(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0121307
(43) 공개일자 2021년10월07일

(51) 국제특허분류(Int. Cl.)
*G06F 21/34* (2013.01) *G06F 21/32* (2013.01)
*G06F 21/40* (2013.01) *G06F 21/60* (2013.01)
*G06F 21/73* (2013.01)
(52) CPC특허분류
*G06F 21/34* (2013.01)
*G06F 21/32* (2013.01)
(21) 출원번호 10-2021-7031145(분할)
(22) 출원일자(국제) 2014년08월29일
심사청구일자 없음
(62) 원출원 특허 10-2016-7008371
원출원일자(국제) 2014년08월29일
심사청구일자 2019년08월26일
(85) 번역문제출일자 2021년09월28일
(86) 국제출원번호 PCT/GB2014/052640
(87) 국제공개번호 WO 2015/028824
국제공개일자 2015년03월05일
(30) 우선권주장
1315420.8 2013년08월29일 영국(GB)

(71) 출원인
**리버티 볼트즈 리미티드**
영국, 엔12 0디알 런던, 핀칠리, 우드베리 그로브 2, 1층
(72) 발명자
**존스턴, 크리스토퍼 이언**
영국, 에스더블유19 5이쥐 런던, 윔블던 빌리지, 하이 스트리트 87
**레듀크, 미셸**
프랑스, 에프-13530 트레츠, 로티스먼트 카바수드, 27
(74) 대리인
**특허법인이지**

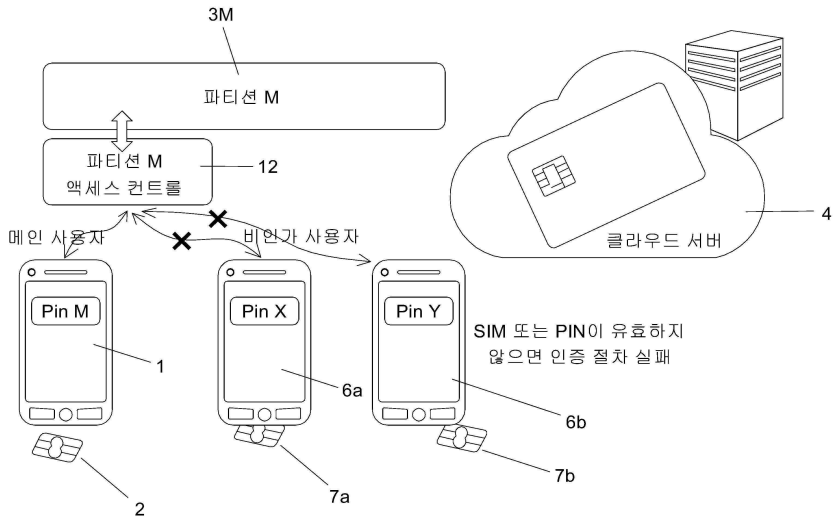
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 **복수의 장치로부터 데이터에 액세스하기 위한 시스템**

## (57) 요 약

장치에서 데이터에 액세스하는 방법으로, 데이터는 상기 장치로부터 원격으로 또는 탈착식 스토리지에 저장되며, 상기 방법은 (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 전송하는 단계-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; (ii) 적어도 부분적으로 상기 식별 코드에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 포함한다.

## 대 표 도



(52) CPC특허분류
*G06F 21/40* (2013.01)
*G06F 21/604* (2013.01)
*G06F 21/73* (2013.01)

# 명 세 서

## 청구범위

### 청구항 1

장치에서 데이터에 액세스하는 방법으로, 상기 데이터는 상기 장치와 연관된 복수의 파티션에 저장되고, 상기 파티션은 상기 장치에 저장되거나 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며,

상기 방법은,

(i) 상기 장치에 의해 신호 송출 장치로부터 판독된 신호에 기초하여, 상기 복수의 파티션으로부터 액세스 될 선택된 파티션을 결정하는 단계;

(ii) 상기 장치로부터 상기 데이터에 액세스하는 요청을 전송하는 단계-여기서, 상기 요청은 액세스 될 상기 선택된 파티션을 특정하는 정보 및 상기 장치와 연관된 안전 요소의 식별 코드를 포함함;

(iii) 적어도 부분적으로 상기 식별 코드에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및

(iv) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 포함하는, 방법.

### 청구항 2

청구항 1에 있어서,

상기 데이터는 클라우드에 저장되는 방법.

### 청구항 3

청구항 1에 있어서,

상기 요청은 상기 장치에서 입력된 패스코드 또는 PIN을 포함하며, 상기 (ii) 단계는 상기 패스코드 또는 PIN에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 포함하는 방법.

### 청구항 4

청구항 1에 있어서,

상기 요청은 상기 장치의 사용자 고유 데이터를 포함하며, 상기 단계 (iii)는 상기 장치의 상기 사용자 고유 데이터에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 포함, 및/또는

상기 요청은 위치를 포함하는 데이터를 포함하며, 상기 단계 (iii)는 상기 장소에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 포함, 및/또는

상기 요청은 시간을 포함하는 데이터를 포함하며, 상기 단계 (iii)는 상기 시간에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 포함, 및/또는

상기 요청은 상기 사용자가 그룹의 일부임을 나타내는 데이터를 포함하며, 상기 단계 (iii)는 상기 그룹의 다른 멤버가 상기 데이터에 액세스할 수 있는지 여부에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 포함하는 방법.

### 청구항 5

청구항 4에 있어서,

상기 사용자 고유 데이터는 상기 사용자의 유전 및/또는 생체 정보를 나타내는 데이터를 포함하는 방법.

### 청구항 6

청구항 1에 있어서,

상기 안전 요소는, SIM, 가상 SIM, SIM 소프트웨어, TPM, SE, TEE, Micro SD, Memory card, USB 키 또는 상기 장치에 연관된 스마트카드인 방법.

**청구항 7**

청구항 1에 있어서,

상기 데이터는 상기 장치에 연관된 파티션에 저장되고, 상기 요청은 상기 파티션을 특정하는 데이터를 포함하며, 바람직하게는 상기 데이터는 제3자 서비스로의 연결을 용이하게 하는 방법.

**청구항 8**

청구항 7에 있어서,

상기 파티션을 특정하는 데이터는,

PIN 또는 패스코드, 및 사용자 고유 데이터 중 하나 이상을 포함하는 방법.

**청구항 9**

청구항 8에 있어서,

상기 장치의 상기 사용자 고유 데이터는 상기 사용자의 유전 및/또는 생체 정보를 나타내는 데이터를 포함하는 방법.

**청구항 10**

청구항 1에 있어서,

상기 장치는 전화, 태블릿, 랩탑 컴퓨터, 데스크탑 컴퓨터, TV, 셋톱박스, 카메라, 자동차, 게임 콘솔, 안경, 시계, Chromecast, 스마트 미터, 또는 원격 장치와 데이터를 송수신할 수 있는 장치인 방법.

**청구항 11**

청구항 1에 있어서,

상기 단계 (i) 내지 (iv) 이전에, 안전 요소의 식별 코드를 상기 데이터에 등록하는 단계를 포함하는 방법.

**청구항 12**

청구항 11에 있어서,

하나 이상의 안전 요소 또는 메모리 카드의 식별 코드가 상기 데이터에 연관되는 방법.

**청구항 13**

장치 및 상기 장치로부터 상기 장치와 연관된 파티션에 저장되고 상기 장치에 저장되거나 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장된 데이터로의 액세스를 제어하는 데이터 액세스 컨트롤러를 포함하는 시스템에 있어서,

상기 장치는 액세스 될 상기 파티션을 식별하는 신호 송출 장치로부터 신호를 판독하고 상기 데이터에 액세스하는 요청을 상기 데이터 액세스 컨트롤러로 전송하도록 구성되고,

상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; 및 상기 데이터 액세스 컨트롤러는 적어도 부분적으로 상기 식별 코드에 기초하여 상기 데이터로의 액세스가 허용 또는 거부할지 검증하고 그에 따라서 상기 데이터로의 장치 액세스를 허용 또는 거부하는 시스템.

**청구항 14**

장치로부터 클라우드 기반 또는 웹 기반 제3자 서비스에 액세스하는 방법에 있어서,

(i) 상기 장치로부터 상기 장치에 연관된 클라우드 기반 파티션에 요청을 전송하는 단계-여기서, 상기 파티션은 상기 제3자 서비스로의 연결을 용이하게 하는 데이터를 포함하며, - 상기 요청은 상기 장치에 연관된 안전 요소

또는 메모리 카드의 식별 코드를 포함함;

(ii) 적어도 부분적으로 상기 식별 코드에 기초하여 상기 파티션으로의 액세스를 허용 또는 거부할지 검증하는 단계;

(iii) 검증 결과에 따라 상기 파티션으로의 장치 액세스를 허용 또는 거부하는 단계; 및

상기 파티션으로의 액세스가 허용된 후

(iv) 크리덴셜을 상기 제3자 서비스로 전송하는 단계를 포함하고,

상기 파티션을 식별 및/또는 액세스하는데 필요한 정보는 신호 송출 장치로부터 판독되는, 방법.

**청구항 15**

청구항 14에 있어서,

상기 신호 송출 장치는 Bluetooth, BLE, wifi, zigbee, NFC, GPS, 또는 ISO14443 장치, 또는 임의의 형태의 비접촉 통신을 이용하는 방법.

**청구항 16**

청구항 1에 있어서,

(v) 상기 장치 및 상기 원격 또는 탈착식 스토리지간 상호 인증 절차를 실행하는 단계;

(vi) 상기 장치 및 상기 원격 또는 탈착식 스토리지간 안전 채널을 생성하는 단계; 및

(vii) 상기 장치 및 상기 원격 또는 탈착식 스토리지간 데이터를 전송하는 단계를 더 포함하는 방법.

**청구항 17**

청구항 16에 있어서,

상기 인증은 이중 또는 삼중 요소를 포함하며, 상기 요소는 다음의 목록에서 선택되는 방법.

- 상기 장치에 연관된 스마트 오브젝트(메모리 카드 또는 안전 요소)의 식별 코드,

- 패스코드 또는 PIN,

- 유전 또는 또는 생체 식별(identification) 데이터,

- 위치,

- 시간, 또는 다른 멤버(예를 들어, 관리자) 또는 상기 사용자가 속한 그룹이 상기 데이터에 액세스하고 있는지 여부

**청구항 18**

청구항 16에 있어서,

상기 인증은 이중 요소를 포함하며,

상기 요소는 상기 장치에 연관된 상기 안전 요소의 식별 코드; 및 패스코드 또는 PIN 인 방법.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 데이터 액세스 분야에 관한 것이다. 상세하게, 본 발명은 복수의 장치로부터 데이터에 액세스하기 위한 시스템에 관한 것이다.

### *배 경 기 술*

[0002] 사용자에게 클라우드 기반 데이터 스토리지를 제공하는 것은 잘 알려져 있다. 이 클라우드 기반 스토리지는 복수의 장치로부터 액세스될 수 있다.

[0003] 예를 들어, 드롭박스는, 사용자들의 데이터를 위한 클라우드 기반 원격 스토리지를 사용자에게 제공하는 시스템이다. 데이터는, 예를 들어, 휴대 전화기로 촬영된 사진을 포함할 수 있다. 데이터가 휴대 전화기로부터, 예를 들어, 원격 스토리지로 업로드되면, 랩탑 또는 데스크탑 컴퓨터와 같이 인터넷에 연결된 다른 장치로부터 액세스될 수 있다. 저장된 데이터는 256 비트 AES로 암호화되며 사용자의 데이터로의 액세스가 허가되기 전에 사용자는 등록된 이메일 주소와 비밀번호를 웹사이트를 통해 반드시 입력해야 한다.

[0004] 그러나, 이러한 시스템의 문제점은 사용자 이메일 주소와 비밀번호가 제3자에 의해 발견되면 제3자도 임의의 장치로부터 저장된 데이터에 액세스할 수 있다는 점이다. 따라서, 하나 또는 복수의 장치로부터 액세스될 수 있는 더욱 안전한 원격 스토리지 시스템에 대한 요구가 있다.

## 발명의 내용

### 해결하려는 과제

[0005] 본 발명은 복수의 장치로부터 데이터에 액세스하기 위한 시스템을 제공하는 것이다.

### 과제의 해결 수단

[0006] 본 발명의 제1 측면에 따르면, 장치에서 데이터에 액세스하는 방법이 제공되고, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며, 상기 방법은, (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 전송하는 단계-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; (ii) 적어도 부분적으로 상기 식별 코드에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 포함한다.

[0007] 상기 데이터로의 액세스는, 상기 장치에 연관된 정확한 식별 코드가 제공되어야만 허용된다. 따라서, 비인가 장치는 정확한 식별 코드를 제공할 수 없으므로, 비인가 장치가 상기 데이터에 액세스하는 것을 방지할 수 있다.

[0008] 상술한 바와 같이, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함한다. 그러나, 식별 코드는 상기 요청에 변형된 형태로 포함될 수 있는데, 예를 들어, 암호화된 형태 및/또는 하나 이상의 추가 코드, 데이터 또는 정보와 결합될 수 있다.

[0009] 액세스하려는 데이터는 메모리에 저장될 수 있는 임의의 형태를 갖는 데이터를 포함한다. 예를 들어, 하나 이상의 데이터 파일, 데이터베이스, 어플리케이션, 소프트웨어, 및/또는 서비스를 포함할 수 있다. 서비스의 일부 예들은 아래에서 설명된다.

[0010] 바람직하게, 식별 코드는 안전 채널(secure channel)을 통해 전송된다. 대체 또는 추가적으로, 식별 코드는 암호화될 수 있다. 이는 절차를 더욱 안전하게 하며 식별 코드가 제3자에 의해 인터셉트 및/또는 발견되지 않도록 하는데 도움이 된다.

[0011] 추가 (또는 대체) 가능성은 안전 요소(secure element) 또는 메모리 카드 및 상기 장치로부터 하나 이상의 다른 요소 또는 코드에 기초하여 상기 장치에서 코드를 생성할 수 있다. 이 생성된 코드는 이후 전송될 수 있으며, 예를 들어, 특정 세션 동안에만 유효할 수 있다. 따라서, 상기 생성된 코드는 인터셉트되더라도, 제3자에게는 쓸모가 없어지게 된다.

[0012] 상기 데이터는 탈착식 스토리지 장치, 클라우드 또는 다른 형태의 원격 데이터 스토리지에 저장될 수 있다. 예를 들어, 상기 데이터는 USB 키, 랩톱, (개인 또는 기업용) 컴퓨터 서버, (개인 또는 기업용) 컴퓨터 네트워크, 태블릿 또는 전화기에 저장될 수 있다.

[0013] 상기 요청은 상기 장치에서 입력된 패스코드 또는 PIN을 포함하며, 상기 (ii) 단계는 상기 패스코드 또는 PIN에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 포함한다. 따라서, 상기 데이터에 액세스하기 위해서 이중 요소 인증이 요구된다.

[0014] 패스코드 또는 PIN은 상기 장치에 연관된 안전 요소 또는 메모리 카드 (예를 들어, SIM, 또는 가상 SIM)에 의해 (먼저) 검증될 수 있다.

[0015] 대체적으로 (또는 추가적으로), 패스코드 또는 PIN은 상기 장치로부터 원격으로 검증될 수 있는데, 예를 들어,

상기 데이터로의 액세스를 제어하는 액세스 컨트롤러에서 검증될 수 있다.

[0016] 패스코드 또는 PIN이 안전 요소 또는 메모리 카드에 의해 검증된 경우에, 이 검증 결과는 예를 들어, 액세스 컨트롤러로, 예를 들어, 안전 채널과 같이 안전 및/또는 보호된 방식으로 바람직하게 전송된다. 예를 들어, 결과는 인증서, 암호화된 코드, 세션 코드 또는 암호화된 세션 코드의 형태로 전달될 수 있다. 바람직하게, 검증이 성공적, 즉, 정확한 패스코드 또는 PIN이 입력되면 검증 결과만 전송된다.

[0017] 패스코드 또는 PIN이 장치로부터 원격으로, 예를 들어, 액세스 컨트롤러에 의해 검증되는 경우에, 패스코드 또는 PIN은, 예를 들어, 액세스 컨트롤러로, 안전 및/또는 보호된 방식으로 전송되는 것이 바람직하다. 예를 들어, 패스코드 또는 PIN은 안전 채널을 통해 및/또는 전송 전에 패스코드 또는 PIN를 암호화하여 전송될 수 있다.

[0018] 대체적으로 또는 추가적으로, 상기 요청은 상기 장치의 사용자 고유 데이터(data representing something inherent to the user)를 포함하며, 상기 단계 (ii)는 상기 장치의 상기 사용자 고유 데이터에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 포함할 수 있다. 따라서, 데이터에 액세스 하기 위해서 이중 또는 삼중 요소 인증이 요구될 수 있으며, 인가된 사용자만이 데이터에 액세스하는 것이 허용될 수 있다.

[0019] 사용자 고유 데이터는, 예를 들어, 지문 또는 홍채 데이터와 같이 상기 사용자의 유전 및/또는 생체 정보를 나타내는 데이터를 포함할 수 있다.

