



(19) 대한민국특허청(KR)  
(12) 등록특허공보(B1)

(45) 공고일자 2020년09월07일  
(11) 등록번호 10-2152008  
(24) 등록일자 2020년08월31일

(51) 국제특허분류(Int. Cl.)  
H04W 8/30 (2009.01) H04W 8/18 (2009.01)  
(21) 출원번호 10-2013-0065995  
(22) 출원일자 2013년06월10일  
심사청구일자 2018년06월07일  
(65) 공개번호 10-2013-0141373  
(43) 공개일자 2013년12월26일  
(30) 우선권주장  
1020120064521 2012년06월15일 대한민국(KR)  
1020120099087 2012년09월07일 대한민국(KR)  
(56) 선행기술조사문헌  
KR100958349 B1\*  
US20080261561 A1\*  
\*는 심사관에 의하여 인용된 문헌

(73) 특허권자  
삼성전자주식회사  
경기도 수원시 영통구 삼성로 129 (매탄동)  
(72) 발명자  
김관래  
경기도 수원시 영통구 봉영로1517번길 76 631동  
604호 (영통동, 신나무실6단지아파트)  
박철현  
경기 용인시 기흥구 예현로 15, 106동 1503호 (서  
천동, 서그내마을에스케이아파트)  
(74) 대리인  
윤앤리특허법인(유한)  
(뒷면에 계속)

전체 청구항 수 : 총 20 항

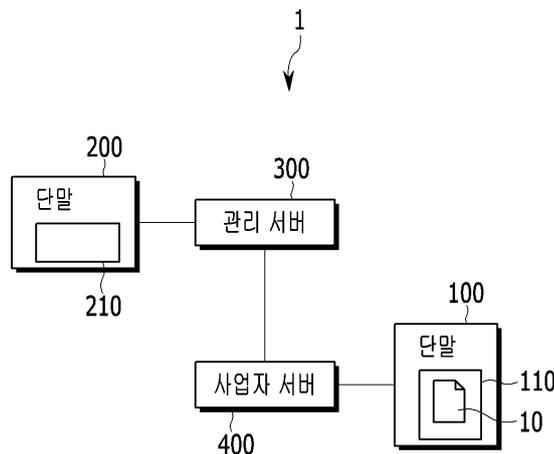
심사관 : 이종익

(54) 발명의 명칭 인증 모듈의 프로파일을 이동하는 방법 및 시스템

(57) 요약

인증 모듈에 저장된 프로파일을 이동하는 시스템으로서, 제1인증 모듈을 포함하고, 상기 제1인증 모듈에 저장된 사용자의 프로파일을 기초로 동작하는 제1단말, 제2인증 모듈을 포함하고, 사용자 식별 정보를 포함하는 제1메시지를 전송하여 상기 사용자의 프로파일을 요청하는 제2단말, 상기 제1메시지를 수신하고, 상기 사용자 식별 정보를 기초로 상기 제1단말에 저장된 프로파일을 획득하며, 획득한 프로파일을 상기 제2단말로 전송하는 관리서버를 포함하고, 상기 제1단말은 저장된 프로파일을 내보내고, 상기 제2단말은 상기 관리서버로부터 수신한 프로파일을 상기 제2인증 모듈에 설치한다.

대표도 - 도1



(72) 발명자

**이진형**

경기 성남시 분당구 느티로 70, 413동 202호 (정자동, 느티마을아파트)

**이형진**

서울 구로구 신도림로 16, 304동 2504호 (신도림동, 신도림대림아파트)

---

## 명세서

### 청구범위

#### 청구항 1

프로파일을 이동하는 제1 단말로서,

신호를 송신 또는 수신하는 송수신부; 및

서버로부터 프로파일 요청 메시지를 수신하고, 제1 암호정보를 기초로 인증 모듈에 저장된 제1프로파일을 암호화하고, 암호화한 상기 제1프로파일을 상기 서버로 전송하고, 상기 인증모듈에 저장된 상기 제1프로파일을 비활성화하도록 제어하는 제어부를 포함하되,

상기 제1 단말은, 사용자 식별 정보를 기초로 상기 서버에 의해 식별되고,

상기 제1프로파일은 제2 암호정보를 기초로 암호화되어 상기 서버에서 제2 단말로 전송되는 것을 특징으로 하는, 단말.

#### 청구항 2

제1항에 있어서,

상기 제1 암호정보는 상기 제1 단말이 프로파일을 로딩, 설치, 또는 관리하기 위해 사용하는 키인 것을 특징으로 하는, 단말.

#### 청구항 3

제1항에 있어서,

상기 제어부는,

상기 서버로부터 암호화된 제2프로파일을 수신하고, 상기 제1 암호정보를 기초로 수신한 상기 제2프로파일을 복호하고, 복호한 상기 제2프로파일을 상기 인증모듈에 설치하도록 더 제어하는 것을 특징으로 하는, 단말.

#### 청구항 4

프로파일을 이동하는 제2 단말로서,

신호를 송신 또는 수신하는 송수신부; 및

사용자 식별 정보를 포함하는 프로파일 요청 메시지를 서버로 전송하고, 상기 서버로부터 암호화된 제1프로파일을 수신하고, 제2 암호정보를 기초로 상기 제1프로파일을 복호하고, 복호한 상기 제1프로파일을 인증모듈에 설치하도록 제어하는 제어부를 포함하되,

상기 제1프로파일은, 상기 사용자 식별 정보를 기반으로 서버에 의해 식별된 다른 단말의 프로파일이고,

상기 제1프로파일은 제1 암호정보를 기초로 암호화되어 제1단말에서 상기 서버로 전송되는 것을 특징으로 하는, 단말.

#### 청구항 5

제4항에 있어서,

상기 제2 암호정보는 상기 제2 단말과 상기 서버가 공유하는 값인 것을 특징으로 하는, 단말.

#### 청구항 6

제4항에 있어서,

상기 제어부는,

상기 인증모듈에 저장된 제2프로파일을 상기 제2 암호정보를 기초로 암호화하고, 상기 암호화한 상기 제2프로파일을 포함하는 프로파일 복원 메시지를 상기 서버로 전송하고, 상기 인증모듈에 저장된 제2프로파일을 삭제하도록 더 제어하는 것을 특징으로 하는, 단말.

