉴 선택에 의하여 사용자가 용이하게 확인 가능하도록 표시될 수 있다. 또는 단말 내장 보안 모듈의 식별자는 단말기 전원을 켜지 않고도 값을 읽을 수 있게끔 외부 스티커 라벨에 단말기 시리얼 번호와 함께 프린트될 수 있다.

[0094] 본 발명의 실시 예에 따르면 단말내장 보안모듈의 식별자 값은 이동통신 서비스 가입 신청 시 이동통신사에 전달되어야 한다. 식별자를 이동통신사에 제공하는 방법에는, 가입자가 이동통신사의 온라인 가입 신청 화면에서 식별자 값을 직접 입력하는 방법, 단말기가 자신의 보안모듈 식별자 값을 온라인 가입 서버에 네트워크 프로토콜을 통해 이동통신사로 전달하는 방법, 오프라인 대리점에서 서비스 가입 시 단말기 라벨을 바코드 리더기로 읽어서 이동통신사 서버에 입력하는 방법 등이 있을 수 있다.

[0095] 가입 신청을 받은 이동통신사는 해당 단말기의 내장 보안모듈에 가입자를 위한 프로파일이 설치될 수 있도록 프로파일 제공 서버와 프로파일 관리 서버를 활용하여 프로파일 설치를 준비한다. 이때, 이동통신사는 해당 단말기의 내장 보안 모듈에 대한 프로파일을 구성하기 위한 정보로써, IMSI와 비밀 키 K 값을 생성할 수 있다(302). 그리고 이동통신사는 프로파일 제공 서버로, 단말내장 보안모듈 식별자와 프로파일 정보를 전달한다(303).

[0096] 이후에, 프로파일 제공 서버는 통신 네트워크를 통해 프로파일 관리 서버에 접속하여, 프로파일이 설치될 대상 단말기의 내장 보안모듈 식별자 값을 프로파일 관리 서버에 등록한다.

[0097] 이를 위하여, 프로파일 제공 서버는 가입이 요청된 단말기의 내장 보안모듈에 대한 관리를 수행하는 프로파일 관리 서버에 접속하기 위해 해당 프로파일 관리 서버의 주소를 획득한다(304).

[0098] 일 실시 예에서, 프로파일 관리 서버의 주소 또는 식별자 값은 가입 신청 시 가입자가 단말내장 보안모듈의 식별자와 함께 프로파일 제공 서버로 전달될 수 있다.

[0099] 다른 실시 예에서, 프로파일 제공 서버는 단말내장 보안모듈 식별자를 활용하여 해당 단말기의 내장 보안모듈에 대한 프로파일 관리를 담당하는 프로파일 관리 서버의 주소를 알아낼 수 있다. 식별자를 활용하여 프로파일 관리 서버의 주소를 알아내는 방법에는, 단말내장 보안모듈 식별자와 프로파일 관리 서버의 매핑 관계를 프로파일 제공 서버 내에서 테이블로 관리하는 방법, 또는 도 4에 도시된 것과 같이, 단말내장 보안모듈 식별자를 키 값으로 이용하여 외부 서버에 프로파일 관리 서버의 주소를 질의하고 외부 서버로부터 주소를 획득하는 방법 등이 사용될 수 있다. 외부서버를 사용하는 방법의 일례로는 DNS 서버에 FQDN(Fully Qualified Domain Name) 형태로 구성된 단말내장 보안모듈의 식별자를 프로파일 관리 서버의 IP주소와 매핑하여 등록하고, DNS 서버를 상기 외부서버로 활용하는 방법이 사용될 수 있다. 또 다른 예로는 식별자를 전화번호와 같은 숫자로 구성하고, 프로파일 관리 서버의 주소는 IP주소 또는 URL과 같은 형태로 구성하여 ENUM 서버에 둘 간의 매핑 관계를 저장하고, ENUM 서버를 상기 외부서버로 활용하는 방법이 사용될 수 있다. 또 다른 예로는 단말내장 보안모듈 식별자와 프로파일 관리 서버의 매핑 관계를 전담하는 새로운 네트워크 엔티티를 정의하여, 상기 외부서버로 활용할 수 있다.