[0020] 대체적으로 또는 추가적으로, PIN 및/또는 사용자 고유 데이터를 사용한 인증 (식별 코드로 이중 또는 삼중 요소 인증)을 대체하거나 추가하여, 다음 형태의 인증이 가능하다.

[0021] 상기 요청은 위치(즉, 사용자가 데이터에 액세스를 시도하는 장소)를 포함하는 데이터를 포함하며, 상기 단계 (ii)는 상기 장소에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 또한 포함할 수 있다.

[0022] 상기 요청은 시간(즉, 사용자가 데이터에 액세스를 시도하는 시간)을 포함하는 데이터를 포함하며, 상기 단계 (ii)는 상기 시간에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 또한 포함할 수 있다.

[0023] 상기 요청은 상기 사용자가 그룹의 일부임을 나타내는 데이터를 포함하며, 상기 단계 (ii)는 상기 그룹의 다른 멤버(예를 들어, 관리자)가 상기 데이터에 액세스할 수 있는지 여부에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 또한 포함할 수 있다.

[0024] 상기 안전 요소 또는 메모리 카드는, 예를 들어, 고유 식별 코드를 가진 “스마트 오브젝트” 또는 안전 또는 부정 조작 방지(tamper-proof) 하드웨어 장치이며, 고유 식별 코드 역시 이상적으로 안전하고 부정 조작이 방지된다. 상기 안전 요소 또는 메모리 카드는, 예를 들어, SIM, 가상 SIM, SIM 소프트웨어, TPM(Trusted Platform Module), SE(secure element), TEE(trusted execution environment), Micro SD, Memory card, USB 키 또는 스마트카드일 수 있다.

[0025] 상술한 바와 같이, 안전 요소의 일반적인 예는 SIM 카드이다. SIM 카드는 모든 GSM 휴대 장치 및 스마트폰에 구비되어 있다. 그러나, SIM 카드는 전화 네트워크에 의해 제공되므로 (SIM 에 애플릿을 쉽게 다운로드할 수 없거나 SIM 을 변형할 수 없다는 의미로) 용이하게 액세스할 수 없다. 더욱이, 장치의 운영 체제는 SIM 과 인터페이스하기 위한 소프트웨어 툴키트를 가지고 있지 않을 수 있다. 이러한 단점을 극복하기 위해서, 장치에 어플리케이션으로 탑재될 수 있는 가상 SIM을 다운로드할 수 있다. 가상 SIM 은 물리적인 SIM처럼 작동하는데, 이는 애플릿을 수신하고 처리하며, 애플릿, 크리덴셜(credential), 키 및 알고리즘 등을 안전하게 저장함을 의미한다.

[0026] 안전 요소 또는 메모리 카드는 내장(local), 원격(remote) 또는 탈착식(removable) 메모리 중 어느 하나일 수 있다.

[0027] 안전 요소 또는 메모리 카드의 식별 코드는 바람직하게는, 예를 들어, 안전 요소 또는 메모리 카드의 세이프 박스에서 잘 보호되고 저장된다.

[0028] 본 발명의 바람직한 실시예로, 안전 요소 또는 메모리 카드는 안전 채널을 생성 및/또는 식별 코드 및/또는 PIN 또는 패스코드를 암호화하는데 사용된다.

[0029] 데이터는 장치에 연관된 파티션, 예를 들어, 메모리 파티션에 저장될 수 있으며, 상기 요청은 파티션, 예를 들

어, 액세스될 파티션을 특정하는 데이터를 포함할 수 있다.

[0030] 안전 채널은 안전 요소 또는 메모리 카드와 파티션 사이에 생성될 수 있으며, 데이터, 파일, 크리덴셜, 또는 다른 양식 채움 데이터(forming filling data)를 상기 장치와 파티션 사이에서 전송하는데 이용될 수 있다.

[0031] 따라서, 상기 방법은 iv) 상기 장치 및 상기 원격 또는 탈착식 스토리지간 상호 인증 절차를 수행하는 단계; (v) 상기 장치 및 상기 원격 또는 탈착식 스토리지간 안전 채널을 생성하는 단계를 포함할 수 있다.

[0032] 상기 인증은 이중 또는 삼중 요소를 포함할 수 있으며, 상기 요소는 다음의 목록에서 선택된다.

[0033] - 상기 장치에 연관된 스마트 오브젝트(메모리 카드 또는 안전 요소)의 식별 코드,

[0034] - 패스코드 또는 PIN,

[0035] - 유전 또는 또는 생체 식별(identification) 데이터,

[0036] - 위치,

[0037] - 시간, 또는

[0038] - 다른 멤버(예를 들어, 관리자) 또는 상기 사용자가 속한 그룹이 상기 데이터에 액세스하고 있는지 여부

[0039] 상기 장치는 NFC (near field communication) 태그, 생체 센서/리더 또는 신호 송출 장치로부터 코드를 읽고 파티션을 식별하고 액세스할 수 있다. NFC 태그, 생체 센서/리더 또는 신호 송출 장치는 파티션을 선택하고 결국은 파티션을 여는데 필요한 장치 정보를 제공(제공하지 않는다면, 사용자가 입력할 필요가 있음) 할 수 있다.

[0040] 상기 신호 송출 장치는 Bluetooth, BLE(Bluetooth Low energy), wifi, zigbee, NFC, GPS, 또는 ISO14443 장치, 또는 임의의 형태의 비접촉 통신을 사용하는 장치일 수 있다.

[0041] 파티션은 제3자 웹 기반 또는 클라우드 기반 서비스 (예를 들어, 은행이 제공하는 인터넷 뱅킹 또는 물류 회사가 제공하는 물류 추적(parcel tracking))로의 연결을 가능하게 하는 데이터를 저장할 수 있다.

[0042] 상기 파티션을 특정하는 데이터는, PIN 또는 패스코드, 및 사용자 고유 데이터 중 하나 이상을 포함할 수 있다. 상기 장치의 상기 사용자 고유 데이터는, 예를 들어, 상기 사용자의 유전 및/또는 생체 정보를 나타내는 데이터를 포함할 수 있다.

[0043] 상기 장치는 전화(휴대 또는 유선), 스마트폰, 태블릿, 랩탑 컴퓨터, 데스크탑 컴퓨터, TV, 셋톱박스, 카메라, 자동차, 게임 콘솔, 안경, 시계, Chromecast, (예를 들어, 건물의 전기, 가스 또는 수도 소비량을 측정하는) 스마트 미터, 장신구(jewellery), 여행 카드, 은행 카드, ATM 장치, 의복, 운동 용품, E-리더, 쌍안경, MP3 플레이어, 휴대형 게임 콘솔, 비행기, 기차, 자전거, 배 또는 버스와 같은 운송 수단, EPO, 주방기기, 거울, 핸드백, 지갑, 모자, 유모차, Hi-fi 또는 다른 음악 재생장치 또는 라디오, 또는 원격 또는 탈착식 장치와 데이터를 송수신할 수 있는 장치이거나 이들을 포함할 수 있다.

[0044] 장치, 또는 바람직하게 안전 요소 또는 메모리 카드는, 데이터에 액세스하기 위해 설치된 데이터 액세스 소프트웨어 코드를 가진다. 바람직하게, 데이터 액세스 소프트웨어 코드를 설치하기 위해서, 상기 장치는, 예를 들어 적어도 안전 요소 또는 메모리 카드의 식별 코드에 관련된 정보를 제출함으로써 시스템에 등록해야 한다.

[0045] 상기 방법은 바람직하게 상기 단계 (i) 내지 (iii) 이전에, 안전 요소 또는 메모리 카드의 식별 코드, 또는 이것에 기초한 코드 또는 인증서를 상기 데이터에 등록하는 단계를 포함한다.

[0046] 하나 이상의 안전 요소 또는 메모리 카드의 식별 코드는 상기 데이터에 연관될 수 있다. 따라서, 하나 이상의 장치가 데이터에 등록될 수 있으며 상기 데이터에 안전하게 액세스할 수 있다.

[0047] 마스터 장치는 예를 들어, 추가 장치에 연관된 식별 코드를 등록하거나 등록을 요청할 수 있다.

[0048] 상술한 바와 같이, 식별 코드는 바람직하게 상기 장치의 스마트 오브젝트에 연관된 식별 코드이다. 스마트 오브젝트는, 예를 들어, SIM, 가상 SIM, SIM 소프트웨어, TPM(Trusted Platform Module), SE(secure element), TEE(trusted execution environment), Micro SD, Memory card, USB 키 또는 장치에 연관된 스마트카드일 수 있다. 상이한 스마트 오브젝트가 상이한 장치에 대한 식별 코드를 제공하는데 사용될 수 있다. 스마트 오브젝트는 내장(local), 원격(remote) 또는 탈착식(removable) 메모리 중 어느 하나일 수 있다.

[0049] 일부 경우에, 장치는, 적어도 하나의 추가 장치 역시 상기 데이터에 액세스하고 있으면, 상기 데이터에 액세스

하도록 허용될 수 있다. 일부 경우에, 적어도 하나의 추가 장치는, 관리자 장치와 같은 특정 장치이어야 할 수 있다.

[0050] 다른 측면에 따르면, 장치로부터 데이터로의 액세스를 제어하는 방법이 제공되고, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며, 상기 방법은, (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 수신하는 단계-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; (ii) 적어도 부분적으로 상기 식별 코드에 기초하여 상기 데이터로의 액세스가 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 포함한다.

[0051] 본 측면은 상술한 첫 번째 측면의 추가적인 또는 선택적인 특징 중 하나를 포함할 수 있다.

[0052] 바람직하게, 상기 본 측면의 방법은 데이터 액세스 컨트롤러에 의해 수행된다. 데이터 액세스 컨트롤러는 상기 데이터에 액세스하고자 하는 상기 장치로부터 원격으로 위치한다. 예를 들어, 데이터 액세스 컨트롤러는 클라우드에 위치할 수 있다.

[0053] 다른 측면에 따르면, 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장된 데이터로의 액세스를 제어하는 데이터 액세스 컨트롤러가 제공되며, 상기 데이터 액세스 컨트롤러는, (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 수신하고-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; (ii) 적어도 부분적으로 상기 식별 코드에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하고; 및 (iii) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 수행한다.

[0054] 데이터 액세스 컨트롤러는 상기 데이터에 액세스하고자 하는 상기 장치로부터 원격으로 위치한다. 예를 들어, 데이터 액세스 컨트롤러는 클라우드에 위치할 수 있다.

[0055] 액세스될 데이터는 제3자 웹 기반 또는 클라우드 기반 서비스로의 액세스를 가능하게 하는 데이터일 수 있다. 본 발명의 이후 측면들은 (그들의 바람직한 또는 선택적인 특징과 함께) 본 선택적인 특징도 포함할 수 있다.

[0056] 상기 데이터에 액세스하는 요청은 클라우드 기반 파티션에 의해 수신될 수 있다. 적용 가능하다면, 본 발명의 이후 측면들은 (그들의 바람직한 또는 선택적인 특징과 함께) 본 선택적인 특징도 포함할 수 있다.

[0057] 다른 측면에 따르면, 장치 및 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장된 데이터로의 액세스를 제어하는 데이터 액세스 컨트롤러를 포함하는 시스템이 제공되며, 상기 장치는 상기 데이터에 액세스하는 요청을 상기 데이터 액세스 컨트롤러로 전송하고, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; 및 상기 데이터 액세스 컨트롤러는 적어도 부분적으로 상기 식별 코드에 기초하여 상기 데이터로의 액세스가 허용 또는 거부할지 검증하고 그에 따라서 상기 데이터로의 장치 액세스를 허용 또는 거부한다.

[0058] 다른 측면에 따르면, 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장된 데이터로의 액세스를 제어하는 컴퓨터 프로그램이 제공되며, 상기 프로그램은 프로세서에 의해 실행될 때 (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 수신하고-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; (ii) 적어도 부분적으로 상기 식별 코드에 기초하여 상기 데이터로의 액세스가 허용 또는 거부할지 검증하고; 및 (iii) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 수행한다.

[0059] 다른 측면에 따르면, 장치가 액세스 컨트롤러를 통해서 데이터에 액세스하도록 상기 장치를 상기 액세스 컨트롤러에 등록하는 방법이 제공되고, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며, 상기 방법은, 데이터에 액세스하기 위해 장치를 등록하는 요청을 전송하는 단계-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; 상기 데이터로의 액세스를 허용할 것인지 검사하는 단계; 및 액세스가 허용되면, 상기 식별 코드를 액세스될 데이터에 대하여 등록하는 단계를 포함한다.

[0060] 상기 요청은 바람직하게 예를 들어, 상기 장치에 연관된 안전 요소 또는 메모리 카드의 상기 식별 코드, 하나 이상의 PIN 또는 패스코드, 및 사용자 고유 데이터에 기초하는 이중 또는 삼중 요소 인증 코드를 포함한다. 이것은 어떤 장치가 파티션 액세스를 요청했는지의 검사 추적(auditable trail)을 가능하게 한다.

[0061] 상기 요청은 이메일 또는 SMS 형태일 수 있다.

[0062] 상기 방법은 바람직하게 상기 요청에 관련된 정보를 관리자 장치로 전송하는 단계를 더 포함하되, 바람직하게 상기 관리자 장치는 상기 데이터로의 액세스를 허용할지 여부를 결정한다. 예를 들어, 상기 요청에 관련된 정보

는 액세스 컨트롤러 또는 등록하려는 장치로부터 전송될 수 있다. 관리자 장치는, 파티션 읽기만 가능하거나 파티션을 편집, 삭제, 추가적인 내용을 추가할 수 있는 권한과 같은 사용자에 대한 액세스 허가(access permission)를 설정하는데 사용될 수 있다.

[0063] 예를 들어, 자녀의 장치(예를 들어, 전화기나 태블릿)의 안전 요소 또는 메모리 카드가 부모의 데이터에 액세스할 수 있도록 등록된 경우에, 부모의 장치(예를 들어, 전화기나 태블릿)의 안전 요소 또는 메모리 카드는 그 데이터에 대한 관리자로 등록될 수 있어서 자녀의 데이터로의 액세스를 감시하고 제어할 수 있다. 데이터 자체는 부모의 관리자 장치에 실제로 저장될 수 있다. 따라서, 장치 (또는 복수의 장치들)는 하나 이상의 추가 장치가 그 장치에 저장된 데이터에 액세스하는 것을 (각각) 허용하지만, 예를 들어, 제한된 또는 특정된 읽기/권한 허가로 허용할 수 있다.

[0064] 바람직하게, 상기 장치가 상기 데이터에 액세스를 허용하도록 관리자가 결정하면, 이것을 지시하는 신호가 상기 관리자로부터 상기 액세스 컨트롤러로 전송된다.

[0065] 다른 측면에 따르면, 장치가 액세스 컨트롤러를 통해서 데이터에 액세스하도록 상기 장치를 상기 액세스 컨트롤러에 등록하는 방법이 제공되고, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며, 상기 방법은, 데이터에 액세스하기 위해 장치를 등록하는 요청을 수신하는 단계-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; 상기 데이터로의 액세스를 허용할 것인지 검사하는 단계; 및 액세스가 허용되면, 상기 식별 코드를 액세스될 데이터에 대하여 등록하는 단계를 포함한다.

[0066] 다른 측면에 따르면, 데이터에 액세스할 수 있는 장치의 등록을 제어하기 위한 데이터 액세스 컨트롤러가 제공되며, 상기 데이터 액세스 컨트롤러는, 데이터에 액세스하기 위하여 장치를 등록하는 요청을 수신하는 단계-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; 상기 데이터로의 액세스를 허용할 것인지 검사하는 단계; 및 액세스가 허용되면, 상기 식별 코드를 액세스될 데이터에 대하여 등록하는 단계를 수행한다.

[0067] 다른 측면에 따르면, 장치 및 데이터에 액세스할 수 있는 장치의 등록을 제어하기 위한 데이터 액세스 컨트롤러를 포함하는 시스템이 제공되며, 상기 데이터 액세스 컨트롤러는, 상기 장치로부터 데이터에 액세스하기 위하여 장치를 등록하는 요청을 수신하는 단계-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; 상기 데이터로의 액세스를 허용할 것인지 검사하는 단계; 및 액세스가 허용되면, 상기 식별 코드를 액세스될 데이터에 대하여 등록하는 단계를 수행한다.

[0068] 상기 시스템은 바람직하게 관리자 장치를 더 포함한다.

[0069] 상기 데이터 액세스 컨트롤러는 바람직하게 등록될 장치에 대해 상기 데이터로의 액세스가 허용되는지 여부를 검사하는 관리자 장치로 신호를 전송한다.

[0070] 상기 관리자 장치는 바람직하게 등록될 장치에 대해 상기 데이터로의 액세스가 허용되는지 여부를 확인 및/또는, 읽기만 또는 편집, 삭제, 추가적인 내용을 추가할 수 있는 권한과 같은, 액세스를 요청하는 장치에 대해 액세스 허가를 설정하는 신호를 전송한다.

[0071] 다른 측면에 따르면, 데이터에 액세스할 수 있는 장치의 등록을 제어하기 위한 컴퓨터 프로그램이 제공되며, 상기 컴퓨터 프로그램은 프로세서에 의해 실행될 때 상기 장치로부터 데이터에 액세스하기 위하여 장치를 등록하는 요청을 수신하는 단계-여기서, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; 상기 데이터로의 액세스를 허용할 것인지 검사하는 단계; 및 액세스가 허용되면, 상기 식별 코드를 액세스될 데이터에 대하여 등록하는 단계를 수행한다.