#### 청구항 7

프로파일 이동을 위한 서버로서,

신호를 송신 또는 수신하는 송수신부; 및

제2단말로부터 사용자 식별 정보를 포함하는 제1 메시지를 수신하고, 상기 사용자 식별 정보를 기초로 제1단말을 식별하고, 상기 제1 단말의 인증모듈에 저장된 제1프로파일을 획득하고, 획득한 상기 제1프로파일을 상기 제2단말로 전송하도록 제어하는 제어부를 포함하고,

상기 제어부는 제1 암호정보를 기초로 암호화된 제1프로파일을 상기 제1 단말로부터 수신하고, 제2 암호정보를 기초로 암호화된 제1프로파일을 상기 제2 단말로 전송하는 것을 특징으로 하는, 서버.

#### 청구항 8

제7항에 있어서,

상기 제어부는,

상기 제1단말과 공유하는 제1 암호정보를 기초로 암호화된 제1프로파일을 제1단말로부터 수신하도록 더 제어하는 것을 특징으로 하는, 서버.

#### 청구항 9

제7항에 있어서,

상기 제어부는

상기 제2단말과 공유하는 제2 암호정보를 기초로 상기 제1프로파일을 암호화하고, 상기 암호화한 제1프로파일을 상기 제2단말로 전송하도록 더 제어하는 것을 특징으로 하는, 서버.

#### 청구항 10

제7항에 있어서,

상기 제어부는,

상기 제2단말로부터 제2단말의 인증모듈에 저장된 제2프로파일을 획득하고, 상기 제2 단말로부터 획득한 제2프로파일을 상기 제1단말로 전송하도록 더 제어하는 것을 특징으로 하는, 서버.

#### 청구항 11

프로파일을 이동하는 제1 단말의 방법으로서,  
 서버로부터 프로파일 요청 메시지를 수신하는 단계,  
 제1 암호정보를 기초로 인증모듈에 저장된 제1프로파일을 암호화하는 단계,  
 암호화한 상기 제1프로파일을 상기 서버로 전송하는 단계, 그리고  
 상기 인증모듈에 저장된 상기 제1프로파일을 비활성화하는 단계  
 를 포함하되,  
 상기 제1 단말은, 사용자 식별 정보를 기초로 상기 서버에 의해 식별되고,  
 상기 제1프로파일은 제2 암호정보를 기초로 암호화되어 상기 서버에서 제2 단말로 전송되는 것을 특징으로 하는  
 프로파일 이동 방법.

**청구항 12**

제11항에서,  
 상기 제1 암호정보는 상기 제1 단말이 프로파일을 로딩, 설치, 또는 관리하기 위해 사용하는 키인 프로파일 이  
 동 방법.

**청구항 13**

제11항에서,  
 상기 서버로부터 암호화된 제2프로파일을 수신하는 단계,  
 상기 제1 암호정보를 기초로 수신한 상기 제2프로파일을 복호하는 단계, 그리고  
 복호한 상기 제2프로파일을 상기 인증모듈에 설치하는 단계  
 를 더 포함하는 프로파일 이동 방법.

**청구항 14**

프로파일을 이동하는 제2 단말의 방법으로서,  
 사용자 식별 정보를 포함하는 프로파일 요청 메시지를 서버로 전송하는 단계,  
 상기 서버로부터 암호화된 제1프로파일을 수신하는 단계,  
 제2 암호정보를 기초로 상기 제1프로파일을 복호하는 단계, 그리고  
 복호한 상기 제1프로파일을 인증모듈에 설치하는 단계  
 를 포함하되,  
 상기 제1프로파일은, 상기 사용자 식별 정보를 기반으로 서버에 의해 식별된 다른 단말의 프로파일이고,  
 상기 제1프로파일은 제1 암호정보를 기초로 암호화되어 제1 단말에서 상기 서버로 전송되는 것을 특징으로 하는  
 프로파일 이동 방법.

**청구항 15**

제14항에서,

상기 제2 암호정보는 상기 제2 단말과 상기 서버가 공유하는 값인 프로파일 이동 방법.

**청구항 16**

제14항에서,  
 상기 인증모듈에 저장된 제2프로파일을 상기 제2 암호정보를 기초로 암호화하는 단계,  
 암호화한 상기 제2프로파일을 포함하는 프로파일 복원 메시지를 상기 서버로 전송하는 단계, 그리고  
 상기 인증모듈에 저장된 제2프로파일을 삭제하는 단계  
 를 더 포함하는 프로파일 이동 방법.

**청구항 17**

프로파일을 이동하는 서버의 방법으로서,  
 제2단말로부터 사용자 식별 정보를 포함하는 제1 메시지를 수신하는 단계;  
 상기 사용자 식별 정보를 기초로 제1단말을 식별하는 단계;  
 상기 제1단말의 인증모듈에 저장된 제1프로파일을 획득하는 단계; 및  
 상기 획득한 제1프로파일을 상기 제2 단말로 전송하는 단계를 포함하고,  
 상기 서버는 제1 암호정보를 기초로 암호화된 제1프로파일을 상기 제1 단말로부터 수신하고, 제2 암호정보를 기초로 암호화된 제1프로파일을 상기 제2 단말로 전송하는 것을 특징으로 하는, 방법.

**청구항 18**

제17항에 있어서,  
 상기 제1단말과 공유하는 제1 암호정보를 기초로 암호화된 제1프로파일을 제1단말로부터 수신하는 단계를 더 포함하는 것을 특징으로 하는, 방법.

**청구항 19**

제17항에 있어서,  
 상기 제2단말과 공유하는 제2 암호정보를 기초로 상기 제1프로파일을 암호화하는 단계; 및  
 상기 암호화한 제1프로파일을 상기 제2단말로 전송하는 단계를 더 포함하는 것을 특징으로 하는, 방법.

**청구항 20**

제17항에 있어서,  
 상기 제2단말로부터 제2단말의 인증모듈에 저장된 제2프로파일을 획득하는 단계; 및  
 상기 제2 단말로부터 획득한 제2프로파일을 상기 제1단말로 전송하는 단계를 더 포함하는 것을 특징으로 하는, 방법.