[0100] 주소를 획득한 후, 프로파일 제공 서버는 프로파일 관리 서버로 프로파일 등록을 요청한다(305). 이때, 프로파일 제공 서버는, 프로파일 관리 서버와 서버 상호 간 또는 일방향 인증을 수행할 수 있다(306). 인증 방식은 아이디/패스워드 기반의 인증, 공유 비밀 키를 이용한 인증, 또는 디지털 인증서를 이용한 인증방식 등이 사용될 수 있다.

[0101] 인증과정이 성공적으로 완료되면, 프로파일 제공 서버는 단말내장 보안모듈 식별자를 프로파일 관리 서버로 전달한다(307). 이때, 프로파일 제공 서버는 디지털 인증서를 함께 프로파일 관리 서버에 전달할 수 있다. 함께 전달된 디지털 인증서는 추후 단말내장 보안모듈에 의해 생성되는 세션 키의 암호화, 그리고 최종적으로 단말내장 보안모듈로 전송되는 프로파일에 대한 검증 시에 사용될 수 있다.

[0102] 프로파일 관리 서버에 단말내장 보안모듈 식별자 등록이 완료되면, 프로파일 관리 서버는 등록을 요청한 프로파일 제공 서버의 주소 또는 식별자, 그리고 단말내장 보안모듈 식별자를 포함한 정보를 데이터베이스에

저장하여, 추후 실행될 프로파일 설치 작업을 대기한다(308). 또한, 프로파일 제공 서버는 상기 정보 이외에, 설치될 프로파일도 미리 생성하여 프로파일 관리 서버에 전달하여 데이터베이스에 저장해 놓을 수 있다.

[0103] 이때, 프로파일 제공 서버 역시, 프로파일을 생성하고 저장하여 관리할 수 있다(309).

[0104] 이후에, 사용자가 서비스를 등록한 단말기의 전원을 켜고(310), 단말기가 무선 네트워크에 연결되면(311), 단말기는 자신의 프로파일 관리 서버 주소를 검색할 수 있다(312). 이때, 단말기는 단말 내장 보안 모듈 식별자를 이용하여 주소 검색 서버를 통해 프로파일 관리 서버에 관한 정보를 획득할 수 있다. 또는, 단말내장 보안모듈 내에 프로파일 관리 서버 주소가 저장되어 있는 경우, 단말기는 이 정보를 참조하여 프로파일 관리 서버에 관한 정보를 획득할 수 있다.

[0105] 프로파일 관리 서버 주소가 획득되면, 단말기는 프로파일 관리 서버로 프로파일을 요청한다(313). 이때, 프로파일 요청에는 단말 내장 보안모듈의 식별자가 포함될 수 있다.

[0106] 설치요청 메시지 전달 후 프로파일 관리 서버와 이동통신 단말기 간 상호인증 또는 일 방향 인증이 수행될 수 있다(314). 상기 과정에서 인증 방식은 사용자 아이디와 패스워드를 이용한 인증, 공유 비밀 키를 이용한 인증, 또는 디지털 인증서를 이용한 인증방식 등이 사용될 수 있다.

[0107] 전송요청을 수신한 프로파일 관리 서버는 프로파일 제공 서버로부터 수신된 디지털 인증서를 단말기에 전달한다(315). 인증서를 전달받은 단말기는 프로파일을 암호화하기 위한 세션 키를 생성하고, 디지털 인증서 내에 포함된 공개키로 세션 키를 암호화한다(316). 또한, 단말 내장 보안 모듈은 암호화된 세션 키를 프로파일 관리 서버에 전달한다(317). 추가로, 단말내장 보안모듈은 상기 세션 키와 상기 디지털 인증서를 내부 메모리에 저장한다.