[0072] 다른 측면에 따르면, 장치에서 데이터에 액세스하는 방법이 제공되고, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며, 상기 방법은, 장치에서 상기 데이터에 액세스하는 초대를 수신하는 단계-여기서, 상기 초대는 패스워드, 코드 또는 PIN을 포함함; 상기 장치로부터 상기 데이터에 액세스하는 요청을 전송하는 단계-여기서, 상기 요청은 상기 패스워드, 코드 또는 PIN을 포함함; 적어도 부분적으로 상기 패스워드, 코드 또는 PIN에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 포함한다.

[0073] 따라서, 사용자가 추가 장치로 초대를 전송하여 (자기 소유 또는 다른 사용자가 소유한) 추가 장치가 데이터에 액세스하는 것이 가능하다. 이 장치들(또는 거기에 연관된 식별 코드)은 액세스를 허용 받기 위해서 등록될 필요는 없다.

[0074] 이 측면에 따르면, 액세스는 제한없는 시간 동안 또는 미리 결정된 시간 동안 허용될 수 있다. 양 경우에서, 액세스가 허용된 이후 예를 들어 다른 사용자에 의한 액세스는 금지될 수 있다.

[0075] 패스워드, 코드 또는 PIN은 예를 들어 난수 발생기에 의해 생성될 수 있다.

[0076] 상기 패스워드, 코드 또는 PIN은 일회용 패스워드이다. 이는 추가 사용자에게 액세스를 허용하는 안전한 방법을 제공할 수 있다.

[0077] 바람직하게, 상기 패스워드, 코드 또는 PIN은 특정된 시구간 동안에만 유효하다. 따라서, 특정된 시구간 동안에 사용되지 않으면, 상기 패스워드, 코드 또는 PIN에 기초하여 액세스는 허용되지 않을 것이다. 시구간은 예를 들어 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 15, 20, 25, 30, 45, 60, 90 또는 120 분까지 일 수 있다. 시구간은 바람직하게 24시간 이하이다. 한편, 일부 실시예에서, 상기 패스워드, 코드 또는 PIN은 특정한 만료 시간을 가지지 않을 수 있다.

[0078] 바람직하게, 상기 패스워드, 코드 또는 PIN은 적어도 안전 채널을 통해 장치로 및/또는 장치로부터 전송(바람직하게는 장치로 및 장치로부터)된다.

[0079] 일부 실시예에서, 상기 패스워드, 코드 또는 PIN은 마스터 장치와 같은 상기 데이터로의 액세스를 제어하는 장치에 의해 생성된다. 대체적으로, 마스터 장치는 이와 동일한 기능성을 마스터 장치가 아닌 장치(non-master device)에 허용할 수 있다.

[0080] 상기 방법은 제1 장치가 제2 장치의 데이터 액세스를 허용하는 방법이되, 상기 데이터는 상기 제1 장치 및 상기 제2 장치로부터 원격으로 저장되고, 상기 초대는 상기 제1 장치로부터 상기 제2 장치로 전송되고, 상기 데이터에 액세스하는 상기 요청은 상기 제2 장치로부터 전송되며, 상기 데이터로의 액세스는 상기 제2 장치에 대해 허용되거나 거부될 수 있다.

[0081] 이 경우, 상기 패스워드, 코드 또는 PIN은 제1 장치에서 생성될 수 있다.

[0082] 대체적으로, 상기 패스워드, 코드 또는 PIN은, 제1 장치 및 제2 장치 모두로부터 원격으로, 예를 들어, 상기 데이터로의 액세스를 제어하는 프로세서에서 생성될 수 있다.

[0083] 어느 경우에서도, 바람직하게 상기 방법은 생성된 패스워드, 코드 또는 PIN을 액세스될 상기 데이터에 등록하는 단계를 더 포함한다.

[0084] 상기 생성된 패스워드, 코드 또는 PIN을 액세스할 데이터에 등록하는 단계는, 상기 생성된 패스워드, 코드 또는 PIN을 등록하기 전에, 상기 제1 장치가 상기 데이터에 액세스하는 추가 장치를 초대하도록 허용되었는지를 검증하는 단계를 포함할 수 있다.

[0085] 상기 방법은 생성될 패스워드, 코드 또는 PIN에 대한 요청을 상기 제1 장치로부터 전송하는 단계를 더 포함하되, 상기 생성될 패스워드, 코드 또는 PIN은, 상기 제1 장치가 상기 데이터에 액세스하는 추가 장치를 초대하도록 허용되었다고 검증된 이후에만 생성된다.

[0086] 따라서, 어느 경우에서도, 인가된 장치만이 상기 데이터에 액세스하는 추가 장치를 초대할 수 있다.

[0087] 상기 제1 장치가 상기 데이터에 액세스하는 추가 장치를 초대하도록 허용되었는지를 검증하는 단계는, 상기 장치에 연관된 안전 요소 또는 메모리 카드와 같은, 상기 장치에 연관된 식별 코드를 검증하는 단계를 포함한다.

[0088] 상기 제1 장치가 상기 데이터에 액세스하는 추가 장치를 초대하도록 허용되었는지를 검증하는 단계는, 상기 제1 장치로부터 전송된 파티션을 특정하는 데이터를 검증하는 단계를 더 포함할 수 있다.

[0089] 파티션을 특정하는 데이터는, PIN 또는 패스코드, 및 상기 사용자의 유전 및/또는 생체 정보와 같은 상기 장치의 사용자 고유 데이터 중 하나 이상을 포함한다.

[0090] 다른 측면에 따르면, 장치에서 데이터로의 액세스를 허용하는 방법이 제공되고, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며, 상기 방법은, 상기 장치로 상기 데이터에 액세스하는 초대를 전송하는 단계-여기서, 상기 초대는 패스워드, 코드 또는 PIN을 포함함; 상기 장치로부터 상기 데이터에 액세스하는 요청을 전송하는 단계-여기서, 상기 요청은 상기 패스워드, 코드 또는 PIN을 포함함; 적어도 부분적으로 상기 패스워드, 코드 또는 PIN에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 포함한다.

[0091] 상기 초대는 관리자 장치로부터, 바람직하게는 액세스 컨트롤러를 통해서 전송될 수 있다. 상기 초대는 이메일 또는 SMS 메시지와 같은 메시지 형태이며 및/또는 데이터 액세스 어플리케이션 내의 메시지 시스템을 통해 전송되고 볼 수 있다. 사용자가 이 어플리케이션을 열거나 로그인하면, 그들은 특정 데이터에 액세스하는 초대가 수신되었음을 알 수 있다. 사용자는 이후 데이터에 액세스할 수 있다.

[0092] 초대는, 웹 브라우저(파티션 액세스 어플리케이션을 통하는 경우와 반대로)를 통해서 파티션에 액세스하기 위해 사용자가 웹 브라우저에 입력할 수 있는 OTP를 포함할 수 있다.

[0093] 다른 측면에 따르면, 제1 장치, 제2 장치, 및 데이터 액세스 컨트롤러를 포함하는 시스템이 제공되고, 상기 제1 장치는 데이터에 액세스하는 상기 제2 장치를 초대하되, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되고, 상기 제1 장치는 상기 제2 장치로 데이터에 액세스하는 초대를 전송하되, 상기 초대는 패스워드, 코드 또는 PIN을 포함하고; 상기 제2 장치는 상기 데이터에 액세스하는 요청을 전송하되, 상기 요청은 상기 패스워드, 코드 또는 PIN을 포함하고; 및 상기 데이터 액세스 컨트롤러는 적어도 부분적으로 상기 패스워드, 코드 또는 PIN에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하며, 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부한다.

[0094] 다른 측면에 따르면, 장치에서 데이터에 액세스하는 방법이 제공되고, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며, 상기 방법은, (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 전송하는 단계-여기서, 상기 요청은 상기 요청에 관련된 데이터를 포함함; (ii) 적어도 부분적으로 상기 요청에 관련된 데이터에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 그리고 상기 데이터에 액세스하는 적어도 하나의 추가 장치가 있으면, 상기 데이터로의 장치 액세스를 허용하는 단계를 포함한다.

[0095] 그러한 방법은, 추가 장치가 있는 경우에만 금융 거래, 메시징 및/또는 (예를 들어, 비밀) 데이터 보기와 같은 특정 동작이 실행되도록 하는 안전한 환경을 제공할 수 있다. 추가 장치(예를 들어, 관리자 장치)는 상기 장치에 의해 수행되는 동작을 감지할 수 있다. 이후, 필요하다면, 상기 데이터로의 추가 액세스 차단 또는 방지와 같은 즉각적인 동작이 취해질 수 있다.

[0096] 상기 방법은, 단계 (iii) 이전에, 적어도 하나의 추가 장치가 상기 데이터에 액세스하고 있는지를 검사하는 단계를 바람직하게 포함한다. 적어도 하나의 추가 장치는, 예를 들어, “마스터” 장치와 같은 특정 장치일 수 있다.

[0097] 다른 측면에 따르면, 장치에서 데이터로의 액세스를 제어하는 방법이 제공되고, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며, 상기 방법은, (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 수신하는 단계-여기서, 상기 요청은 상기 요청에 관련된 데이터를 포함함; (ii) 적어도 부분적으로 상기 요청에 관련된 데이터에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 그리고 상기 데이터에 액세스하고 있는 적어도 하나의 추가 장치가 있으면, 상기 데이터로의 장치 액세스를 허용하는 단계를 포함한다.

[0098] 다른 측면에 따르면, 장치에서 데이터로의 액세스를 제어하는 데이터 액세스 컨트롤러가 제공되고, 상기 데이터는 상기 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장되며, 상기 데이터 액세스 컨트롤러는, (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 수신하는 단계-여기서, 상기 요청은 상기 요청에 관련된 데이터를 포함함; (ii) 적어도 부분적으로 상기 요청에 관련된 데이터에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 그리고 상기 데이터에 액세스하고 있는 적어도 하나의 추가 장치가 있으면, 상기 데이터로의 장치 액세스를 허용하는 단계를 수행한다.

[0099] 상기 데이터 액세스 컨트롤러는, 상기 단계 (iii)을 수행하기 이전에 적어도 하나의 추가 장치가 상기 데이터에 액세스하고 있는지를 바람직하게 검사한다.

[0100] 다른 측면에 따르면, 장치 및 상기 장치에서 데이터로의 액세스를 제어하는 데이터 액세스 컨트롤러를 포함하는 시스템이 제공되며, 상기 데이터 액세스 컨트롤러는, (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 수신하는 단계-여기서, 상기 요청은 상기 요청에 관련된 데이터를 포함함; (ii) 적어도 부분적으로 상기 요청에 관련된 데이터에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 그리고 상기 데이터에 액세스하고 있는 적어도 하나의 추가 장치가 있으면, 상기 데이터로의 장치 액세스를 허용하는 단계를 수행한다.

[0101] 바람직하게, 상기 장치는 상기 데이터에 액세스하는 요청을 상기 데이터 액세스 컨트롤러로 전송한다.

[0102] 상기 데이터 액세스 컨트롤러는 상기 단계 (iii)을 수행하기 이전에 적어도 하나의 추가 장치가 상기 데이터에 액세스하고 있는지를 바람직하게 검사한다.

[0103] 다른 측면에 따르면, 장치로부터 원격으로 저장되거나 탈착식 스토리지에 저장된 데이터로의 액세스를 제어하는 컴퓨터 프로그램이 제공되며, 상기 프로그램은 프로세서에 의해 실행될 때 (i) 상기 장치로부터 상기 데이터에 액세스하는 요청을 수신하고- 여기서, 상기 요청은 상기 요청에 관련된 데이터를 포함함; (ii) 적어도 부분적으로 상기 요청에 관련된 데이터에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 그리고 상기 데이터에 액세스하고 있는 적어도 하나의 추가 장치가 있으면, 상기 데이터로의 장치 액세스를 허용하는 단계를 수행한다.

[0104] 상기 컴퓨터 프로그램은 상기 단계 (iii)을 수행하기 이전에 적어도 하나의 추가 장치가 상기 데이터에 액세스하고 있는지를 바람직하게 검사한다.

[0105] 본 발명의 다른 측면은 장치에서 데이터에 액세스하는 방법에 관련되고, 상기 데이터는 상기 장치로부터 원격으로 저장, 탈착식 스토리지에 저장, 또는 상기 장치에 저장되며, 상기 방법은, (i) 상기 데이터에 액세스하는 요청을 전송하는 단계-여기서, 상기 요청은 다음 중 하나 이상의 상기 장치에 연관된 식별 코드를 포함함: PIN 또는 패스코드, 및 사용자의 유전 및/또는 생체 정보와 같은 사용자 고유 데이터; (ii) 상기 식별 코드, 및 PIN 또는 패스코드 및/또는 상기 사용자 고유 데이터에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 포함한다.

[0106] 상기 데이터는 파티션에 저장된다. 이 경우, 상기 PIN 또는 패스코드, 및/또는 유전 및/또는 생체 정보와 같은 상기 장치의 상기 사용자 고유 데이터는 사용자가 액세스하려는 상기 데이터에 연관된다. 예를 들어, 상기 PIN 또는 패스코드, 및/또는 유전 및/또는 생체 정보와 같은 상기 장치의 상기 사용자 고유 데이터는 상기 데이터 또는 상기 데이터가 저장된 파티션을 식별할 수 있다.

[0107] 유전 및/또는 생체 정보의 경우에, 상이한 손가락으로부터 채취된 지문은 상이한 데이터 또는 파티션에 연관되어, 어느 지문이 입력되어 전송되는지에 따라 상응하는 데이터 또는 파티션에 액세스할 수 있다.

[0108] 본 발명의 다른 측면은 장치에서 데이터로의 액세스를 제어하는 방법에 관련되고, 상기 데이터는 상기 장치로부터 원격으로 저장, 탈착식 스토리지에 저장, 또는 상기 장치에 저장되며, 상기 방법은, (i) 상기 데이터에 액세스하는 요청을 수신하는 단계-여기서, 상기 요청은 다음 중 하나 이상의 상기 장치에 연관된 식별 코드를 포함함: PIN 또는 패스코드, 및 사용자의 유전 및/또는 생체 정보와 같은 사용자 고유 데이터; (ii) 상기 식별 코드, 및 PIN 또는 패스코드 및/또는 상기 사용자 고유 데이터에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 포함한다.

[0109] 본 발명의 다른 측면은 장치에서 데이터로의 액세스를 제어하는 데이터 액세스 컨트롤러에 관련되고, 상기 데이터는 상기 장치로부터 원격으로 저장, 탈착식 스토리지에 저장, 또는 상기 장치에 저장되며, 상기 데이터 액세스 컨트롤러는, (i) 상기 데이터에 액세스하는 요청을 수신하는 단계-여기서, 상기 요청은 다음 중 하나 이상의 상기 장치에 연관된 식별 코드를 포함함: PIN 또는 패스코드, 및 사용자의 유전 및/또는 생체 정보와 같은 사용자 고유 데이터; (ii) 상기 식별 코드, 및 PIN 또는 패스코드 및/또는 상기 사용자 고유 데이터에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 수행한다.

[0110] 본 발명의 다른 측면은 장치에서 데이터로의 액세스를 제어하는 컴퓨터 프로그램에 관련되고, 상기 데이터는 상기 장치로부터 원격으로 저장, 탈착식 스토리지에 저장, 또는 상기 장치에 저장되며, 상기 컴퓨터 프로그램은 프로세서에 의해 실행될 때 (i) 상기 데이터에 액세스하는 요청을 수신하는 단계-여기서, 상기 요청은 다음 중 하나 이상의 상기 장치에 연관된 식별 코드를 포함함: PIN 또는 패스코드, 및 사용자의 유전 및/또는 생체 정보와 같은 사용자 고유 데이터; (ii) 상기 식별 코드, 및 PIN 또는 패스코드 및/또는 상기 사용자 고유 데이터에 기초하여 상기 데이터로의 액세스를 허용 또는 거부할지 검증하는 단계; 및 (iii) 검증 결과에 따라 상기 데이터로의 장치 액세스를 허용 또는 거부하는 단계를 수행한다.

[0111] 본 발명의 측면들은, 본 발명의 다른 측면들의, 바람직한 또는 선택적인 특징을 포함하는, 특징들 중 어느 하나를 포함할 수 있다.

[0112] 임의의 측면에서, 상기 데이터는 암호화된다. 바람직하게, 상기 데이터는 상기 데이터에 액세스하는 장치에 의해 복호된다. 이 경우에, 상기 장치는 상기 데이터를 복호하기 위한 키를 바람직하게 가질 수 있다. 상기 키는 안전 요소 또는 메모리 카드에 바람직하게 저장되나 원격으로 저장될 수도 있다. 바람직하게, 상기 키 자체는 암호화된다. 상기 키는, 예를 들어, TSM (trusted service manager)에 의한, 안전한 방식으로 상기 장치로 바람직하게 전달된다.

[0113] 이상으로부터, 본 발명의 실시예들이 다음의 방법들과 시스템을 제공할 수 있음이 이해될 수 있다.