**발명의 설명**

**기술 분야**

[0001] 본 발명은 인증 모듈의 프로파일을 이동하는 방법 및 시스템에 관한 것이다.

**배경 기술**

[0002] UICC(Universal Integrated Circuit Card)는 단말에 삽입되는 스마트 카드로서, 사용자 인증을 위한 모듈이다. UICC는 사용자의 개인 정보 및 사용자가 가입한 이동 통신 사업자의 사업자 정보를 포함하는 프로파일을 저장할 수 있다. 예를 들면, UICC는 사용자를 식별하기 위한 IMSI(International Mobile Subscriber Identity)를 포함할 수 있다. UICC는 GSM(Global System for Mobile) 방식의 경우 SIM(Subscriber Identity Module) 카드, WCDMA(Wideband Code Division Multiple Access)방식의 경우 USIM(Universal Subscriber Identity Module)카드로 불리기도 한다.

[0003] 단말은 UICC에 저장된 정보들을 이용하여 사용자 인증을 한다. 따라서, 사용자는 UICC를 이용하여 편리하게 통신하고 인증하고 결제할 수 있다. 또한, 사용자가 단말을 교체할 때, 사용자는 기존 단말의 UICC를 새로운 단말에 삽입한다. 따라서, 사용자는 착탈형 UICC를 교체하여, 사용자의 개인 정보 및 이동 통신 사업자 정보를 새로운 장치에 옮길 수 있다.

[0004] 최근 M2M(Machine to Machine)과 같은 통신 단말이 소형으로 제작된다. 이러한 단말에 착탈형 UICC 대신 내장 UICC(eUICC, embedded UICC)가 장착된다. 내장 UICC는 착탈형 UICC와 달리, 물리적으로 단말에서 제거되거나, 단말에 삽입될 수 없다. 따라서, UICC에 저장된 프로파일을 다른 내장 UICC나 다른 저장소에 옮기기 어렵다.

**발명의 내용**

**해결하려는 과제**

[0005] 본 발명이 해결하고자 하는 과제는 인증 모듈의 프로파일을 이동하는 방법 및 시스템을 제공하는 것이다.

**과제의 해결 수단**

[0006] 본 발명의 한 실시예에 따른 인증 모듈에 저장된 프로파일을 이동하는 시스템으로서, 제1인증 모듈을 포함하고, 상기 제1인증 모듈에 저장된 사용자의 프로파일을 기초로 동작하는 제1단말, 제2인증 모듈을 포함하고, 사용자 식별 정보를 포함하는 제1메시지를 전송하여 상기 사용자의 프로파일을 요청하는 제2단말, 상기 제1메시지를 수신하고, 상기 사용자 식별 정보를 기초로 상기 제1단말에 저장된 프로파일을 획득하며, 획득한 프로파일을 상기 제2단말로 전송하는 관리서버를 포함하고, 상기 제1단말은 저장된 프로파일을 내보내고, 상기 제2단말은 상기 관리서버로부터 수신한 프로파일을 상기 제2인증 모듈에 설치한다.

[0007] 상기 시스템은 상기 프로파일을 기초로 상기 제1단말과 연결된 사업자 서버를 더 포함하고, 상기 관리서버는 상기 사용자 식별 정보를 기초로 상기 사업자 서버를 찾고, 상기 사업자 서버로 상기 사용자 식별 정보에 대응하는 프로파일을 요청하는 제2메시지를 전송할 수 있다.

[0008] 상기 사업자 서버는 상기 제2메시지를 수신하고, 상기 사용자 식별 정보를 기초로 상기 제1단말을 찾으며, 상기 제1단말로 프로파일을 요청하는 제3메시지를 전송하고, 상기 제1단말로부터 수신한 프로파일을 상기 관리서버로 전송할 수 있다.

[0009] 상기 제1단말은 상기 사업자 서버와 공유하는 제1암호정보를 기초로 상기 인증 모듈에 저장된 프로파일을 암호화하고, 암호화한 프로파일을 상기 사업자 서버로 전송할 수 있다.

[0010] 상기 사업자 서버는 상기 제1암호정보를 기초로 수신한 프로파일을 복호할 수 있다.

[0011] 상기 사업자 서버는 복호한 프로파일을 상기 관리서버와 공유하는 제2암호정보를 기초로 암호화하고, 암호화한 프로파일을 상기 관리서버로 전송할 수 있다.

[0012] 상기 관리서버는 상기 제2단말과 공유하는 제3암호정보를 기초로 상기 제2단말로 전송하는 프로파일을 암호화할 수 있다.

[0013] 상기 제2단말은 상기 제3암호정보를 기초로 수신한 프로파일을 복호할 수 있다.

[0014] 상기 제2단말은 상기 제2인증 모듈에 저장된 프로파일을 상기 관리서버로 전송하여 저장된 프로파일을 상기 제1

단말로 내보내고, 저장된 프로파일을 삭제할 수 있다.

- [0015] 본 발명의 다른 실시예에 따른 단말이 인증 모듈에 저장된 프로파일을 이동하는 방법으로서, 서버로부터 프로파일 요청 메시지를 수신하는 단계, 암호정보를 기초로 인증모듈에 저장된 제1프로파일을 암호화하는 단계, 암호화한 상기 제1프로파일을 상기 제1서버로 전송하는 단계, 그리고 상기 인증모듈에 저장된 상기 제1프로파일을 비활성화하는 단계를 포함한다.
- [0016] 상기 암호정보는 상기 단말이 프로파일을 로딩, 설치, 또는 관리하기 위해 사용하는 키일 수 있다.
- [0017] 상기 방법은 상기 서버로부터 암호화된 제2프로파일을 수신하는 단계, 상기 암호정보를 기초로 수신한 상기 제2 프로파일을 복호하는 단계, 그리고 복호한 상기 제2프로파일 정보를 상기 인증모듈에 설치하는 단계를 더 포함할 수 있다.
- [0018] 본 발명의 또 다른 실시예에 따른 단말이 인증 모듈에 저장된 프로파일을 이동하는 방법으로서, 사용자 식별 정보를 포함하는 프로파일 요청 메시지를 서버로 전송하는 단계, 상기 서버로부터 암호화된 프로파일을 수신하는 단계, 상기 서버와 공유하는 암호정보를 기초로 상기 프로파일을 복호하는 단계, 그리고 복호한 상기 프로파일을 인증모듈에 설치하는 단계를 포함한다.
- [0019] 상기 암호정보는 상기 단말과 상기 서버가 공유하는 값일 수 있다.
- [0020] 상기 방법은 상기 인증모듈에 저장된 프로파일을 상기 암호정보를 기초로 암호화하는 단계, 암호화한 상기 프로파일을 포함하는 프로파일 복원 메시지를 상기 서버로 전송하는 단계, 그리고 상기 인증모듈에 저장된 프로파일을 삭제하는 단계를 더 포함할 수 있다.