[0108] 암호화된 세션 키를 수신한 프로파일 관리 서버는 상기 세션 키를 암호화된 상태 그대로 프로파일 제공 서버에 전달한다(318).

[0109] 암호화된 세션 키를 수신한 프로파일 제공 서버는 디지털 인증서에 포함된 공개 키와 한 쌍을 이루는 개인 키를 사용하여 암호화된 세션 키를 복호화하고, 복호화 된 세션 키를 이용하여 프로파일을 암호화한다(319). 또한, 프로파일 제공 서버는 암호화된 프로파일을 프로파일 관리 서버로 전달한다(320). 이때 암호화된 프로파일과 함께, 프로파일에 대한 송신자 인증과 메시지 무결성 검증을 위한 프로파일 검증 값이 전달될 수 있다.

[0110] 프로파일 검증 값은 상기 복호화된 세션 키와 상기 프로파일을 SHA1과 같은 해쉬 함수에 적용함으로써 생성될 수 있다. 또는 프로파일 검증 값은 상기 디지털 인증서의 개인키로 상기 프로파일에 대해 SHA1withRSA와 같은 전자서명을 수행함으로써 생성될 수 있다. 프로파일 검증 값을 생성함에 있어서, 상기 예시된 것과 다른 종류의 해쉬 함수 또는 전자서명 함수를 사용하는 것도 가능하다.

[0111] 프로파일 관리 서버는 전달받은 암호화된 프로파일 및 프로파일 검증 값을 단말기로 전송한다(321).

[0112] 단말기는 암호화된 프로파일을 미리 저장된 세션 키를 이용하여 복호화한다. 그리고 단말내장 보안 모듈은 암호화된 프로파일과 함께 전달받은 검증 값을 상기 세션 키 또는 상기 디지털 인증서의 공개 키를 사용하여 검증한다(322).

[0113] 검증 값의 검증이 실패하면 단말내장 보안모듈은 프로파일 설치 과정을 중단하고 프로파일 관리 서버로 실패 메시지를 전달한다.

[0114] 반대로, 검증 값의 검증이 성공하면 단말내장 보안 모듈은 상기 디지털 인증서에 대한 검증을 수행한다.

[0115] 상기 디지털 인증서의 정당성 검증을 위해, 상기 단말내장 보안모듈은 디지털 인증서 내에 포함된 특정 정보와, 복호화 및 검증이 완료된 상기 프로파일 내에 포함된 특정 정보가 일치하는지 확인한다.

[0116] 한편, 상기 특정 정보의 예로 이동통신사 정보가 이용될 수 있다. 예를 들어 프로파일 내에 포함된 USIM 애플리케이션의 IMSI 값은 MCC, MNC, MSIN 정보로 이루어질 수 있으며, 단말내장 보안 모듈은 MCC와 MNC 값을 이용하여 이동통신사 정보를 확인할 수 있다. 또는 프로파일 내의 다른 파일 또는 필드에 이동통신사 정보가 포함될 수 있으며, 단말내장 보안 모듈은 이를 정당성 검증에 이용할 수 있다.

[0117] 상기 디지털 인증서의 정당성 검증을 위해, 상기 디지털 인증서 내에도 이동통신사 정보가 포함될 수 있다. 예를 들어 디지털 인증서의 DN(Distinguished Name) 필드 또는 다른 확장 필드에 이동통신사 정보가 포함될 수 있다. 디지털 인증서 내에 포함된 정보는 인증서를 발행한 인증기관에 의해 서명되어 있어 제 3자에 의해 수정 및

변경이 불가능하므로, 단말내장 보안모듈은 인증서 내에 포함된 이동통신사 정보와, 프로파일 내에 포함된 이동통신사 정보의 비교를 통해 해당 프로파일이 정당한 인증서를 통해 암호화 처리가 된 것임을 검증할 수 있다.