[0114] 복수의 장치들이 파티션 액세스를 할 수 있음

[0115] 사용자들은 제어와 검사 추적을 유지한 채 다른 사용자(장치)와 안전하게 공유할 수 있음

[0116] 거래는 안전하게 수행될 수 있음

[0117] 복수의 장치들은 동일한 원격 파티션에 액세스할 수 있다.

[0118] 데이터 또는 파티션에 액세스하면, 상기 장치는 하나 이상의 다음 서비스에 액세스할 수 있다: 메시징, 미디어, TV, 영화, 라디오, 잡지, 소셜 미디어, 전자상거래, 스마트 장치(예를 들어, 유틸리티 등 및 홈 컨트롤), 기업 서비스, 그림, 사진 및 비디오 공유, 정부 서비스, 금융 서비스, 의료 서비스, 여행 서비스, 음악 및 게임. 물론, 여기에 언급되지 않은 추가 서비스들이 더 있을 수 있으며, 액세스 가능할 수 있다.

[0119] 장치들은, 파티션에 액세스하기 위해서 이중 또는 삼중 요소 인증을 제공할 수 있다. 장치는, 스마트 오브젝트의 식별 코드인 단일 요소의 인증으로 보호될 수 있으며, 패스코드 또는 PIN, 또는 유전 또는 생체 식별 데이터의 형태, 또는 위치, 또는 시간, 또는 다른 멤버(예를 들어, 관리자) 또는 사용자가 속한 그룹이 데이터에 액세스하고 있는지 여부인, 추가적인 요소 또는 요소들의 인증으로 보호될 수 있다.

[0120] 다음 표는 사용자가 파티션에 액세스하기 위해 사용하는 예시적인 장치 및 그들에 대응하는 "스마트 오브젝트"(예를 들어, 안전 요소 또는 메모리 카드)를 열거하고 있다. 스마트 오브젝트는, 그것의 식별 코드가 파티션에 연관되어 있으며 허용된 상기 파티션에 액세스하기 위해 반드시 검증되어야 하는, 오브젝트이다.

*표 1*

[0121]

| 장치 | 스마트 오브젝트 |
|---|---|
| 전화 | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, (NFC 스마트폰용)NFC 스마트 오브젝트 |
| 태블릿 | SIM, SE, TEE, Micro SD, 메모리 카드 |
| 랩탑 | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, TPM, Micro SD, 메모리 카드, USB 키 , 스마트카드 |
| 데스크탑 | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |
| TV | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |
| 셋톱박스 | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |
| 카메라 | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |
| 자동차 | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |
| 게임 콘솔 | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |
| 안경 | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |
| 시계 | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |
| Chromecast | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |
| 스마트 미터(홈 유틸리티) | SIM, 가상 SIM, SIM 소프트웨어, SE, TEE, Micro SD, 메모리 카드, USB 키, 스마트카드 |

[0122] 다음과 같은 상이한 종류의 파티션이 제공될 수 있다.사용자만이 액세스할 수 있는 폐쇄된 파티션

[0123] 초대에 의해 다른 사용자와 공유할 수 있는 폐쇄된 파티션

[0124] 검사된 이력 추적을 가진 공개 파티션

[0125] 사용자의 이력 또는 검사 추적을 가지지 않는 공개 및 익명 파티션

[0126] 타임 슬롯과 같은 원칙에 기초하여 어느 종류의 파티션도 공개 또는 폐쇄로 전환될 수 있다. 예를 들어, 파티션은 특정한 미리 지정된 시간에 공개로 설정되며, 특정한 미리 지정된 시간에 폐쇄될 수 있다.

[0127] 사용자는 복수의 장치를 파티션에 대해 등록할 수 있으며, 전환, 편집 및 업로드 기능을 그들이 등록하는 추가 장치에 대해 등록할 수 있다. 예를 들어, 사용자는 그들의 카메라가 파티션에 사진을 업로드하고 파티션 내에서 사진을 보는 권한을 가지길 원하지만, 파티션 내에서 어떠한 내용도 삭제하거나 편집하는 권한은 가지지 않기를 원한다.

[0128] 사용자는 하나 또는 복수의 장치를 파티션의 관리자 장치로 선택할 수 있다. 이는 관리자가 파티션으로의 액세스를 제어하고 필요하다고 보이면 액세스를 멈출 수 있도록 한다. 사용자는 또한, 관리자의 권한 내에서, 사용자가 관리자인 파티션에 액세스가 허용된 모든 다른 사용자들의 장치들에 액세스할 수 있다. 이는 사용자가 실시간으로 파티션에 대한 액세스 허가를 편집하거나 삭제할 수 있도록 한다. 또한, 그가 장치를 분실하거나 더 이상 소유하지 않으면, 사용자가 장치에 대한 액세스를 금지할 수 있도록 한다.

[0129] 관리자 장치는 사용자가 전환할 수 있으며 등록된 스마트 오브젝트에 연결되지 않은 기계에 로그인하는 액세스를 그에게 줄 수 있는 바람직하게 시간에 민감한 코드를 생성하는 권한을 가질 수 있다. 이 코드는 임의의 길이가 될 수 있고 및/또는 액세스 컨트롤러에 연결된 인터페이스에 입력될 수 있으며 파티션으로의 액세스가 데스크탑 또는 랩탑과 같이 등록되지 않은 장치에서 허용되도록 할 수 있다. 사용자는, 예를 들어, 관리자 장치에서 정지 버튼을 가동함으로써, 이 세션을 임의의 시점에 관리자 장치로부터 정지하는 권한을 가질 수 있다. 생성된 코드는, 바람직하게, 관리자 장치와의 이중 또는 삼중 요소 인증의 결과이다.

[0130] 스마트 오브젝트는 그들에 부여된 동일 또는 상이한 패스코드/인증자(authenticator)를 가진 복수의 파티션을 관리할 수 있다. 파티션 내에서, 시스템은 사용자가 로그인하거나 자동적으로 많은 상이한 제3자 서비스에 로그인하도록 허용할 수 있다. 파티션 내에서, 시스템은 사용자에 의해 설정된 사용자 ID 및 패스워드를 사용자 ID 및 패스워드에 대한 문자와 숫자 스트링으로 변환할 수 있다. 이는 제3자 서비스 제공자에게 전달될 수 있다. 이들 코드는 그 서비스에 대한 최선 가이드라인(best practice guideline)에 기초하여 갱신(renew)될 수 있다. 예를 들어, 사용자가 영국에서 NHS Information Governance 요건에 따라 의료 기록에 액세스하고 있다면 그들은 60일마다 갱신될 수 있다.

[0131] 따라서, 본 발명의 다른 측면에 따르면, 장치를 사용하여 클라우드 기반 또는 웹 기반 제3자 서비스에 액세스하는 방법이 제공되며, 상기 방법은 (i) 상기 장치로부터 상기 장치에 연관된 클라우드 기반 파티션에 대한 요청을 전송하는 단계-여기서, 상기 파티션은 상기 제3자 서비스에 연결할 수 있는 데이터를 포함하며, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; (ii) 적어도 부분적으로 상기 식별 코드에 기초하여 상기 파티션으로의 액세스를 허용 또는 거부할지 검증하는 단계; (iii) 검증 결과에 따라 상기 파티션으로의 장치 액세스를 허용 또는 거부하는 단계; 및 상기 파티션으로의 액세스가 허용된 후 (iv) 크리덴셜을 상기 제3자 서비스로 전송하는 단계를 포함한다.

[0132] 본 발명의 다른 측면에 따르면, 장치에 의해 클라우드 기반 또는 웹 기반 제3자 서비스로의 액세스를 제어하는 방법이 제공되며, 상기 방법은 (i) 상기 장치로부터 상기 장치에 연관된 클라우드 기반 파티션에 대한 요청을 수신하는 단계-여기서, 상기 파티션은 상기 제3자 서비스에 연결할 수 있는 데이터를 포함하며, 상기 요청은 상기 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함함; (ii) 적어도 부분적으로 상기 식별 코드에 기초하여 상기 파티션으로의 액세스를 허용 또는 거부할지 검증하는 단계; (iii) 검증 결과에 따라 상기 파티션으로의 장치 액세스를 허용 또는 거부하는 단계; 및 상기 파티션으로의 액세스가 허용되면 (iv) 크리덴셜을 상기 제3자 서비스로 전송하는 단계를 포함한다.

[0133] 따라서 제3자 서비스로의 액세스는, 상기 장치에 연관된 정확한 식별 코드가 제공되어야만 허용된다. 따라서, 그들은 정확한 식별 코드를 제공할 수 없기 때문에, 비인가된 장치가 제3자 서비스에 액세스하는 것이 방지될 수 있다.

[0134] 다음의 바람직한 특징들은 전술한 본 발명의 두 측면에 동일하게 적용된다.

[0135] 상기 장치가 특정 파티션에 액세스할 수 있도록 하기 위해서, 상기 장치는 그 안에 파티션에 액세스하기 위해 적합한 소프트웨어(예를 들어, 어플리케이션)을 설치할 수 있다. 이것은, 예를 들어, 상기 장치에 연관된 안전 요소 또는 메모리 카드에 저장된다.

[0136] 대체적으로, 상기 어플리케이션은 상기 안전 요소 또는 메모리 카드에 부분적으로만 저장될 수 있다. 예를 들어, 어플리케이션은 표준 모바일 어플리케이션 및 안전 요소 내부의 애플릿으로 구성될 수 있다.

[0137] 상기 파티션은 다수의 상이한 웹 서비스에 연관될 수 있다.

[0138] 인증 코드에 적어도 부분적으로 기초하여, 상기 파티션으로의 액세스가 허용된다고 검증되면, 상호 인증 절차가 장치의 안전 요소 또는 메모리 카드와 클라우드 파티션 사이에서 개시될 수 있다. 이 절차는 장치의 안전 요소 또는 메모리 카드와 클라우드 파티션 사이에 안전 채널의 생성을 가능하게 한다. 이후 데이터는 장치의 안전 요소 또는 메모리 카드와 클라우드 파티션 사이에서 전송될 수 있다. 데이터는 암호화될 수 있다.

[0139] 상기 크리덴셜을 전송하는 (iv) 단계는, 상기 장치의 상기 안전 요소 또는 메모리 카드와 상기 파티션 사이에 상호 인증 절차를 수행하는 단계; 및 상기 장치의 상기 안전 요소 또는 메모리 카드와 상기 파티션 사이에 안전 채널을 생성하는 단계를 포함한다. 상기 단계는 상기 크리덴셜을 상기 안전 채널을 통해 상기 파티션으로 전송하는 단계를 포함할 수 있다. 상기 크리덴셜은 암호화될 수 있으며, 이 경우 상기 크리덴셜은 상기 안전 채널을 통한 전송 이전에 암호화된다. 이후 크리덴셜은 파티션에 의해 제3자 서비스에 제공될 수 있다.

[0140] 대체적으로, 상기 크리덴셜은 상기 파티션의 안전 요소에 저장될 수 있다. 그 경우, 크리덴셜을 안전 요소 또는 메모리 카드로부터 상기 파티션으로 전송할 필요가 없다. 대신에, 상기 크리덴셜은, 상기 파티션으로의 액세스가 상기 장치에 허용되면, 상기 파티션으로부터 상기 제3자 서비스로 직접 전송될 수 있다.

[0141] 상기 크리덴셜은 암호화된 형태로 제3자 서비스에 전송될 수 있다. 그 경우, 호환되는 안전 요소가 웹 서비스의 레벨에서 구현되어 전송된 암호화된 크리덴셜의 비암호화(de-encryption)를 가능하게 한다.

[0142] 상기 안전 요소 또는 메모리 카드는, 예를 들어, 고유 식별 코드를 가진 “스마트 오브젝트” 또는 안전 또는 부정 조작 방지(tamper-proof) 하드웨어 장치이며, 고유 식별 코드 역시 이상적으로 안전하고 부정 조작이 방지된다. 상기 안전 요소 또는 메모리 카드는, 예를 들어, SIM, 가상 SIM, SIM 소프트웨어, TPM(Trusted Platform Module), SE(secure element), TEE(trusted execution environment), Micro SD, Memory card, USB 키 또는 스마트카드일 수 있다.

[0143] 따라서, 안전 요소는 데이터(예를 들어, 키, 알고리즘, 애플릿, 크리덴셜)를 안전하게 저장 및/또는 처리할 수 있는 다양한 종류의 안전한 칩, 장치 또는 소프트웨어 솔루션에 대한 일반적인 명칭이다.

[0144] 안전 요소 또는 메모리 카드는 내장, 원격 또는 탈착식 메모리 중 어느 하나일 수 있다.

[0145] 안전 요소 또는 메모리 카드의 식별 코드는 바람직하게는, 예를 들어, 안전 요소 또는 메모리 카드의 세이프 박스에서 잘 보호되고 저장된다. 바람직하게, 식별 코드는 안전 채널을 통해 전송된다. 대체적으로 또는 추가적으로, 식별 코드는 암호화될 수 있다. 이는 절차를 더욱 안전하게 하며 식별 코드가 제3자에 의해 인터셉트 및/또는 발견되지 않도록 하는데 도움이 된다.

[0146] 상술한 바와 같이, 상기 요청은 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드를 포함한다. 그러나, 식별 코드는 상기 요청에 변형된 형태로 포함될 수 있는데, 예를 들어, 암호화된 형태 및/또는 하나 이상의 추가 코드, 데이터 또는 정보와 결합될 수 있다.

[0147] 상기 요청은 상기 장치에서 입력된 패스코드 또는 PIN을 포함하며, 상기 (ii) 단계는 상기 패스코드 또는 PIN에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 포함한다. 따라서, 상기 데이터에 액세스하기 위해서 이중 요소 인증이 요구된다.

[0148] 패스코드 또는 PIN은 상기 장치에 연관된 안전 요소 또는 메모리 카드 (예를 들어, SIM, 또는 가상 SIM)에 의해 (먼저) 검증될 수 있다.

[0149] 대체적으로 또는 추가적으로, 상기 요청은 상기 장치의 사용자 고유 데이터를 포함하며, 상기 단계 (ii)는 상기 장치의 상기 사용자 고유 데이터에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 포함할 수 있다. 따라서, 데이터에 액세스하기 위해서 이중 또는 삼중 요소 인증이 요구될 수 있으며, 인가된

사용자만이 데이터에 액세스하는 것이 허용될 수 있다.

[0150] 사용자 고유 데이터는, 예를 들어, 지문 또는 홍채 데이터와 같이 상기 사용자의 유전 및/또는 생체 정보를 나타내는 데이터를 포함할 수 있다.

[0151] 대체적으로 또는 추가적으로, PIN 및/또는 사용자 고유 데이터를 사용한 인증 (식별 코드로 이중 또는 삼중 요소 인증)을 대체하거나 추가하여, 다음 형태의 인증이 가능하다.

[0152] 상기 요청은 위치(즉, 사용자가 데이터에 액세스를 시도하는 장소)를 포함하는 데이터를 포함하며, 상기 단계 (ii)는 상기 장소에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 또한 포함할 수 있다.

[0153] 상기 요청은 시간(즉, 사용자가 데이터에 액세스를 시도하는 시간)을 포함하는 데이터를 포함하며, 상기 단계 (ii)는 상기 시간에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 또한 포함할 수 있다.

[0154] 상기 요청은 상기 사용자가 그룹의 일부임을 나타내는 데이터를 포함하며, 상기 단계 (ii)는 상기 그룹의 다른 멤버(예를 들어, 관리자)가 상기 데이터에 액세스할 수 있는지 여부에 기초해서 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계를 또한 포함할 수 있다.

[0155] 본 발명의 바람직한 실시예로, 안전 요소 또는 메모리 카드는 상호 인증 절차를 수행 및/또는 안전 채널을 생성 및/또는 식별 코드 및/또는 PIN 또는 패스코드를 암호화하는데 사용될 수 있다.

[0156] 상기 방법은 사용자 등록 절차를 포함하되, 사용자는 상기 제3자 서비스를 사용하기 위해 등록할 수 있다. 상기 사용자 등록 절차는, 상기 제3자 서비스에 액세스하기 위한 크리덴셜 및/또는 양식 채움 데이터를 수집하는 단계; 및 상기 크리덴셜 및/또는 양식 채움 데이터를 안전하게 저장하는 단계를 포함할 수 있다. 상기 크리덴셜은 사용자 ID 및/또는 패스워드를 포함할 수 있다. 추가적으로, 상기 크리덴셜은 상기 제3자 서비스에 등록하는데 필요한 사용자에 관한 정보(예를 들어, 지불 상세를 포함)를 포함할 수 있다. 예를 들어, 상기 크리덴셜은 하나 이상의 후술하는 정보를 포함할 수 있다: 이름, 성, 타이틀, 주소, 나이, 생일, 성별, 로열티 상태, 로열티 카드 번호, 지불 카드 번호, 카드 종류, 만료일, CVV 코드, ID 카드 또는 여권 번호. 이러한 종류의 정보는 양식 채움 데이터로도 불릴 수 있다.