**발명의 효과**

- [0021] 본 발명의 실시예에 따르면 내장 인증 모듈을 물리적으로 착탈할 수 없더라도, 사용자는 프로파일을 내장 인증 모듈 사이에서 자유롭게 이동할 수 있다. 본 발명의 실시예에 따르면 사용자는 프로파일을 원하는 단말로 가져올 수 있으므로 복수의 단말을 동일한 환경에서 이용할 수 있다.

**도면의 간단한 설명**

- [0022] 도 1은 본 발명의 한 실시예에 따른 통신 시스템을 설명하는 도면이다.
- 도 2와 도 3은 본 발명의 한 실시예에 따른 프로파일 획득 방법의 흐름도이다.
- 도 4와 도 5는 본 발명의 다른 실시예에 따른 프로파일 복원 방법의 흐름도이다.
- 도 6과 도 7은 본 발명의 한 실시예에 따른 프로파일 획득을 위한 어플리케이션 화면의 예시이다.
- 도 8과 도 9는 본 발명의 한 실시예에 따른 프로파일 복원을 위한 어플리케이션 화면의 예시이다.

**발명을 실시하기 위한 구체적인 내용**

- [0023] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0024] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [0025] 도 1은 본 발명의 한 실시예에 따른 통신 시스템을 설명하는 도면이다.
- [0026] 도 1을 참고하면, 통신 시스템(1)은 제1단말(100), 제2단말(200), 관리서버(300), 그리고 적어도 하나의 사업자 서버(400)를 포함한다. 관리서버(300)는 프로파일을 안전하게 이동하기 위한 관리를 한다. 가입자 관리 서버(Subscriber Management Server, SMS)일 수 있다. 사업자 서버(400)는 이동 통신 사업자(Mobile Network Operator, MNO)의 서버일 수 있다. 관리서버(300)와 사업자 서버(400)는 통합될 수 있다.
- [0027] 제1단말(100)과 제2단말(200) 각각은 인증 모듈(110, 210)을 포함한다. 인증 모듈은 가입자 식별 모듈, 가입자

식별 모듈 카드, 범용 가입자 식별 모듈 등 다양한 용어로 대체될 수 있다. 인증 모듈(110/210)은 단말(100/200)에 내장(embedded)되는 내장 인증 모듈일 수 있다. 내장 인증 모듈(110/210)은 단말(100/200)에서 분리되어 제거될(removed) 수 없다. 단말에 장착된 내장 인증 모듈은 다른 내장 인증 모듈로 교체될(replaced) 수 없다. 여기서, 내장 인증 모듈은 내장 UICC(embedded Universal Integrated Circuit Card, eUICC)일 수 있다.

- [0028] 인증 모듈(110/210)은 프로파일(profiles)을 저장한다. 프로파일은 사용자 인증 정보 등 단말 동작에 관련된 각종 정보를 포함한다. 프로파일은 사용자의 개인 정보 그리고 사용자가 가입한 통신 사업자의 사업자 정보를 포함할 수 있다. 단말은 프로파일을 사용하여 사용자 인증이나 단말 인증을 수행한다.
- [0029] 프로파일(10)은 제1단말(100)의 인증 모듈(110)에 설치(install)되어 있고, 제2단말(200)의 인증 모듈(210)은 비어있을 수 있다. 이 경우, 제2단말(200)은 관리서버(300)와 사업자 서버(400)를 통해 제1단말(100)로부터 프로파일을 가져오고(import), 제1단말(100)은 관리서버(300)와 사업자 서버(400)를 통해 제2단말(200)로 프로파일을 내보낸다(export). 즉, 사용자가 단말을 교체할 때, 인증 모듈을 교체하는 것이 아니라, 인증 모듈에 저장된 프로파일이 이동한다.
- [0030] 제1단말(100)은 관리서버(300)와 사업자 서버(400)를 통해 제2단말(200)로 프로파일(10)을 전송한다. 프로파일(10)을 전송한 제1단말(100)은 프로파일(10)을 비활성화(disable)한다. 프로파일(10)을 수신한 제2단말(200)은 프로파일(10)을 인증 모듈(210)에 설치(install)하고, 프로파일(10)을 실행(enable)한다. 즉, 프로파일은 하나의 단말에서만 활성화된다.
- [0031] 제2단말(200)은 프로파일(10)을 원래 위치인 제1단말(100)로 전송할 수 있다. 프로파일(10)을 전송한 제2단말(200)은 프로파일(10)을 삭제한다. 프로파일(10)을 수신한 제1단말(100)은 프로파일(10)을 활성화한다.
- [0032] 관리서버(300)와 사업자 서버(400)는 제2단말(200)과 제1단말(100) 사이에 위치하여 프로파일을 이동한다. 이를 위해, 제2단말(200)과 관리서버(300), 관리서버(300)와 사업자 서버(400), 그리고 사업자 서버(400)와 제1단말(100)이 통신한다. 이때, 각 통신 주체 사이에서 주고받는 전송 정보는 통신 주체 사이에서 공유된 암호 정보(credentials)를 기초로 암호화(encrypt)된다. 즉, 프로파일은 인증 모듈 외부에서 암호화되어 전송된다.
- [0033] 도 2와 도 3은 본 발명의 한 실시예에 따른 프로파일 획득 방법의 흐름도이다.
- [0034] 도 2를 참고하면, 제2단말(200)은 관리서버(300)로 사용자의 프로파일을 요청한다(S110). 제2단말(200)은 프로파일 요청에 관계된 사용자를 인증하도록 사용자 식별 정보를 전송한다. 제2단말(200)은 관리서버 연결을 위한 초기 정보를 가지고 있다. 사용자 식별 정보는 가입자 식별 정보일 수 있다. 사용자 식별 정보는 예를 들면, 사용자 크리덴셜(credentials)이나 단말 고유 정보일 수 있다. 사용자 크리덴셜은 예를 들면, 아이디(identification, ID), 패스워드(password), 접근 토큰(access token) 등 다양할 수 있다. 단말 고유 정보는 예를 들면, IMSI(International Mobile Subscriber Identity) 등 다양할 수 있다.
- [0035] 관리서버(300)는 프로파일 요청 시 전송된 사용자 식별 정보를 기초로 사용자가 가입한 사업자 서버(400)를 확인한다(S120). 예를 들면, 관리서버(300)는 사용자의 ID/PW 또는 IMSI 정보 등 사업자 서버 고유의 사용자 식별 정보를 이용할 수 있다.
- [0036] 관리서버(300)는 사업자 서버(400)로 사용자의 프로파일을 요청한다(S122).
- [0037] 사업자 서버(400)는 사용자의 프로파일이 저장된 등록 단말, 즉 제1단말(100)을 식별한다(S130). 제1단말(100)은 사용자의 프로파일을 기초로 사용자가 가입한 통신 사업자 망에 접속되어 있다. 따라서, 단말의 사용자를 식별할 수 있는 사업자 서버(400)는 요청받은 사용자의 프로파일이 제1단말(100)에 설치되어 있음을 알 수 있다. 즉, 사업자 서버(400)는 자신의 망에 접속된 단말 중에서, 제2단말(200)의 사용자 식별 정보에 일치하는 제1단말(100)을 찾는다.
- [0038] 사업자 서버(400)는 제1단말(100)로 프로파일을 요청한다(S132).
- [0039] 제1단말(100)은 사업자 서버(400)와 공유된 제1암호정보를 기초로 인증 모듈(110)에 저장된 프로파일을 암호화한다(S140). 제1단말(100)과 사업자 서버(400)가 공유하는 제1암호정보는 제1단말(100)이 프로파일을 로딩, 설치, 또는 관리할 때 사용하는 키일 수 있다. 제1암호정보는 내장 인증 모듈에 존재할 수 있다.
- [0040] 제1단말(100)은 암호화한 프로파일을 사업자 서버(400)로 전송한다(S142).
- [0041] 제1단말(100)은 프로파일을 비활성화한다(S144).