[0118] 디지털 인증서의 검증이 실패하면 단말기는 프로파일 설치 과정을 중단하고 프로파일 관리 서버로 실패 메시지를 전달한다(323).

[0119] 반면, 상기 이동통신사 정보의 비교 검증을 포함한 디지털 인증서의 검증이 성공하면, 단말기는 해당 프로파일을 내부 메모리에 저장 및 설치하여 이동통신 서비스에 사용될 수 있는 상태로 만들 수 있다.

부호의 설명

[0120] 201: 단말기 제조사 220: 이동통신 단말기

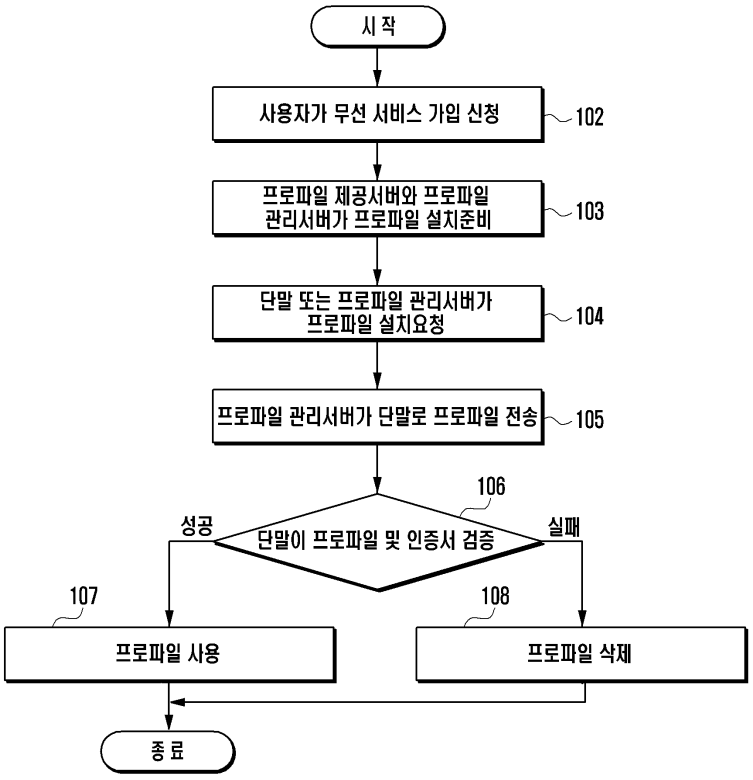
221: 단말내장 보안모듈 230: 이동통신사

240: 프로파일 제공 서버 250: 인증서 발급기관

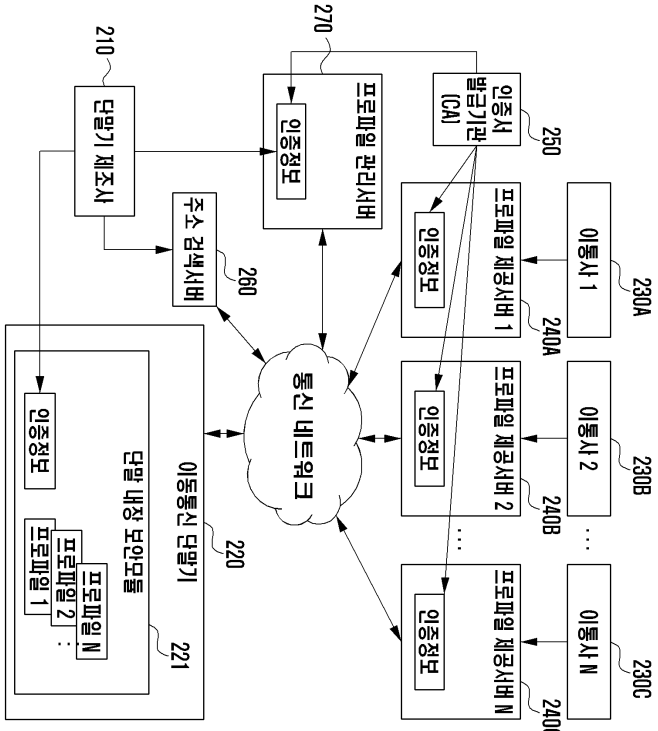
260: 주소 검색 서버 270: 프로파일 관리 서버

도면

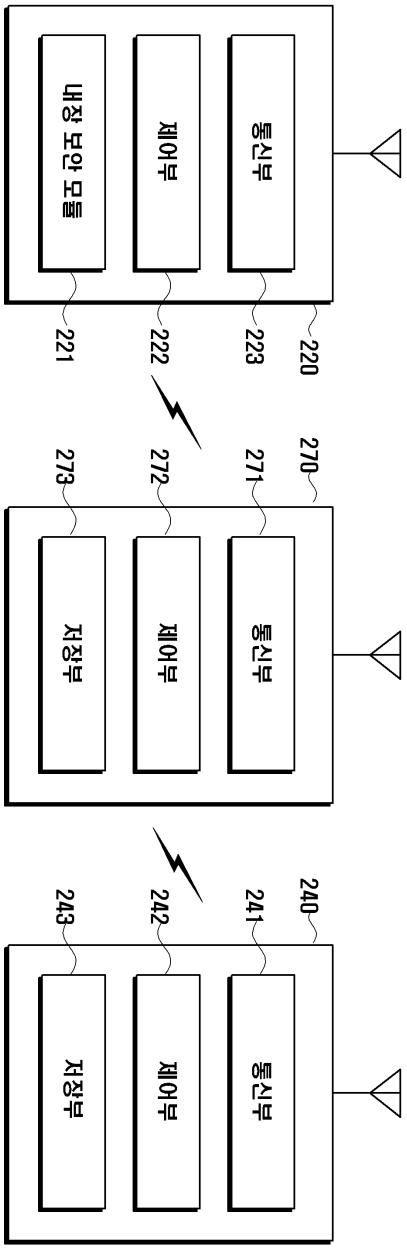
도면1



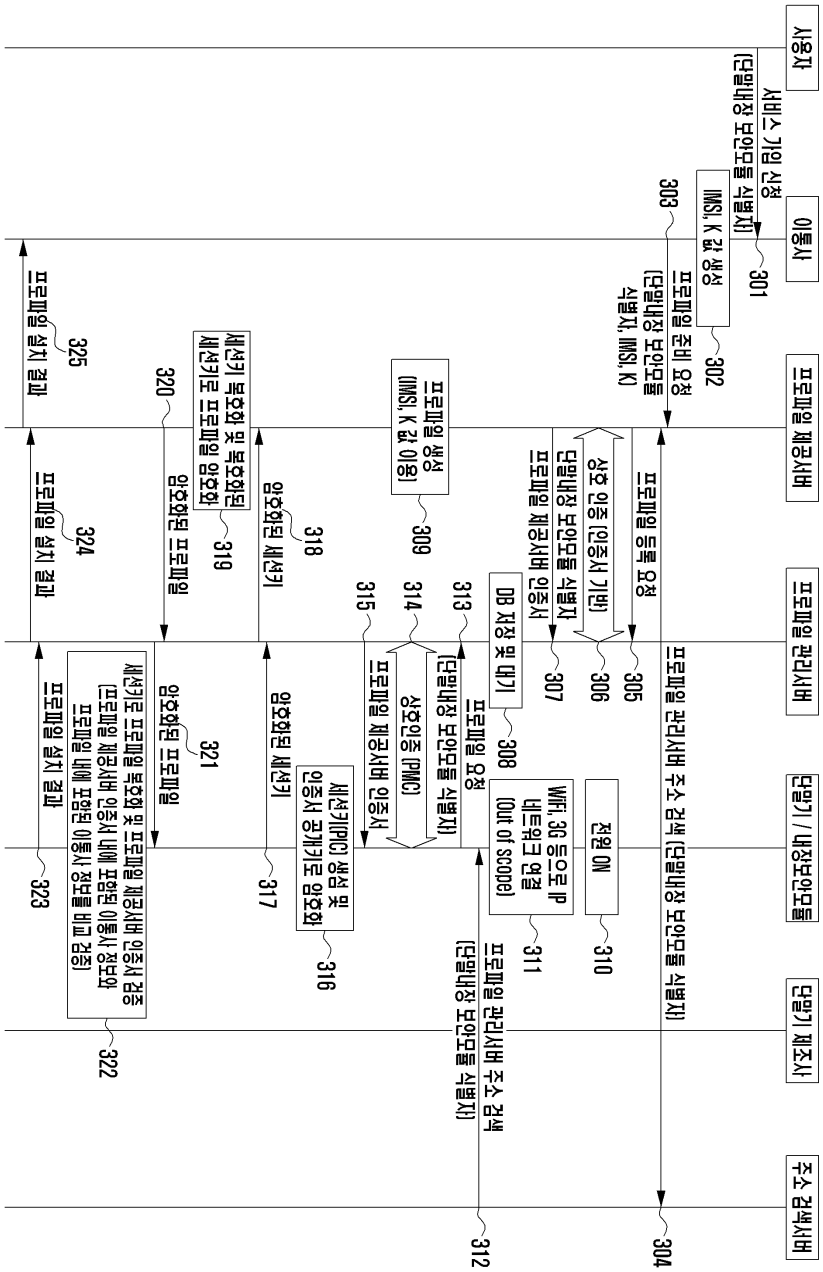