[0157] 크리덴셜이 사용자 등록 절차에서 수집되는 대신에, 상기 크리덴셜은, 상기 파티션으로의 액세스가 허용된 후에 상기 파티션에 의해 자동적으로 생성될 수 있다. 즉, 등록 절차는, 사용자의 적극적인 개입 없이, 제3자 서비스와 연합하여 장치에 의해서 관리된다. 그러한 경우에, 사용자 등록 절차는, 상기 상호 인증 절차를 초기화하는 단계; 및 상기 제3자 서비스를 선택하는 단계를 포함할 수 있다. 즉, 사용자는 제3자 서비스에 액세스하기 위해서 자기의 크리덴셜을 제공할 필요가 없게 된다. 파티션에 액세스하기 위해서 정확한 식별 코드(및 바람직하게 패스코드/PIN, 패스코드/PIN을 또한 요구하는 실시예에서)가 제공되면 충분할 것이다.

[0158] 상기 크리덴셜 및/또는 양식 채움 데이터는 상기 파티션에 안전하게 저장될 수 있다. 대체적으로, 상기 크리덴셜 및/또는 양식 채움 데이터는 안전 요소 또는 메모리 카드에 안전하게 저장될 수 있다. 양 경우 모두, 상기 크리덴셜은 필요하면 상기 안전 요소 또는 메모리 카드로부터 상기 파티션으로 제공될 수 있다.

[0159] (사용자 ID 및/또는 패스워드와 같은) 크리덴셜이 자동적으로 생성되는 실시예에서, 자동적으로 생성된 크리덴셜은 주기적으로 또는 요청에 의해 갱신될 수 있다. 자동적으로 생성된 크리덴셜의 갱신 주기는 사용자 보안 정책 또는 제3자 서비스 보안 정책에 따라 조정될 수 있다. 자동적으로 생성된 크리덴셜은 다른 수단(예를 들어, PC, 태블릿, 또는 스마트폰 등으로부터 웹 브라우저(즉, 특정 어플리케이션을 사용하지 않음)를 사용한 표준 웹 액세스)에 의해 서비스에 액세스할 때 사용되는 크리덴셜과는 상이할 수 있다. 자동적으로 생성된 크리덴셜의 정교성(sophistication) 및 복잡성(complexity)은 사용자 보안 정책 또는 제3자 서비스 보안 정책에 따라 조정될 수 있다. 패스워드의 최소 길이는 사용자 보안 정책 또는 제3자 서비스 보안 정책에 따라 설정될 수 있다. 사용자 ID 및 패스워드는 둘 이상의 소문자, 대문자, 문장부호 또는 기호, 및 숫자의 조합을 포함하도록 요구될 수도 있다.

[0160] 단일 애플릿이 상기 장치의 안전 요소 또는 메모리 카드에 설치될 수 있으며, 단일 애플릿은 모든 인증 절차 및 서비스로의 액세스를 추진한다. 그러나, 일부 종류의 서비스는 그들 자체의 보안을 관리하는 권한을 요구할 수 있어서, 안전 요소 또는 메모리 카드에 설치된 다른 애플릿에 대해 독립적으로 인증 절차 및 그들의 서비스로의 액세스를 제어할 수 있다. 은행 서비스가 일 예이다. 따라서, 대체적으로, 복수의 애플릿이 장치의 안전 요소

또는 메모리 카드에 저장될 수 있다. 각 애플릿은 소정의 애플릿에 관련된 제3자 서비스에 액세스하는 크리덴셜을 생성하기 이전에 분리된 인증 절차를 수행할 수 있다.

[0161] 장치의 안전 요소 및 메모리 카드와 파티션 사이의 인증 단계뿐 아니라, 상기 방법은 장치의 안전 요소 및 메모리 카드와 상기 제3자 서비스의 안전 요소간 제2 인증 절차를 수행하는 단계를 포함할 수 있다. 이는 제3자 서비스가, 제3자 서비스가 인증 절차에 대한 제어를 요구하는 것과 같이, 추가적인 보안을 요구하는 경우일 수 있다. 제3자 서비스는 예를 들어, 은행일 수 있다.

[0162] 따라서, 상기 크리덴셜을 전송하는 (iv) 단계는, 상기 장치의 상기 안전 요소 또는 메모리 카드와 상기 제3자 서비스의 안전 요소 사이에 상호 인증 절차를 수행하는 단계; 상기 장치의 상기 안전 요소 또는 메모리 카드와 상기 제3자 서비스의 안전 요소 사이에 안전 채널을 생성하는 단계; 상기 크리덴셜을 암호화하는 단계; 및 암호화된 크리덴셜을 상기 안전 채널을 통해 상기 장치의 상기 안전 요소 또는 메모리 카드로부터 상기 제3자 서비스의 안전 요소로 전송하는 단계를 포함할 수 있다.

[0163] 상기 제3자 서비스는 제3자 서비스에 액세스하는 패스코드/PIN을 요청하며, 상기 패스코드/PIN은 상기 장치의 상기 안전 요소 또는 메모리 카드와 상기 제3자 서비스의 안전 요소 사이에 생성된 상기 안전 채널을 통해 전송될 수 있다.

[0164] 바람직하게, 상기 제3자 서비스에 액세스하는 크리덴셜 및/또는 상기 제3자 서비스에 의해 요청된 양식 채움 데이터(form filling data)는, 제2 인증 절차의 성공적인 완료 이후에, 상기 안전 요소 또는 메모리 카드로부터 제3자 파티션으로 안전 채널을 통해 자동적으로 제공된 후 제3자 서비스로 제공된다.

[0165] 상기 제3 자 서비스는 제2 인증 절차의 성공적인 완료 이후에 자동적으로 개시될 수 있다.

[0166] 상기 장치는, 추가 장치(예를 들어, PC 또는 태블릿)도 제3자 서비스에 액세스하도록 허용하는, 마스터 장치로서 동작할 수 있다. 그러한 경우에, 액세스 코드는 상기 장치에서 생성되어 디스플레이될 수 있으며(또는 예를 들어 SMS 또는 이메일에 의해 사용자에게 전송될 수 있음), 사용자에 의해 추가 장치를 사용하여 제3자 서비스에 연관된 웹사이트에 입력될 수 있다. 액세스 코드는 바람직하게 상기 장치에서 구동중인 어플리케이션에 의해 생성될 수 있다.

[0167] 대체적으로, 마스터 장치는 (다른 장치를 위해서 액세스 코드를 생성하는) 동일한 기능을 마스터 장치가 아닌 장치에게 허용할 수 있다.

[0168] 상기 액세스 코드는 시간에 민감, 예를 들어, 특정 시구간 동안만 유효할 수 있다. 시구간은 예를 들어 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 15, 20, 25, 30, 45, 60, 90 또는 120 분까지 일 수 있다.

[0169] 상기 마스터 장치는 새로운 크리덴셜을 생성하거나 상기 제3자 서비스에 액세스하는 크리덴셜을 갱신하는데 사용될 수 있다. 추가 장치가 파티션(및 그에 따라 상기 파티션에 연관된 웹 서비스)에 연결되면, 크리덴셜은 연결된 장치들(즉, 상기 장치와 추가 장치) 사이에서 동기화될 수 있다. 대체적으로 또는 추가적으로, 파티션 내용은 연결된 장치들 사이에서 동기화될 수 있다. 예를 들어, 새로운 크리덴셜, 새로운 서비스, 또는 새로운 내용이 상기 장치로부터 이용 가능할 때, 추가 장치가 연결되고 인증 절차를 성공적으로 통과하자마자 그것들은 추가 장치에 즉시 이용가능하게 된다.

[0170] 상기 장치는 NFC 태그로부터 파티션에 액세스하는 코드를 읽어 오고 상기 파티션으로부터 제3자 서비스를 구동할 수 있다. NFC 태그는 파티션을 선택하고 결국은 파티션을 여는데 필요한 장치 정보를 제공(제공하지 않는다면, 사용자가 입력할 필요가 있음) 할 수 있다.

[0171] 대체적으로, 상기 장치는 생체 센서/리더로부터 파티션에 액세스하는 코드를 읽어 오고 상기 파티션으로부터 제3자 서비스를 구동할 수 있다. 상기 생체 센서/리더는 파티션을 선택하고 결국은 파티션을 여는데 필요한 장치 정보를 제공(제공하지 않는다면, 사용자가 입력할 필요가 있음) 할 수 있다.

[0172] 다른 실시예로, 상기 장치는 상기 장치는 파티션을 선택하고 결국은 파티션을 여는데 필요한 장치 정보를 제공(제공하지 않는다면, 사용자가 입력할 필요가 있음)하는 신호 송출 장치로부터 코드를 수신할 수 있다. 상기 신호 송출 장치는 Bluetooth, BLE(Bluetooth Low energy), wifi, zigbee, NFC, GPS, 또는 ISO14443 장치, 또는 임의의 형태의 비접촉 통신을 사용하는 장치일 수 있다.

[0173] 상기 파티션은 전화 또는 메시징 서비스를 위한 고유 식별자를 저장할 수 있다. 상기 전화 또는 메시징 서비스는, 예를 들어, 휴대 전화 서비스, VOIP 서비스, 또는 인스턴트 메시징 서비스일 수 있다. 상기 고유 식별자는,

사용자 이름 및 패스워드 또는 (국내 또는 국제) 전화번호와 같은, 전화 또는 메시징 서비스 식별자에 링크된다.

[0174] 파티션당 하나의 고유한 식별자를 가진 복수의 파티션이 있을 수 있다. 예를 들어, 한 사용자는 열개의 파티션을 가질 수 있으며, 각각은 하나의 고유 식별자에 연관되며, 각각은 서로 다른 전화 번호에 링크될 수 있다.

[0175] 상기 고유 식별자 및 상기 전화 또는 메시징 서비스 식별자간의 매핑은 상기 장치의 안전 요소 또는 메모리 카드에 저장될 수 있다. 대체적으로, 상기 매핑은 클라우드에 저장될 수 있다. 대체적으로, Mobile Network Operator는 상기 고유 식별자를 전화 또는 메시징 서비스 식별자에 매핑할 수 있도록 한다.

[0176] 상기 식별자가 상기 파티션에 저장되므로, 상기 사용자가 장치로부터 상기 파티션에 액세스할 수 있는 동안, 상기 사용자는 (그들이 상기 파티션에 액세스하기 위해 어떤 장치를 사용하고 있는지에 상관 없이) 전화 또는 메시징 서비스에 액세스 할 수 있다. 그러므로, 사용자는, 사용중인 장치에 상관 없이, 상기 전화 또는 메시징 서비스에 연관된 음성, 텍스트 또는 데이터 메시지를 전송하거나 수신하는 권한을 가질 수 있다.

[0177] 특정 전화 또는 메시징 서비스 식별자 및 연관된 전화 또는 메시징 서비스는 사용자의 위치에 따라 활성화될 수 있다. 사용자의 위치가 이중 또는 삼중 요소 인증 절차의 일부인 경우가 될 수 있다. 예를 들어, 홈 와이파이 네트워크를 통해서 상기 파티션에 연결되면, 집전화 번호가 상기 장치에서 활성화될 수 있다. 유사하게, 다른 나라에서 GPS 또는 4G 기지국을 통해 연결되면, 그 지역 내 현지 전화번호가 상기 장치에서 활성화될 수 있다. 예를 들어, 사용자가 프랑스에 여행을 가면, 프랑스 전화번호가 사용을 위해 생성될 수 있다. 프랑스를 떠나면, 사용자는 그 번호를 유지하거나 다른 사용자가 사용하게 하기 위해서 해제하는 옵션을 받을 수 있다.

[0178] 다른 가능한 어플리케이션은 종업원이 고용주로부터 업무용 휴대 전화를 지급받는 경우이다. 종업원은 개인용 전화기와 업무용 전화기 모두를 휴대하고 싶어하지 않을 수 있다. 대신에, 종업원은 자기의 개인 전화번호에 링크된 고유 식별자를 가진 (업무용 전화기에 연관된) 파티션을 생성할 수 있다. 이후, 종업원은, 고용주의 전화 계약을 사용하지 않고도, 업무용 전화기를 사용하여 전화를 걸고 받을 수 있다.

[0179] 초대는 또한 장치에 의한 클라우드 기반 또는 웹 기반 제3자 서비스로의 액세스를 제어하는 컴퓨터 프로그램까지 연장될 수 있다. 상기 프로그램은 상술한 측면들의 방법(및/또는 상술한 방법들의 바람직한 특징들)을 수행할 수 있다.

[0180] 본 발명의 모든 측면들은, 바람직한 또는 선택적인 특징들을 포함한, 본 발명의 다른 측면들의 특징을 포함할 수 있다.

[0181] 따라서, 본 발명은, 본 발명의 상술한 모든 측면에서 정의된 바와 같이, 데이터 액세스 컨트롤러, 장치를 데이터 액세스 컨트롤러에 등록하는 방법, 장치와 액세스 컨트롤러를 포함하는 시스템, 장치의 등록을 제어하는 컴퓨터 프로그램, 장치에서 데이터에 액세스하는 방법, 장치에서 데이터로의 액세스를 허용하는 방법, 제1 장치, 제2 장치 및 데이터 액세스 컨트롤러를 포함하는 시스템으로 확장되되, 액세스될 데이터는 클라우드 기반 또는 웹 기반 제3자 서비스이고 및/또는 상기 데이터에 액세스하는 요청은 클라우드 기반 파티션에 의해 전송되고 및/또는 수신된다.

[0182] 클라우드 기반 또는 웹 기반 제3자 서비스로의 액세스에 관련된 마지막 두 측면의 바람직한 특징들은, 본 발명의 상술한 모든 측면(및 그 바람직한 특징들)에서 정의된 데이터 액세스 컨트롤러, 장치와 액세스 컨트롤러를 포함하는 시스템, 장치의 등록을 제어하는 컴퓨터 프로그램, 장치에서 데이터에 액세스하는 방법, 장치에서 데이터로의 액세스를 허용하는 방법, 및 제1 장치, 제2 장치 및 데이터 액세스 컨트롤러를 포함하는 시스템과 결합하여 사용될 수 있다.

[0183] 파티션은 또한 복수의 스마트 오브젝트 락(lock)으로 제어될 수 있다. 예를 들어, 파티션은 둘 이상의 상이한 사용자가 파티션에 로그인해야만 개방될 수 있다. 이것은 기업 분야(corporate landscape)에서 문서를 공유하거나 보안이 필요한 회의를 착수하게 될 때 특히 적절하다. 파티션을 개방하는 복수의 스마트 오브젝트의 사용은, 제3자 벤더와의 거래와 같은 서비스 또는 안전한 환경이 필요한 피어-투-피어 거래와 같은 약식 거래(informal transaction)를 허용할 때 제3자의 신분을 보호하는데에도 사용될 수 있다.

[0184] 상술한 많은 측면들은, 장치에 연관된 안전 요소 또는 메모리 카드의 식별 코드에 기초하여, 상기 데이터로의 액세스가 허용 또는 거부될지를 검증하는 단계(또는 유사한 단계)를 언급한다.

[0185] 이 측면들은, 파티션에 액세스(액세스는 파티션의 생성, 편집 또는 삭제를 포함함)하기 위해 이중 (또는 그 이상) 요소 인증을 제공할 수 있다. 인증의 일 요소는 장치에 연관된 스마트 오브젝트(메모리 카드 또는 안전 요

소)의 인증 코드일 수 있으며, 추가 요소(들)은 패스코드 또는 PIN, 또는 유전 또는 생체 식별 정보, 또는 위치, 또는 시간, 또는 다른 멤버(예를 들어, 관리자) 또는 상기 사용자가 속한 그룹이 상기 데이터에 액세스하고 있는지 여부일 수 있다.

[0186] 상술한 내용에 대응하는 측면으로, 요소들 중 하나가 장치에 연관된 메모리 카드 또는 안전 요소의 식별 코드일 필요는 없다.

[0187] 따라서, 본 발명의 다른 측면으로, 상기 파티션과 상기 장치 사이에 상호 인증을 수행하는 단계; 및 상기 파티션과 상기 장치 사이에 안전 채널을 생성하는 단계를 포함하되, 상기 인증은 이중 또는 삼중 요소를 포함하며, 상기 요소는 다음의 목록에서 선택되는 장치로부터 파티션에 액세스하는 방법이 제공된다. 상기 장치에 연관된 스마트 오브젝트(메모리 카드 또는 안전 요소)의 식별 코드, 패스코드 또는 PIN, 유전 또는 또는 생체 식별(identification) 데이터, 위치, 시간, 또는 다른 멤버(예를 들어, 관리자) 또는 상기 사용자가 속한 그룹이 상기 데이터에 액세스하고 있는지 여부. 바람직하게, "액세스"는 파티션의 생성, 편집 또는 삭제를 포함한다.

[0188] 상기 목록에 포함된 요소들은, 본 발명의 측면들을 참조하여 이상에서 상세히 설명되었다.

## 도면의 간단한 설명

[0189] 본 발명의 바람직한 실시예들은 도면을 참조하여 예시를 통해 설명된다.

도 1은 휴대 전화 및 그에 대응하는 클라우드 기반 원격 스토리지를 포함하는 시스템의 개요도이다.

도 2는 휴대 전화, 테블릿 장치 및 그에 대응하는 클라우드 기반 원격 스토리지를 포함하는 시스템의 개요도이다.