- [0042] 사업자 서버(400)는 제1단말(100)과 공유된 제1암호정보를 기초로 프로파일을 복호(decrypt)한다(S150).
- [0043] 사업자 서버(400)는 관리서버(300)와 공유된 제2암호정보를 기초로 프로파일을 암호화한다(S152).
- [0044] 사업자 서버(400)는 암호화된 프로파일을 관리서버(300)로 전송한다(S154).
- [0045] 관리서버(300)는 사업자 서버(400)와 공유된 제2암호정보를 기초로 프로파일을 복호한다(S160).
- [0046] 관리서버(300)는 제2단말(200)과 공유된 제3암호정보를 기초로 프로파일을 암호화한다(S162). 관리서버(300)와 제2단말(200)이 공유하는 제3암호정보는 제2단말(200)이 프로파일을 로딩, 설치, 또는 관리할 때 사용하는 키일 수 있다. 제3암호정보는 내장 인증 모듈에 존재할 수 있다.
- [0047] 관리서버(300)는 암호화된 프로파일을 제2단말(200)로 전송한다(S164).
- [0048] 제2단말(200)은 관리서버(300)와 공유된 제3암호정보를 기초로 프로파일을 복호한다(S170).
- [0049] 제2단말(200)은 프로파일을 인증 모듈(210)에 설치한다 (S180).
- [0050] 제2단말(200)은 프로파일을 실행한다(S190).
- [0051] 도 3을 참고하면, 제1단말(100)은 사업자 서버(400)로부터 사용자의 프로파일 요청을 수신한다.
- [0052] 제1단말(100)은 사업자 서버(400)와 공유된 제1암호정보(20)를 기초로 프로파일(10)을 암호화한다(S210).
- [0053] 제1단말(100)은 암호화된 프로파일(10)을 사업자 서버(400)로 전송한다(S2120). 제1단말(100)은 프로파일(10)을 비활성화한다(S214).
- [0054] 사업자 서버(400)는 제1단말(100)과 공유된 제1암호정보(20)를 기초로 프로파일(10)을 복호한다(S220).
- [0055] 사업자 서버(400)는 관리서버(300)와 공유된 제2암호정보(30)를 기초로 프로파일(10)을 암호화한다(S222).
- [0056] 사업자 서버(400)는 암호화된 프로파일(10)을 관리서버(300)로 전송한다(S224).
- [0057] 관리서버(300)는 사업자 서버(400)와 공유된 제2암호정보(30)를 기초로 프로파일(10)을 복호한다(S230).
- [0058] 관리서버(300)는 제2단말(200)과 공유된 제3암호정보(40)를 기초로 프로파일(10)을 암호화한다(S232).
- [0059] 관리서버(300)는 암호화된 프로파일(10)을 제2단말(200)로 전송한다(S234).
- [0060] 제2단말(200)은 관리서버(300)와 공유된 제3암호정보(40)를 기초로 프로파일(10)을 복호한다(S240).
- [0061] 제2단말(200)은 프로파일을 실행한다(S242).
- [0062] 이와 같이, 사용자는 제1단말(100)의 프로파일을 제2단말(200)로 가져온다. 사용자는 인증 모듈을 교체할 필요 없이, 제1단말(100)에 저장된 사용자의 개인 정보 그리고 사용자가 가입한 통신 사업자의 사업자 정보를 제2단말(200)로 안전하게 가져올 수 있다.
- [0063] 도 4와 도 5는 본 발명의 다른 실시예에 따른 프로파일 복원 방법의 흐름도이다.
- [0064] 도 4를 참고하면, 사용자는 프로파일을 가져온 제2단말(200)을 한시적으로 사용한 후, 제1단말(100)을 다시 사용할 수 있다.
- [0065] 제2단말(200)은 저장된 프로파일을 제1단말(100)로 전송하고, 저장된 프로파일을 삭제한다. 제1단말(100)은 수신한 프로파일(10)을 실행한다. 여기서, 제2단말(200)이 제1단말(100)로 전송하는 프로파일은 제2단말(200)이 제1단말(100)로부터 받은 프로파일에서 개인 정보 등 일부 정보가 갱신될 수 있다.
- [0066] 제2단말(200)은 관리서버(300)와 공유된 제3암호정보를 기초로 프로파일(10)을 암호화한다(S310).
- [0067] 제2단말(200)은 관리서버(300)에 프로파일 복원을 요청한다(S312). 제2단말(200)은 암호화된 프로파일(10)와 사용자 식별 정보를 관리서버(300)로 전송한다.
- [0068] 제2단말(200)은 프로파일(10)을 삭제한다(S314).
- [0069] 관리서버(300)는 제2단말(200)과 공유된 제3암호정보를 기초로 프로파일(10)을 복호한다(S320).
- [0070] 관리서버(300)는 프로파일 복원에 관계된 사용자 식별 정보를 기초로 사용자가 가입한 사업자 서버(400)를 확인한다(S322).