도면2


210
단말기 제조사
270
프로파일 관리서버
인증정보
인증서 발급기관 (CA)
250
주소 검색서버
260
통신 네트워크
이동통신 단말기
220
단말 내장 보안모듈
221
인증정보
프로파일 1
프로파일 2
프로파일 N
프로파일 제공서버 1
240A
프로파일 제공서버 2
240B
프로파일 제공서버 N
240C
이통사 1
230A
이통사 2
230B
이통사 N
230C

도면3


내장 보안 모듈
제어부
통신부
221
222
223
220
273
272
271
270
저장부
제어부
통신부
243
242
241
240
저장부
제어부
통신부

도면4


사용자
서비스 기입 신청
[단말내장 보안모듈 식별자]
301
이통사
303
IMSI, K 값 생성
302
프로파일 준비 요청
[단말내장 보안모듈 식별자, IMSI, K]
프로파일 관리서버
프로파일 등록 요청
305
상호 인증 (인증서 기반)
306
단말내장 보안모듈 식별자
프로파일 관리서버 인증서
307
DB 저장 및 대기
308
프로파일 요청
[단말내장 보안모듈 식별자]
313
프로파일 관리서버 주소 검색 [단말내장 보안모듈 식별자]
304
프로파일 관리서버 주소 검색
[단말내장 보안모듈 식별자]
312
단말기 / 내장보안모듈
전원 ON
310
WiFi, 3G 등으로 IP
네트워크 연결
[Out of SCOPE]
311
단말기 제조사
프로파일 생성
(IMSI, K 값 이용)
309
상호인증 (PMK)
314
프로파일 관리서버 인증서
315
세션키(PMK) 생성 및
인증서 공개키로 암호화
316
암호화된 세션키
317
세션키로 프로파일 복호화 및 프로파일 관리서버 인증서 검증
[프로파일 관리서버 인증서 내에 포함된 이통사 정보를 비교 검증]
322
암호화된 프로파일
321
프로파일 설치 결과
323
암호화된 세션키
318
세션키로 프로파일 암호화
319
세션키 복호화 및 복호화된
암호화된 프로파일
320
프로파일 설치 결과
324
프로파일 설치 결과
325