도 3은 휴대 전화로부터 원격으로 저장된 데이터로의 인가 및 비인가 액세스 시도들을 나타낸 개요도이다.

도 4는 휴대 전화로부터 원격으로 저장된 데이터로의 인가되고, 초대되고, 인가되지 않은 액세스 시도들을 나타낸 개요도이다.

도 5는 액세스 모니터링을 구비한 휴대 전화로부터 원격으로 저장된 데이터로의 인가되고, 초대되고, 인가되지 않은 액세스 시도들을 나타낸 개요도이다.

도 6은 액세스 모니터링을 구비하지 않은 휴대 전화로부터 원격으로 저장된 데이터로의 인가되고, 초대되고, 인가되지 않은 액세스 시도들을 나타낸 개요도이다.

도 7은 파티션에 액세스할 수 있도록 장치를 등록하는 절차를 나타낸 흐름도이다.

도 8은 인증 절차를 나타낸 흐름도이다.

도 9는 액세스 코드 암호화 절차를 나타낸 흐름도이다.

도 10은 휴대 장치, 클라우드 및 제3자 웹 서비스를 포함하는 시스템의 개요도이다.

도 11은 휴대 장치, 클라우드 및 제3자 웹 서비스를 포함하는 높은 보안을 요구하는 시스템의 개요도이다.

## 발명을 실시하기 위한 구체적인 내용

[0190] 도 1에 도시된 바와 같이, 휴대 전화(1)는 SIM(2)을 포함하며, 클라우드 서버(4)의 데이터 스토리지 파티션들(3a, 3b, 3c)에 액세스한다. SIM(2)은 원격 데이터 파티션들에 액세스하기 위한 소프트웨어를 내장하고 있다.

[0191] 휴대 전화(1)는, 파티션들(3a, 3b, 3c)에 대한 정확한 패스코드 또는 PIN을 입력하면, 파티션들(3a, 3b, 3c)에만 액세스할 수 있다. 각 파티션은 사용자에 의해 설정된 고유 패스코드 또는 PIN을 가지고 있다.

[0192] 정확한 패스코드 또는 PIN에 더해서, SIM(2)으로부터의 식별 코드가 제공되어야만 파티션들(3a, 3b, 3c)에 있는 데이터에 액세스가 허가될 수 있다.

[0193] 사용자가 특정 파티션들(3a, 3b, 3c)에 액세스하길 원하면, 사용자는 휴대 전화(1)의 키패드 또는 터치감지 스크린을 타이핑하여 파티션들(3a, 3b, 3c)에 대한 패스코드 또는 PIN을 입력하여야 한다. 입력된 패스코드 또는 PIN은 SIM(2)에 전달되며, 전달된 패스코드 또는 PIN을 SIM 식별 코드와 결합하여 해쉬를 생성하는 암호화 알고리즘으로 전달된다.

[0194] 이후, 해쉬는 복호되어 패스코드 또는 PIN을 추출하고 사용자가 어느 파티션(3a, 3b, 3c)에 액세스하려고 하는

지를 식별하는 클라우드 서버(4)의 프로세서로 전달된다. 이후, 해쉬가 클라우드 서버(4)의 메모리에 이미 저장된 파티션(3a, 3b, 3c)에 대한 해쉬에 상응하면, 요청된 파티션(3a, 3b, 3c)에 대한 액세스가 허가되며, 파티션(3a, 3b, 3c)에 저장된 데이터는 휴대 전화(1)를 통해 액세스될 수 있다.

[0195] 일부 실시예에서, 예를 들어, 사용자가 보유한 유전 또는 생체(genetic or biometric) ID 형태(예를 들어, 지문 또는 홍채 스캔)와 같은 제3 형태의 인증이, 파티션(3a, 3b, 3c)에 대한 액세스가 허가되기 위해서 더 요구된다. 다른 실시예에서, 이것은 파티션(3a, 3b, 3c)에 대한 패스코드 또는 PIN을 대신하여 요구된다.

[0196] 각 파티션(3a, 3b, 3c)에 저장된 내용 또는 데이터는 암호화되어 있어서, 특정 파티션(3a, 3b, 3c)에 대한 액세스가 허가되면, 파티션(3a, 3b, 3c)의 내용은 파티션(3a, 3b, 3c)에 대한 패스코드 또는 PIN 및 SIM 식별 코드, 또는 SIM(2)에 저장된 키를 이용하여 복호된다.

[0197] 파티션(3a, 3b, 3c) 액세스가 허가되고 그 내용이 복호되면, 내용은 휴대 전화(1)의 스크린에 표시될 수 있다.

[0198] 휴대 전화(1)는 파티션(3a, 3b, 3c)을 제어하는 관리자 장치이다. 그러나, 사용자(또는 다른 사용자)는 파티션(3a, 3b, 3c)에 액세스하려고 하는 추가 장치를 가질 수 있다. 예를 들어, 도 2에 도시된 바와 같이, 사용자는, 파티션(3a, 3b, 3c)에 액세스하려고 하는 SIM(5a)이 장착된 태블릿 장치(5)를 소유하고 있다. 태블릿 장치(50)의 SIM(5a) 역시 파티션(3a, 3b, 3c)에 등록되어 있어서 정확한 PIN 또는 패스코드 및/또는 정확한 유전 또는 생체 정보를 태블릿 장치(5)에 입력하면, 태블릿 장치(5)는 파티션(3a, 3b, 3c) 액세스가 허가된다. 파티션(3a, 3b, 3c) 액세스가 허가되는 방식은 상술한 휴대 전화(1)에 대한 방식과 동일하게 제어된다.

[0199] 도 3은 비인가된 사용자가 클라우드 서버(4)에 저장된 파티션(3M)에 액세스하려는 경우를 나타낸다. 비인가된 사용자는 SIM(7a 또는 7b)이 장착된 휴대 전화(6a 또는 6b)를 각각 소유하고 있다. 파티션 액세스는 액세스 컨트롤러(12)에 의해 제어된다. 액세스 컨트롤러(12)는 클라우드에 위치한다. 일부 실시예에서, 액세스 컨트롤러(12)는 휴대 전화 제공 시스템의 일부이다.

[0200] 비인가 사용자는 PIN 또는 패스코드를 자신의 휴대 전화(6a 또는 6b)에 입력하더라도, PIN 또는 패스코드가 부정확 및/또는 SIM 식별 코드가 부정확하기 때문에 파티션(3M) 액세스는 허가되지 않는다. 액세스 컨트롤러(12)는 휴대 전화(6a 또는 6b)가 파티션(3M)에 액세스하는 것을 허가하지 않는다. 그러나, 메인 휴대 전화(1)가 파티션(3M)에 액세스하는 것은 허가한다.

[0201] 도 4는 비인가 사용자 및 초대된 사용자가 클라우드 서버(4)에 저장된 파티션(3M) 액세스하려는 경우를 나타내고 있다.

[0202] 이 경우에, 도 3의 경우와 같이, 액세스 컨트롤러(12)는 비인가 사용자의 휴대 전화(6a)로 파티션(3M) 액세스를 거부한다.

[0203] 액세스가 초대된 사용자에게 허가되기 위해서, 메인 사용자는 파티션(3M) 액세스에 대한 일회용 패스워드(OTP)를 위한 요청을 자기의 휴대 전화(1)에서 클라우드 서버(4)로 전송한다. 클라우드 서버(4)는 휴대 전화(1)의 SIM(2)의 식별 코드가 파티션(3M)에 등록되었는지와, SIM(2)에 연관된 사용자가 다른 사용자를 초대하여 파티션(3M)에 액세스하게 할 수 있는지를 검증하고, 그렇다면, OTP를 휴대 전화(1)에 반환한다. 메인 사용자는 이후 이 OTP를 초대된 사용자의 휴대 전화(8)로 전송한다. 초대된 사용자는 이후 파티션(3M) 액세스 요청을 액세스 컨트롤러(12)로 전송하고 OTP를 입력한다. 액세스 컨트롤러(12)는 OTP를 검증하고, OTP가 정확하면 초대된 사용자는 파티션(3M) 액세스가 허가된다.

[0204] 대체 실시예로(미도시), 메인 사용자는 자기의 휴대 전화(1)에서 OTP를 생성한 후 OTP를 파티션(3M)에 대한 등록을 위해서 클라우드 서버(4)로 전송한다. OTP는 또한 휴대 전화(1)에서 초대된 사용자의 휴대 전화(8)로 전송된다. OTP가 파티션(3M)에 대해 등록되면, 초대된 사용자는 상술한 OTP를 입력함으로써 파티션(3M)에 액세스할 수 있다.

[0205] 일부 실시예에서, OTP는, 예를 들어 5분과 같이, 특정 시구간 동안에만 유효하다.

[0206] 일부 실시예에서, 파티션(3M) 액세스는 초대된 사용자에게 1-24시간과 같은 특정 시 구간 동안에만 허가된다.

[0207] 일부 실시예에서, OTP는 파티션(3M)에 대한 한 번의 액세스 시도에만 유효하다. 한 번 사용되면, 파티션(3M) 액세스에 더 이상 사용될 수 있다. 파티션(3M)에 대한 다음 번 액세스를 위해서 추가적인 OTP가 메인 사용자에 의해 요청되어야 한다.

[0208] 일부 실시예에서, 필요하다면, 메인 사용자는 초대된 사용자의 파티션(3M) 액세스를 감시 및/또는 차단할 수 있

다.

[0209] 파티션이 클라우드 서버(4)에 설정될 때, "공개" 파티션으로 설정되어 누구나 거기에 저장된 데이터에 액세스할 수 있다. 도 5는 공개 파티션(30A)의 예를 나타낸다. 일부 실시예에서, 일부 사용자는 파티션(30A)에 저장된 데이터로의 "읽기" 액세스만 할 수 있는 반면, 초대 또는 메인 사용자와 같은 다른 사용자는 거기에 저장된 데이터로의 "읽기" 및 "쓰기" 액세스 모두 할 수 있다.

[0210] 도 5에 도시된 경우에서, 파티션(30A)는 메인 휴대 전화(1), 초대 사용자 휴대 전화(8) 및 다른 (초대받지 않은) 사용자의 휴대 전화(10)로부터 액세스될 수 있는 공개 파티션이므로, 파티션(30A)으로의 액세스는 감시되며 메모리(30A-h)에 기록된다. 기록된 데이터는, 예를 들어, 파티션(30A)에 액세스한 장치에 연관된 식별 코드 및/또는 액세스 시도 시간으로 구성된다. 다른 데이터도 기록될 수 있다. 이것은 메인 사용자가 파티션(30A) 액세스를 감시하며, 기록된 데이터에 기초하여, 원한다면, 특정 사용자가 파티션(30A)에 액세스하는 것을 차단할 수 있게 한다.

[0211] 도 6은 파티션(30) 액세스를 감시하는 기능이 없다는 점을 제외하면 도 5와 유사하다.

[0212] 특정 파티션에 액세스할 수 있도록 장치를 등록하기 위해서, 장치에는 파티션에 액세스하기 위해서 적합한 소프트웨어(예를 들어, 어플리케이션)가 반드시 설치되어 있어야 한다. 이것은, 예를 들어, 장치에 연관된 안전 요소(secure element) 또는 메모리 카드에 저장된다.

[0213] 장치가 특정 파티션에 액세스할 수 있도록 장치를 등록하기 위해서, 도 7에 도시된 바와 같이, 후속 절차가 이후에 수행된다.

[0214] 등록될 장치의 사용자는 파티션(들)로의 액세스를 얻기 위한 요청을 파티션 액세스 컨트롤러를 통해 장치로부터 관리자 장치로 전송한다(S1). 요청은, 예를 들어, 이메일 또는 SMS의 형태이다. 요청은 이중 요소 인증 코드(two-factor authenticated code)를 포함한다. 이 코드는 장치에 연관된 안전 요소 또는 메모리 카드의 식별 정보 및 패스코드 또는 PIN 중 어느 하나, 또는 사용자 고유 데이터(data representing something inherent to the user)로부터 생성된다. 이것은 어떤 장치가 파티션 액세스를 요청했는지의 검사 추적을 가능하게 한다.

[0215] 파티션 관리자가 관리자 장치에서 요청을 수신하면, 관리자는 파티션(들)에 대한 액세스를 허가하거나 액세스를 거부할 것인지를 결정한다(S2). 관리자는 파티션 읽기만 가능하거나 파티션을 편집, 삭제, 추가적인 내용을 추가할 수 있는 권한과 같은 사용자에 대한 액세스 허가도 설정할 수 있다.

[0216] 소유자가 파티션에 대한 액세스를 사용자에게 허가하기로 결정하면, 그들은 파티션에 대해 등록될 장치에 대한 그들의 합의를 확인하는 신호를 관리자 장치에서 액세스 컨트롤러로 전송할 수 있어서, 장치는 (관리자에 의해 특정된 액세스 파티션으로) 파티션에 액세스할 수 있다(S3).

[0217] 액세스 컨트롤러는 이후 장치(즉, 메모리 카드 또는 안전 요소에 연관된 식별 코드)를 특정된 액세스 파티션으로 파티션에 대해 등록한다.

[0218] 사용자가 파티션에 액세스하기 위한 어플리케이션을 열거나 로그인하면, 그들은 PIN 또는 패스코드 또는 파티션에 상응하는 사용자 고유 데이터를 입력함으로써 파티션(들)에 액세스할 수 있다. 상이한 장치는 상이한 PIN 또는 패스코드 또는 소정의 파티션에 액세스하기 위해서 사용자 고유 데이터를 가질 수 있다.

[0219] 등록될 장치의 사용자는 관리자와 같이 동일한 사람이거나 상이한 사람일 수 있다.

[0220] 파티션의 관리자는 파티션에 액세스하는 누군가를 초대할 수도 있고 그들에게 그렇게 하라는 초대를 전송할 수도 있다. 상술한 경우와 같이, 초대된 사용자는 반드시 그들의 장치에 파티션에 액세스하기 위해서 적합한 소프트웨어(예를 들어, 어플리케이션)를 반드시 설치하여야 한다. 초대는 액세스 컨트롤러를 통해서 전송된다. 초대는 이메일 또는 SMS 메시지와 같은 메시지 형태이며 및/또는 파티션 액세스 어플리케이션 내의 메시지 시스템을 통해 전송되고 볼 수 있다. 사용자가 이 어플리케이션을 열거나 로그인하면, 그들은 특정 파티션에 액세스하는 초대가 수신되었음을 알 수 있다. 사용자는 이후 파티션에 액세스할 수 있다.

[0221] 초대는, 웹 브라우저(파티션 액세스 어플리케이션을 통하는 경우와 반대로)를 통해서 파티션에 액세스하기 위해 사용자가 웹 브라우저에 입력할 수 있는 OTP를 포함할 수 있다.

[0222] 임의의 사용자가 파티션 액세스 어플리케이션을 열거나 로그인하기 위해서, 사용자는 어플리케이션에 대한 자기의 PIN 또는 패스코드, 또는 생체 정보를 반드시 입력해야 하며, 이것은 그들의 장치에 연관된 안전 요소 또는 메모리 카드에 대한 식별 코드와 함께 검사(check)된다.

[0223] 도 8은 장치의 인증 또는 검증 절차 실시예를 나타낸 흐름도이다. 장치의 사용자는 그들의 장치에서 파티션 액세스 어플리케이션을 열고 로그인한다. 이는 어플리케이션이 열렸음을 알리는 신호가 파티션 액세스 컨트롤러로 자동적으로 전송되도록 한다. 머신-머신 핸드쉐이크가 이후 수행되되, 이는, 장치가 액세스 컨트롤러의 ID 인증서(certificate)를 검사하는 단계뿐 아니라, 액세스 컨트롤러가 SIM(또는 다른 안전 요소 또는 메모리 카드)의 식별 코드가 등록되었는지를 검사하는 단계를 포함한다. 이것은 액세스 컨트롤러로부터 장치로 전송되는 "challenge"에 의해 수행되는데, 이후 "answer"로 응답한다. 이 검사가 정확한 것으로 확인되면, 안전 채널이 장치와 액세스 컨트롤러 사이에 열린다(S5).

[0224] 이후에, 액세스 컨트롤러는 사용자가 액세스하고자 하는 파티션에 대한 그들의 PIN 또는 패스코드를 입력하는 요청을, 안전 채널을 통해서, 장치로 전송한다(S6).

[0225] 사용자는 PIN 또는 패스코드를 입력하고, SIM(또는 장치에 연관된 다른 안전 요소 또는 메모리 카드)은 이것이 정확한지 검사한다. 정확하다면, SIM(또는 다른 안전 요소 또는 메모리 카드)는 입력된 PIN 또는 패스코드에 기초한 인증서를 생성한다(S7).

[0226] 대체 실시예에서, PIN 또는 패스코드 대신에 또는 PIN 또는 패스코드에 추가로, 사용자는, 생체 데이터와 같이, 사용자 고유 데이터를 요청받아서 입력할 수 있다. 인증서는 이 데이터에 기초할 수 있다.

[0227] 생성된 인증서는 이후 장치에서 액세스 컨트롤러로 안전 채널을 통해서 전송된다(S8).

[0228] 액세스 컨트롤러는 인증서를 검사하고, 요청된 파티션에 대해 등록되어 있다면, 장치가 요청된 파티션에 액세스하는 것을 허가하고 장치는 요청된 파티션에 액세스한다(S9).