- [0071] 관리서버(300)는 사업자 서버(400)와 공유된 제2암호정보를 기초로 프로파일(10)을 암호화한다(S324).
- [0072] 관리서버(300)는 사업자 서버(400)로 사용자의 프로파일 복원을 요청한다(S326). 관리서버(300)는 암호화된 프로파일을 사업자 서버(400)로 전송한다.
- [0073] 사업자 서버(400)는 관리서버(300)와 공유된 제2암호정보를 기초로 프로파일을 복호화한다(S330).
- [0074] 사업자 서버(400)는 프로파일을 복원할 단말, 즉 제1단말(100)을 식별한다(S332).
- [0075] 사업자 서버(400)는 제1단말(100)과 공유된 제1암호정보를 기초로 프로파일을 암호화한다(S334).
- [0076] 사업자 서버(400)는 제1단말(100)로 프로파일 복원을 요청한다(S336). 사업자 서버(400)는 암호화된 프로파일을 제1단말(100)로 전송한다.
- [0077] 제1단말(100)은 사업자 서버(400)와 공유된 제1암호정보를 기초로 프로파일을 복호화한다(S340).
- [0078] 제1단말(100)은 프로파일(10)을 인증 모듈(110)에 설치한다(S350).
- [0079] 제1단말(100)은 프로파일(10)을 실행한다(S360)
- [0080] 도 5를 참고하면, 제2단말(200)은 관리서버(300)와 공유된 제3암호정보(40)를 기초로 프로파일(10)을 암호화한다(S410).
- [0081] 제2단말(200)은 관리서버(300)에 프로파일 복원을 요청한다(S412). 이때, 제2단말(200)은 제3암호정보(40)를 기초로 암호화된 프로파일(10)을 관리서버(300)로 전송한다.
- [0082] 제2단말(200)은 프로파일(10)을 삭제한다(S414).
- [0083] 관리서버(300)는 제2단말(200)과 공유된 제3암호정보(40)를 기초로 프로파일(10)을 복호화한다(S420).
- [0084] 관리서버(300)는 사업자 서버(400)와 공유된 제2암호정보(30)를 기초로 프로파일(10)을 암호화한다(S422).
- [0085] 관리서버(300)는 사업자 서버(400)로 사용자의 프로파일 복원을 요청한다(S424). 관리서버(300)는 암호화된 프로파일(10)을 사업자 서버(400)로 전송한다.
- [0086] 사업자 서버(400)는 관리서버(300)와 공유된 제2암호정보(30)를 기초로 프로파일(10)을 복호화한다(S430).
- [0087] 사업자 서버(400)는 제1단말(100)과 공유된 제1암호정보(20)를 기초로 프로파일(10)을 암호화한다(S432).
- [0088] 사업자 서버(400)는 암호화된 프로파일(10)을 제1단말(100)로 전송한다(S434).
- [0089] 제1단말(100)은 사업자 서버(400)와 공유된 제1암호정보(20)를 기초로 프로파일(10)을 복호화한다(S440).
- [0090] 제1단말(100)은 프로파일을 실행한다(S442).
- [0091] 도 6과 도 7은 본 발명의 한 실시예에 따른 프로파일 획득을 위한 어플리케이션 화면의 예시이다.
- [0092] 도 6을 참고하면, 제2단말(200)은 프로파일의 이동을 위한 어플리케이션을 제공한다. 제2단말(200)이 어플리케이션을 실행하면, 어플리케이션은 제2단말(200)의 디스플레이(500)에 프로파일 가져오기(get profile) 아이콘(510)과 프로파일 백업(backup profile) 아이콘(520)을 표시한다. 어플리케이션은 관리서버(300) 연결을 위한 정보를 가지고 있다.
- [0093] 사용자가 프로파일 획득 아이콘(510)을 누르면, 제2단말(200)은 관리서버(300)에 다른 단말에 저장된 프로파일을 요청한다.
- [0094] 제2단말(200)은 관리서버(300)로부터 수신한 프로파일을 복호화하여 실행한다. 그러면, 도 7과 같이, 어플리케이션은 디스플레이(500)에 프로파일을 가져왔고(import), 제2단말(200)이 동작함을 나타내는 안내창(530)을 표시할 수 있다.
- [0095] 도 8과 도 9는 본 발명의 한 실시예에 따른 프로파일 복원을 위한 어플리케이션 화면의 예시이다.
- [0096] 도 8을 참고하면, 사용자가 프로파일 복원 아이콘(520)을 누르면, 제2단말(200)은 관리서버(300)에 제1단말(100)의 프로파일 복원을 요청한다.
- [0097] 제2단말(200)은 저장된 프로파일을 삭제한다. 그러면, 도 9와 같이, 어플리케이션은 디스플레이(500)에 프로파

일을 내보냈고(export), 제2단말(200)이 동작하지 않음을 나타내는 안내창(540)을 표시할 수 있다.