[0229] 도 9는 초대된 사용자가 파티션에 액세스하기 위한 액세스 코드가 암호화되는 과정을 나타낸 흐름도이다.

[0230] 관리자는, 다른 사용자가 등록되지 않은 장치로부터 파티션에 액세스할 수 있도록(또는 관리자가 파티션에 액세스할 수 있도록) 파티션에 대한 액세스 코드를 제공하고자 할 때, PIN 요청이 액세스 컨트롤러로부터 관리자 장치로 전송된다(S10).

[0231] 관리자는 그들이 액세스를 허가하고자 하는 파티션에 대한 PIN을 관리자 장치에 입력하고, 관리자 장치의 SIM(또는 장치에 연관된 다른 안전 요소 또는 메모리 카드)는 이후 암호화된 코드를 생성한다(S11).

[0232] 암호화된 코드는 이후 관리자 장치에서 액세스 컨트롤러로 안전 채널을 통해 전송된다(S12).

[0233] 액세스 컨트롤러는, 이후에 입력되면, 그 파티션에 대한 액세스가 허가되도록, 암호화된 코드를 파티션에 대해 등록한다(S13).

[0234] 또한, 액세스 컨트롤러는, 초대된 장치가 파티션에 액세스할 수 있도록, 암호화된 코드를 초대된 장치로 안전 채널을 통해 전송한다.

[0235] 일부 실시예에서, 암호화된 코드는 한 번의 액세스 시도에만 및/또는 제한된 시 구간 동안에만 유효하다. 다른 실시예에서, 암호화된 코드는 무기한 유효하거나 만료되지 않는다.

[0236] 일부 실시예에서, 파티션 액세스 어플리케이션은 Apache Cordova Javascript bridge로 액세스되는 API이다. 안전 요소 또는 메모리 카드에 저장되며, 내부(즉, 안전 요소 또는 메모리 카드 내)에서 생성되는 다음의 키와 PIN을 유지한다.

[0237] ● 어플리케이션에 대한 하나의 RSA2048 공개키/개인키 쌍

[0238] ● 사용자를 인증하기 위한 파티션당 하나의 가변 크기 PIN

[0239] ● 암호화된 파일에 사용되는 파티션당 하나의 3DES-2 키

[0240] 서버 또는 액세스 컨트롤러는 장치당 변화될 수 있는 두 개의 3DES-2 마스터 키를 유지한다. 이 두 개의 키는 생성 후 어플리케이션에 전송되며 어플리케이션 보안 영역의 안전 채널에 의해 보호된다.

[0241] ● 어플리케이션의 진정성(authenticity)을 검증하기 위하여 안전 요소 어플리케이션에 의해 반환된 공개키 데이터를 암호화하는데 사용되는 초기화 키(Initialization Key)

[0242] ● 파티션에 대한 원격 액세스 코드를 생성할 때 안전한 시간(Secure Time) 소스를 제공하는데 사용되는 시간키(Time Key)

[0243] Secure Time은 UNIX 타임스탬프 이후에 타겟 장치가 부여한 임시어(nonce)이며, 3DES-2 CBC는 Time Key에 의해 암호화된다.

[0244] 타겟 파일의 크기에 따라서, 파티션 키가 파일 데이터를 직접적으로 암호화하는데 사용되거나, 핸드셋에 의해 관리되는 키가 파일 데이터를 암호화하는데 사용될 수 있다.

[0245] 다음은 사용자 Sarah가 그녀의 파티션 데이터를 다른 사람 Robert와 공유하길 원할 때 전개되는 절차이다.

[0246] 전제 조건:

[0247] ● Robert의 장치 공개키(Public Key)는 인증 서버(액세스 컨트롤러)에 등록되어 있고, (Robert의 이메일과 같은) 공개 식별자에 의해 식별된다.

[0248] ● Sarah가 공유할 파티션에 로그인한다.

[0249] ● Sarah가 이 파티션을 Robert와 공유 요청한다.

[0250] ○ 서버가 Sarah의 어플리케이션에 대한 Secure Time Nonce를 획득한다.

[0251] ○ 서버가 Robert의 Public Key와 현재 Secure Time을 전송하는데, 이 둘은 Sarah의 어플리케이션을 위해 암호화된다.

[0252] ○ 핸드셋 어플리케이션이 공유 블로브(sharing blob)를 획득하고, 공유 코드를 Sarah에게 표시한다.

[0253] ○ 공유 블로브가 서버로 전송되며 Robert의 공개 아이덴티티에 연관된다.

[0254] ○ Sarah가 공유 코드를 (이메일, SMS, 전화, 음성 등으로) Robert에게 제공한다.

[0255] ● Robert는 서버에 연결함으로써 새로운 파티션이 그에게 공유되었음을 알게 되고, Sarah한테 받은 공유 코드를 입력한다.

[0256] ○ 서버가 Robert의 어플리케이션에 대한 Secure Time Nonce를 획득한다.

[0257] ○ 서버가 Sarah의 어플리케이션에 대해 암호화된 공유 블로우와 현재 Secure Time을 전송한다.

[0258] ○ 파티션 액세스 키가 Robert의 안전 요소(Secure Element) 또는 Robert의 어플리케이션에 의해 복구된다.

[0259] 다음의 로우 레벨 매니지먼트 API가 정의된다.

[0260] isSecureElementPresent()

[0261] Secure Element가 존재하면 true를 리턴한다.

[0262] getSecureElementID()

[0263] (CPLC로부터 추출된) Secure Element의 고유 ID를 HexString으로 리턴한다.

[0264] getCCSEApplicationVersion()

[0265] CCPartition 어플리케이션의 버전을 스트링 또는 어플리케이션이 설치되지 않았으면 "undefined"로 리턴한다.

[0266] 다음의 어플리케이션 업데이트 및 설치 API가 정의된다.

[0267] getKeysetCounter(aid, keysetVersion) (HexString, Number)

[0268] 소정의 Security Domain AID에 대한 카운터 및 키셋 버전을 리턴한다.

[0269] executeAPDUScript(apdus) (Array of HexString)

[0270] Secure Element상의 APDU를 실행하며, 각 APDU에 대해 90 00 Status Word가 예상된다.

[0271] getPublicKey()

[0272] Initialization Key로 3DES-2 CBC 암호화된 어플리케이션의 Public Key를 리턴한다.

[0273] createPartition(shortName, pin) (String, HexString)

[0274] 짧은 이름(short name) 및 PIN이 주어진 파티션을 생성하고, 1 바이트의 파티션 ID를 리턴한다.

[0275] listPartitions()

[0276] Secure Element 상에서 생성된 파티션을 식별하는 [id, shortName] Array를 리턴한다.

[0277] deletePartition(id) (Number)

[0278] 파티션을 삭제한다. 사용자는 삭제할 파티션에 반드시 로그인하거나, 파티션의 PIN이 반드시 차단되어야 한다.

[0279] 다음의 Usage API가 정의된다.

[0280] loginPartition(id, pin) (Number, HexString)

[0281] 소정의 파티션에 로그인한다.

[0282] logoutPartition()

[0283] 현재 로그인된 파티션에서 로그아웃한다.

[0284] encryptData(data, iv) (HexString, HexString)

[0285] 소정의 IV와 현재 선택된 파티션 키로 3DES-2 CBC 암호를 사용하여 데이터를 암호화한다.

[0286] decryptData(data, iv) (HexString, HexString)

[0287] 소정의 IV와 현재 선택된 파티션 키로 3DES-2 CBC 암호를 사용하여 데이터를 복호한다.

[0288] getSecureTimeNonce()

[0289] 서버로 전달될 8 바이트 임시어를 리턴하여 되어 다음 Secure Time을 제공한다.

[0290] getSharingCode(secureTime, encryptedPublicKey, validityMinutes) (HexString, HexString, Number)

[0291] 다른 장치를 위한 공유 코드를 얻는다. 예를 들어, 두 개 요소의 Array, 원격 장치로 전달된 블로브, 및 생성된 8자리 코드를 리턴한다. 블로브는, 파티션 키에 연결되고 PKCS #1 패딩을 사용하여 원격 장치의 Public Key로 암호화된, 공유 코드의 유효 시간(validity time)의 만료 타임 스탬프를 포함한다. 다른 실시예로, 공유 코드는 임의의 길이 및/또는 문자와 숫자일 수 있다.

[0292] useSharingCode(secureTime, blob, accessCode) (HexString, HexString, String)

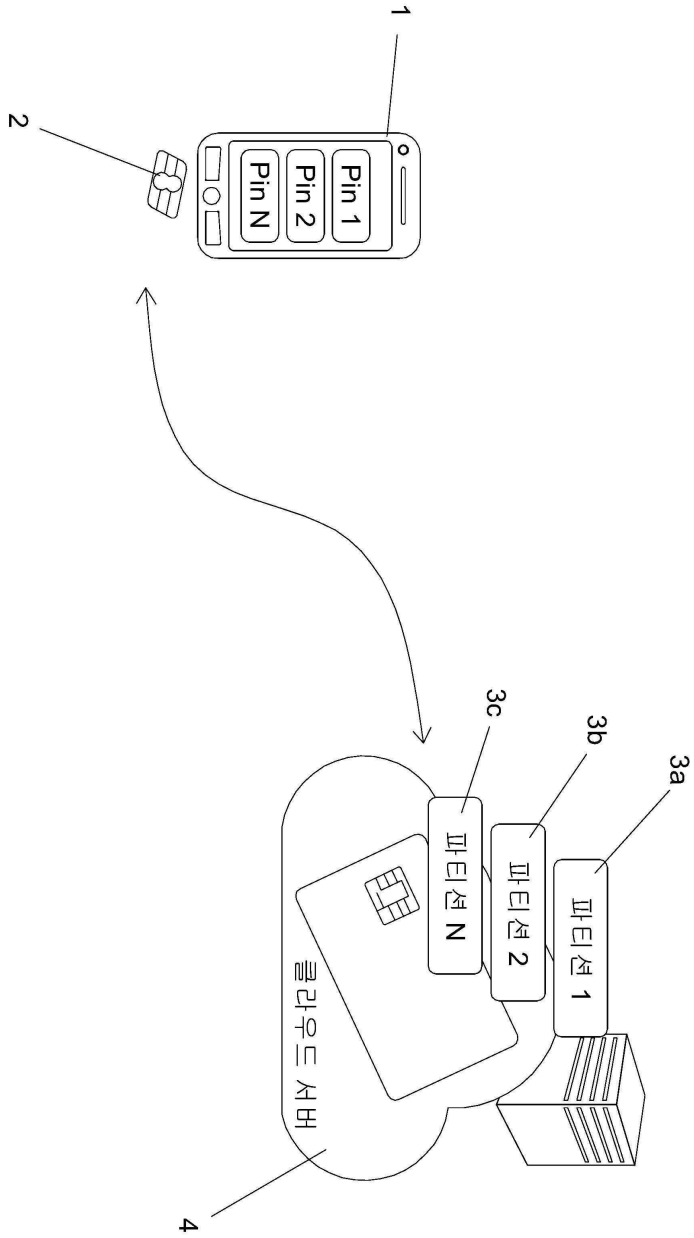
[0293] 원격 장치로부터 획득된 공유 코드를 사용한다. 블로브, 액세스 코드 및 유효 시간이 어플리케이션에 의해 승인되면, 사용자가 로그아웃하거나 Secure Element의 전원이 꺼질 때까지, 파일은 추출된 파티션 키로 파티션 Id 0xff를 사용하여 암호화되고 복호될 수 있다.

[0294] 도 10은 휴대 장치(1), 클라우드(4) 및 제3자 웹 서비스(14)를 포함하는 시스템의 개략적인 구성도이다. 휴대 장치(1)는, 클라우드 파티션(3d)을 통해서 웹 서비스(14)에 액세스를 가능하게 하도록 동작하는 어플리케이션을 구동한다. 어플리케이션이 구동되면, 사용자는 PIN 코드를 입력한다. 정확한 PIN 코드가 제공되면, 클라우드 파티션(3d)이 개방된다. 파티션이 개방되면, 웹 서비스에 액세스하는 크리덴셜(credential) C가 파티션(3d)로부터 전달되어, 웹 서비스(14)에 액세스할 수 있다.

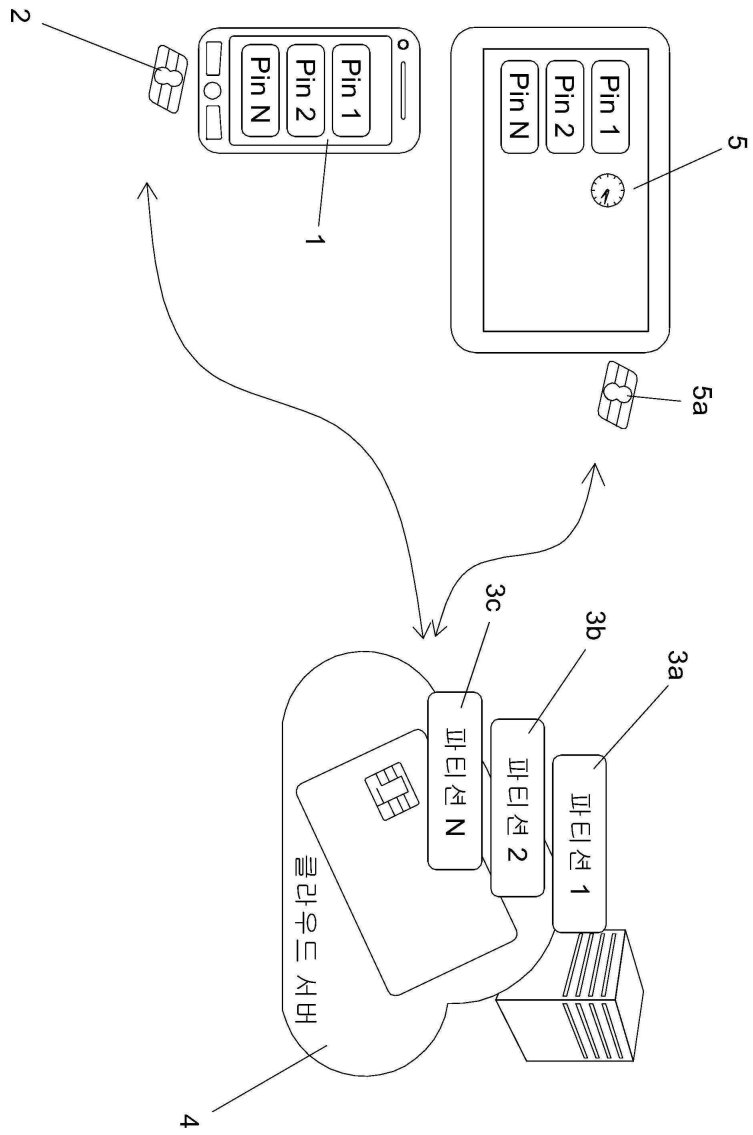
[0295] 도 11은 도10과 유사한 개략적인 구성도이나, 제2 인증이 장치와 제3자 파티션(3e) 사이에서 수행되는 경우를 나타낸다. 도 10과 같이, 휴대 장치(1)는, 클라우드 파티션(3d)을 통해서 웹 서비스(14)에 액세스를 가능하게 하도록 동작하는 어플리케이션을 구동한다. 어플리케이션이 구동되면, 사용자는 PIN 코드를 입력한다. 정확한 PIN 코드가 제공되면, 클라우드 파티션(3d)이 개방된다. 제3자 파티션은 다음 단계를 포함하는 새로운 절차를 개시한다. 장치로부터 새로운 PIN 코드를 요청하고, 정확한 PIN이 수신되면, 장치 안전 요소와 제3자 클라우드 안전 요소간 상호 인증 절차를 개시한다. 웹 서비스에 액세스하는 크리덴셜C가 파티션(3e)로부터 전달되어, 웹 서비스(14)에 액세스할 수 있다.