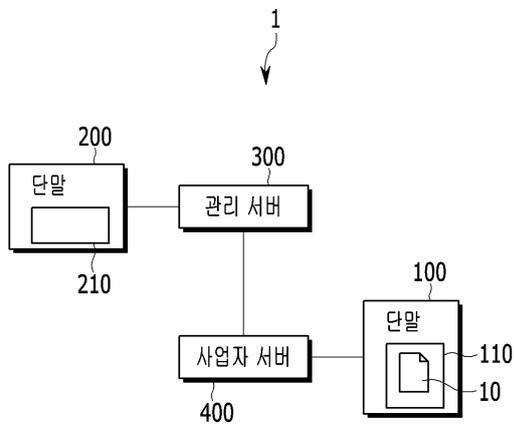
[0098] 이와 같이, 본 발명의 실시예에 따르면 내장 인증 모듈을 물리적으로 착탈할 수 없더라도, 프로파일을 내장 인증 모듈사이에서 자유롭게 이동할 수 있다. 본 발명의 실시예에 따르면 사용자는 프로파일을 원하는 단말로 가져올 수 있으므로 복수의 단말을 동일한 환경에서 이용할 수 있다.

[0099] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있다.

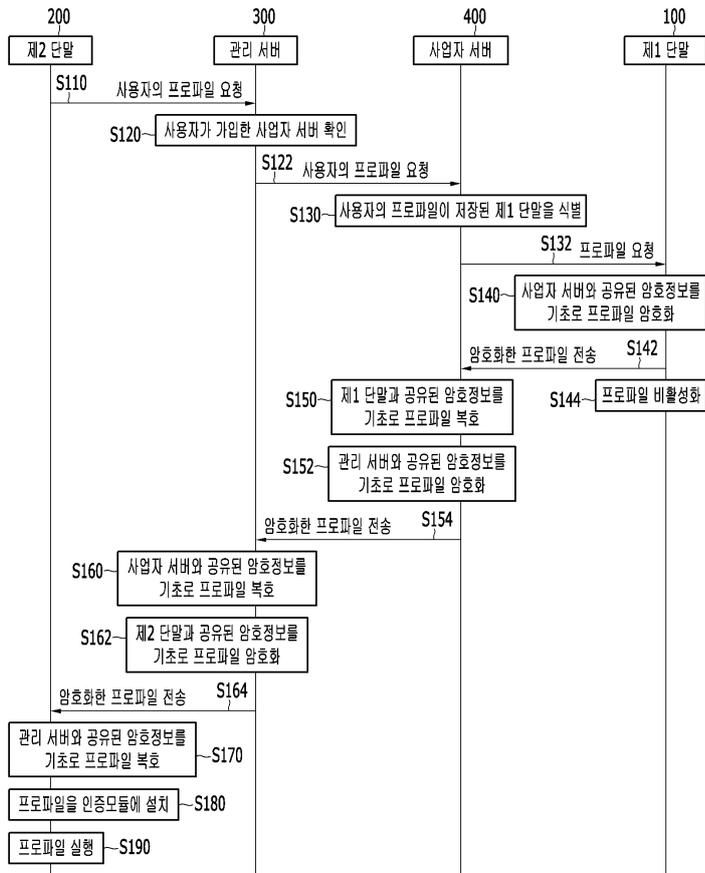
[0100] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

**도면**

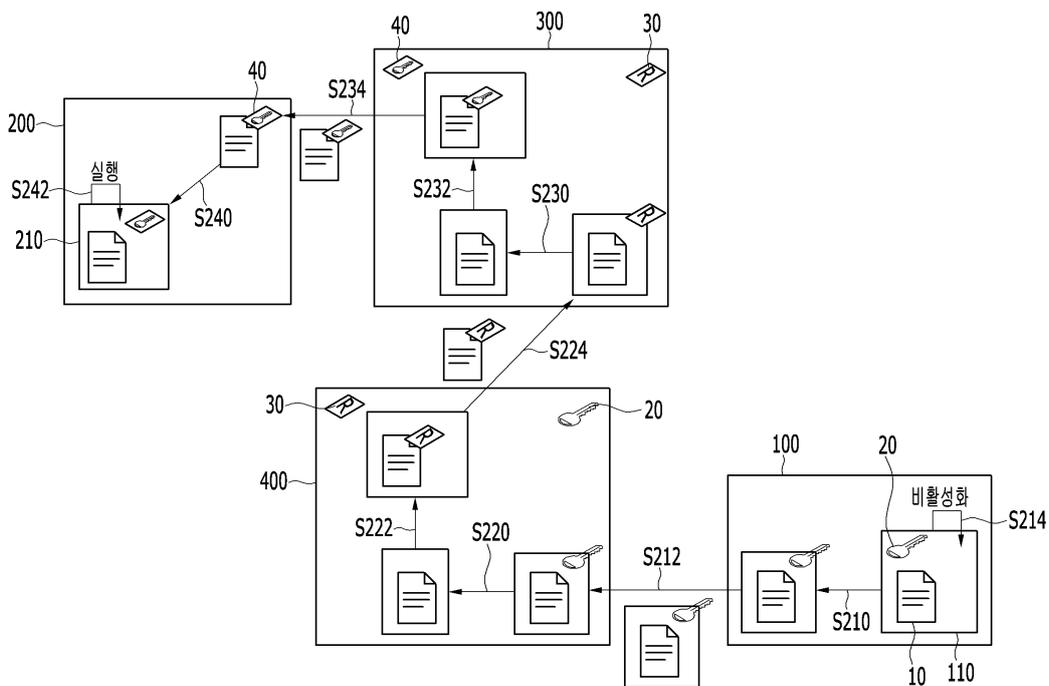
**도면1**



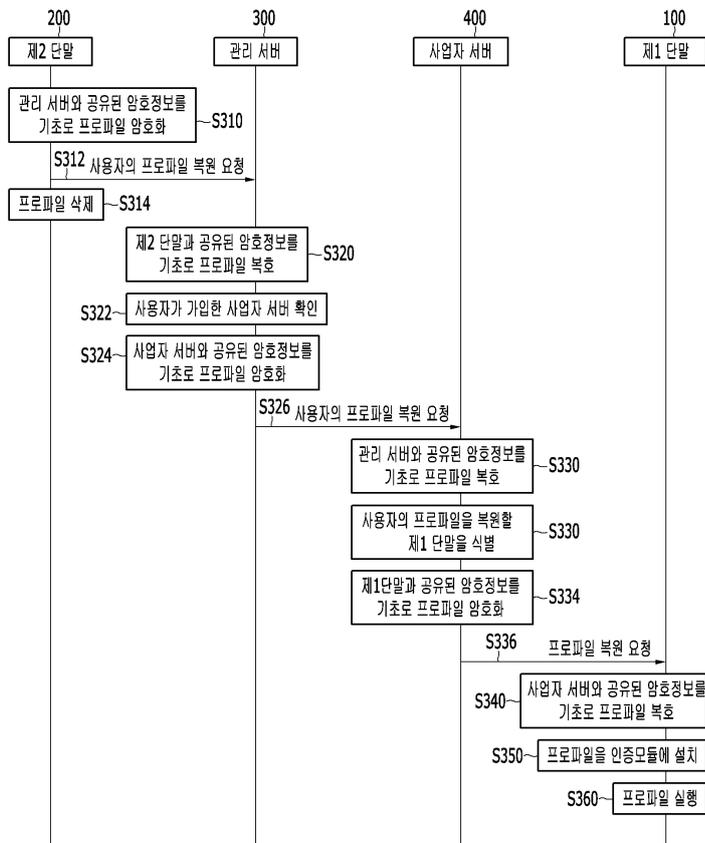
도면2



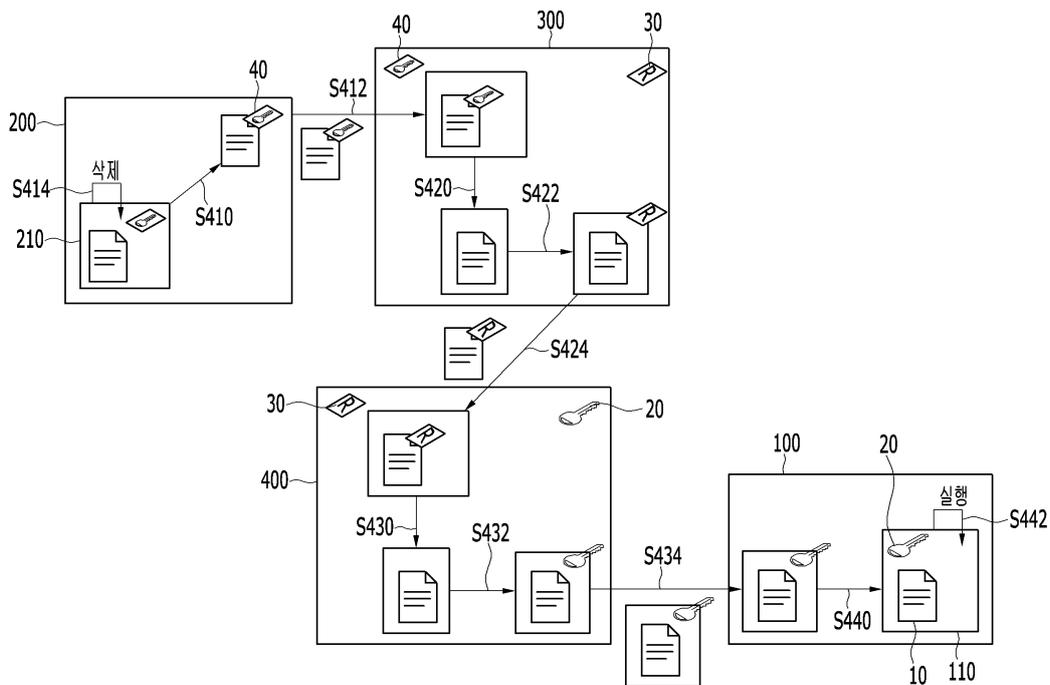
도면3



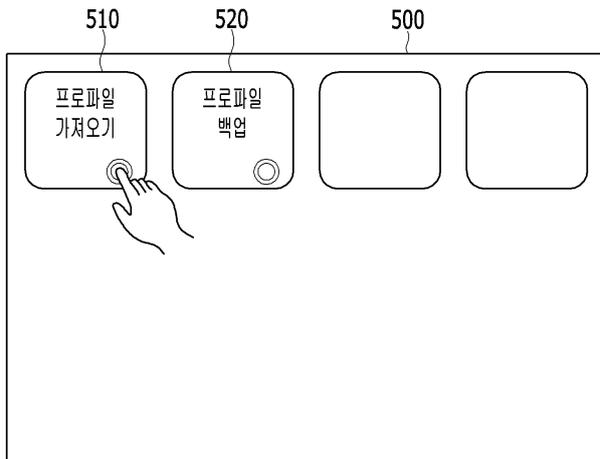
도면4



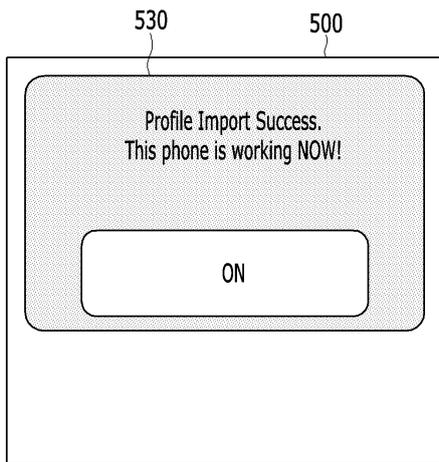
도면5



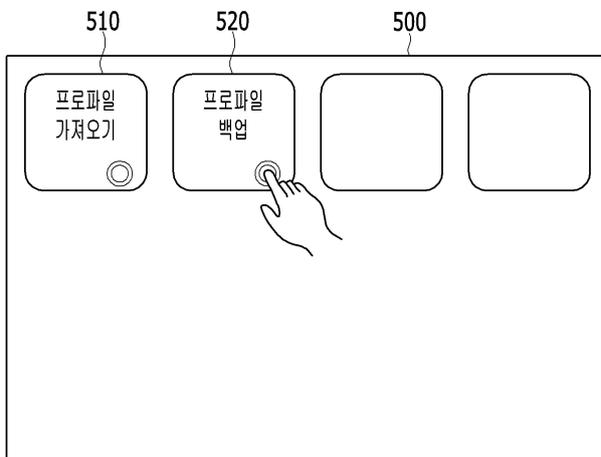
도면6



도면7



도면8



도면9