도면

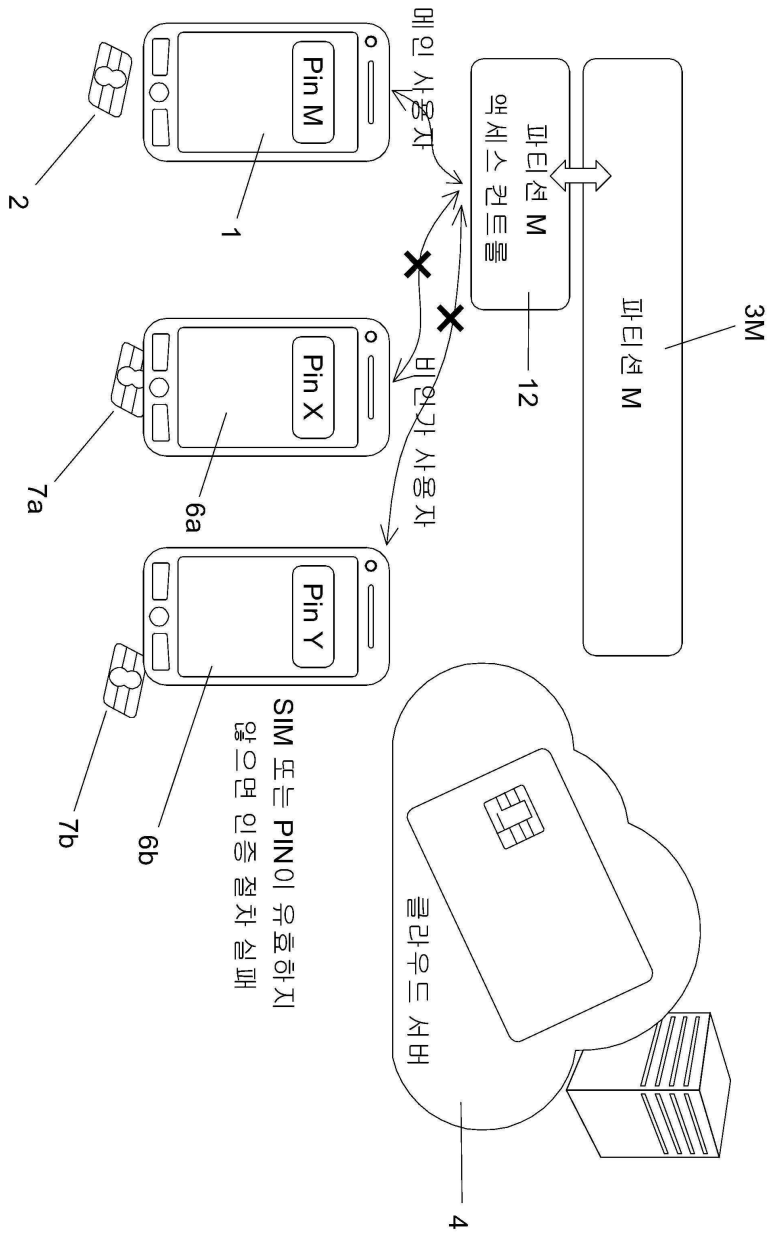
도면1



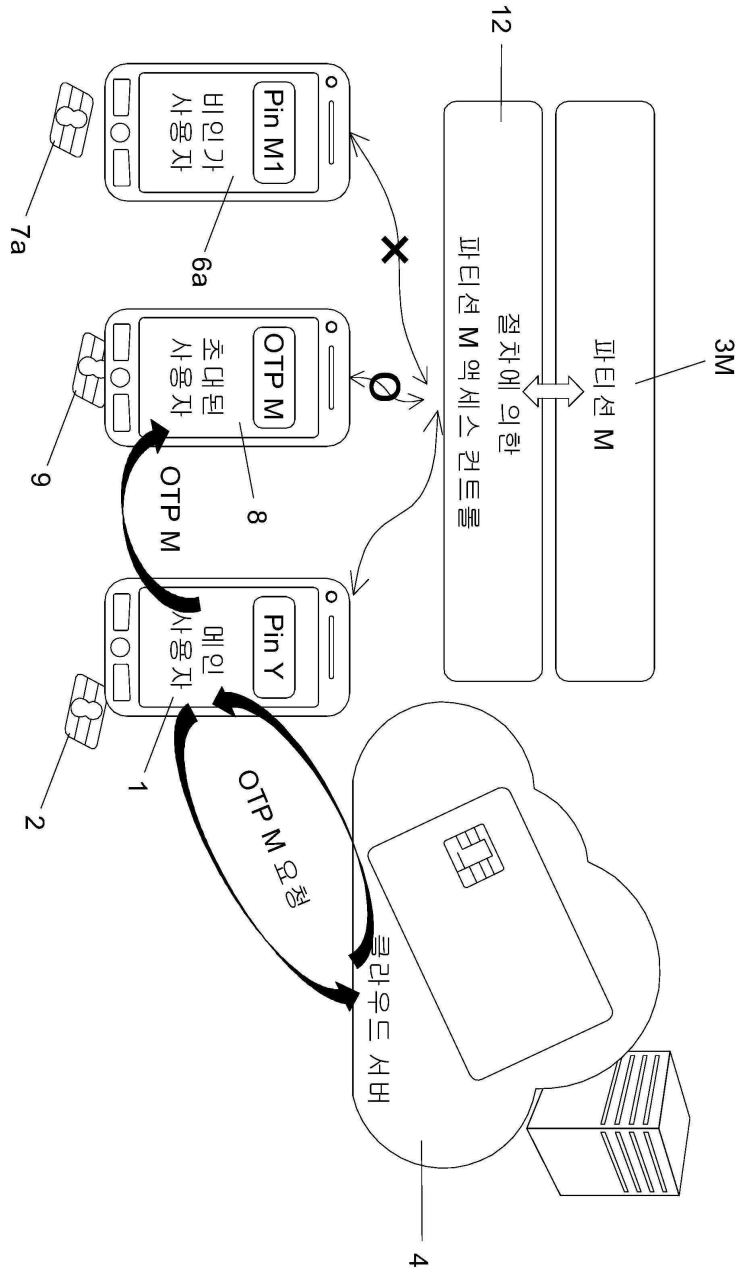
도면2


2
Pin 1
Pin 2
Pin N
1
Pin 1
Pin 2
Pin N
5
5a
3c
3b
3a
파티션 N
파티션 2
파티션 1
클라우드 서버
4

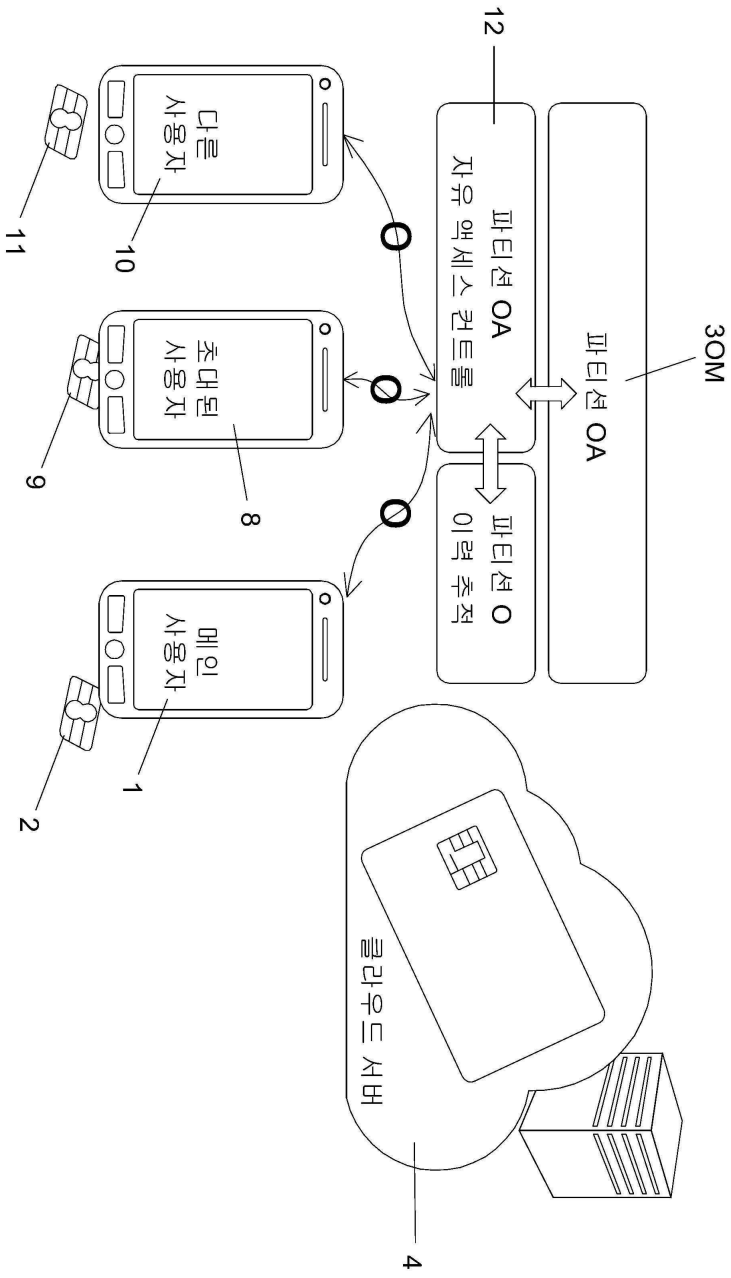
도면3


메인 사용자
파티션 M
액세스 컨트롤
12
3M
파티션 M
Pin M
1
2
비 인가 사용자
Pin X
6a
7a
Pin Y
6b
7b
SIM 또는 PIN이 유효하지
않으면 인증 절차 실패
클라우드 서버
4

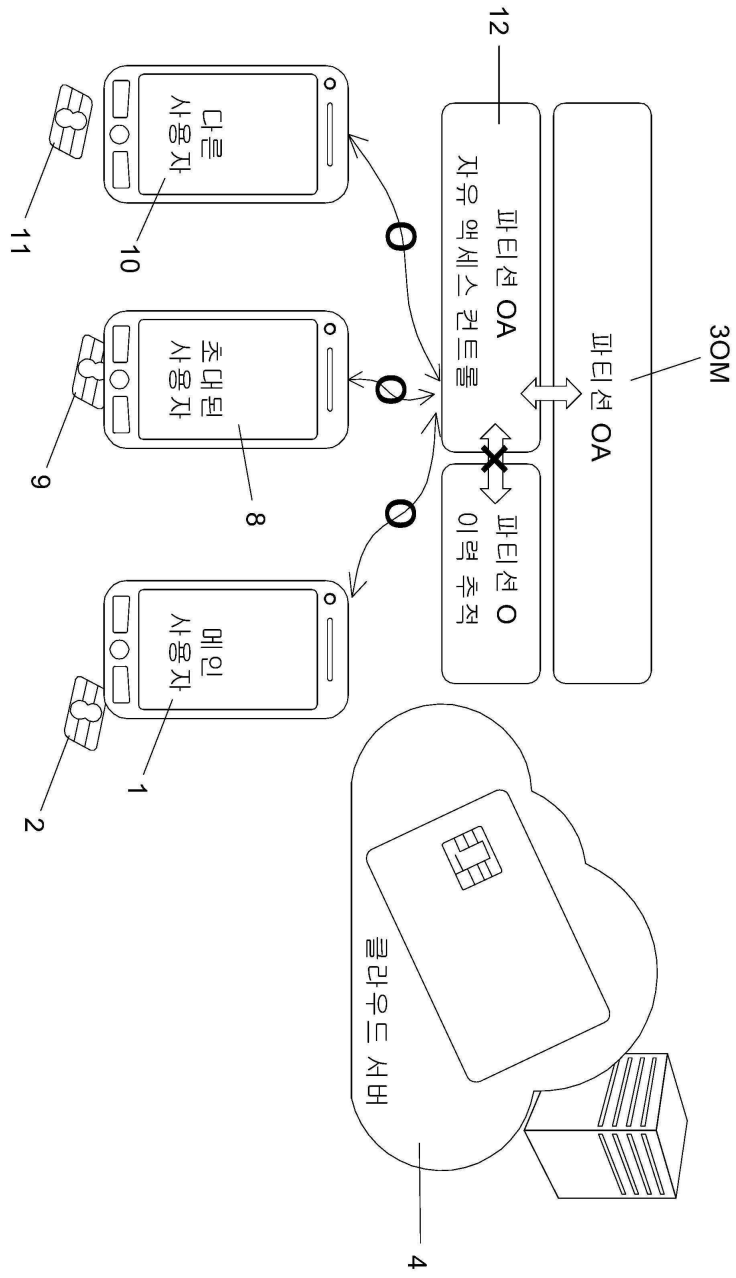
도면4


12
3M
파티션 M
절차에 의한
파티션 M 액세스 컨트롤
Pin M1
비인가
사용자
7a
6a
OTP M
초대된
사용자
9
8
OTP M
Pin Y
메인
사용자
1
2
OTP M 요청
클라우드 서버
4

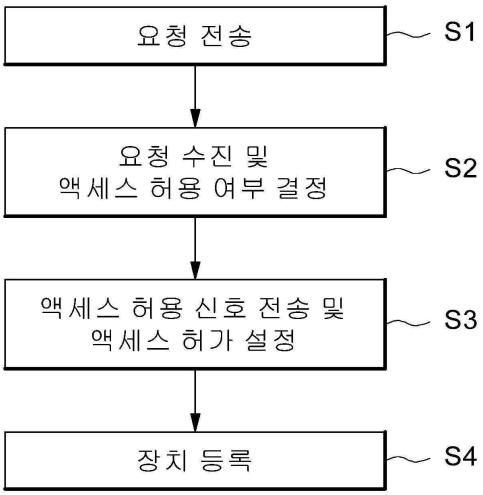
도면5


12
다른 사용자
11
10
파티션 OA 자유 액세스 컨트롤
파티션 OA
30M
초대된 사용자
9
8
파티션 O 이력 추적
메인 사용자
2
1
클라우드 서버
4

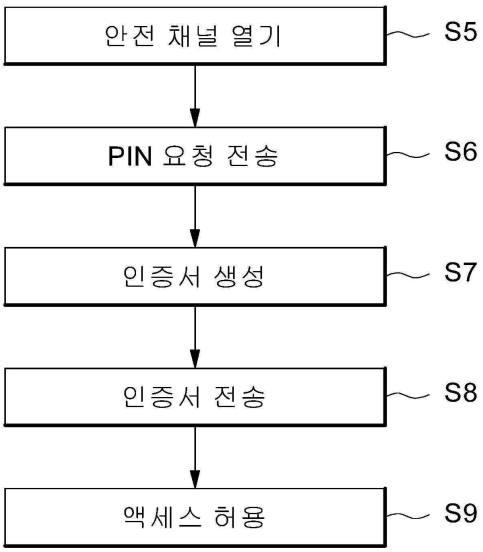
도면6


12
다른 사용자
11
10
파티션 OA 자유 액세스 컨트롤
파티션 OA
30M
초대된 사용자
9
8
파티션 O 이력 추적
메인 사용자
2
1
클라우드 서버
4

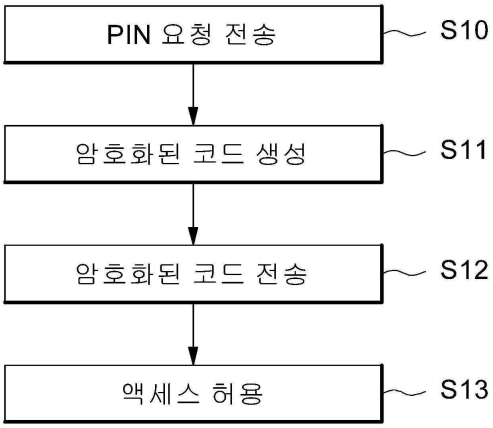
도면7


요청 전송
S1
요청 수신 및
액세스 허용 여부 결정
S2
액세스 허용 신호 전송 및
액세스 허가 설정
S3
장치 등록
S4

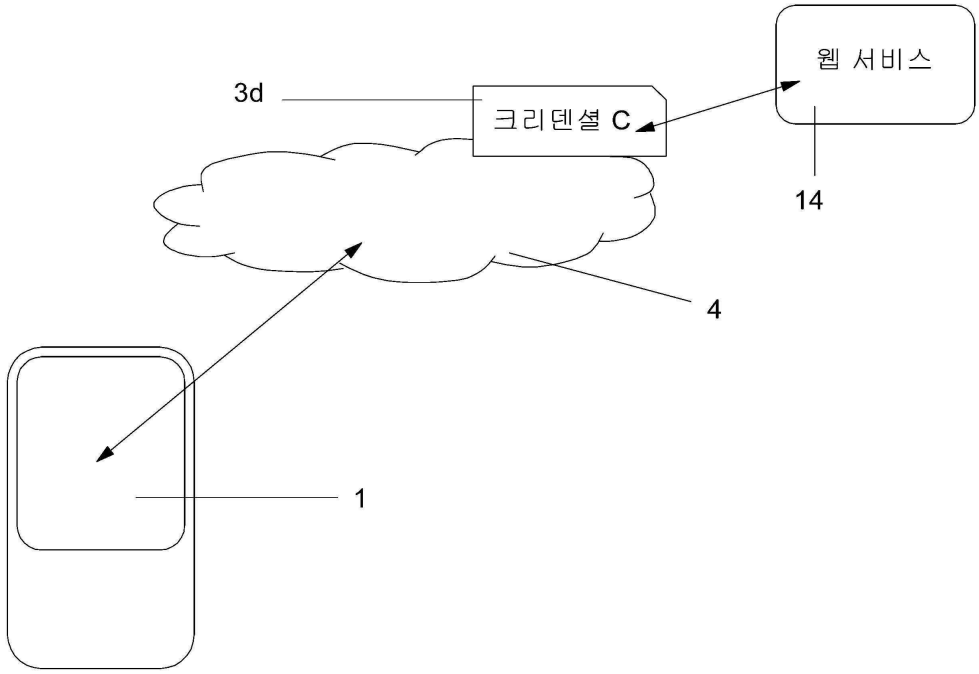
도면8


안전 채널 열기
S5
PIN 요청 전송
S6
인증서 생성
S7
인증서 전송
S8
액세스 허용
S9

도면9


PIN 요청 전송
S10
암호화된 코드 생성
S11
암호화된 코드 전송
S12
액세스 허용
S13

도면10




도면11