(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년09월17일
(11) 등록번호 10-2156803
(24) 등록일자 2020년09월10일

(51) 국제특허분류(Int. Cl.)
H04B 1/40 (2015.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2014-0012729
(22) 출원일자 2014년02월04일
심사청구일자 2019년01월30일
(65) 공개번호 10-2014-0099835
(43) 공개일자 2014년08월13일
(30) 우선권주장
13/758,303 2013년02월04일 미국(US)
(56) 선행기술조사문헌
KR1020110071201 A*
US20090254749 A1*
US20110270751 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
쑤 차오
미국, 캘리포니아 95131, 산호세, 1953 T1A PL
아머 카니
미국, 캘리포니아 95136, 산호세, 4400 더 우즈 드라이브 #1621
(뒷면에 계속)
(74) 대리인
권혁록, 이정순

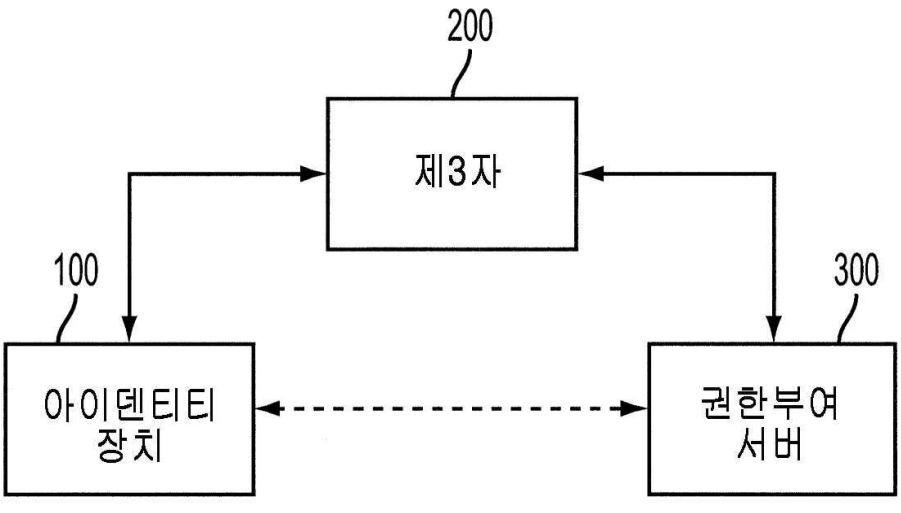
전체 청구항 수 : 총 19 항 심사관 : 임동우

(54) 발명의 명칭 **역권한 부여 방법 및 그 전자 장치**

(57) 요 약

사용자 아이덴티티 제어를 위한 역권한부여 방법 및 그 전자 장치가 제공될 수 있다. 전자 장치는 통신부, 고유 ID 및 복수의 섹션들을 포함하고, 각 섹션은 다른 아이덴티티 정보를 포함하는 저장부, 및 트랜잭션 요구에 응답하여, 상기 통신부를 통해 아이덴티티 정보에 대한 요구를 권한부여 서버로 전송하고, 상기 권한부여 서버로부터 수신된 권한부여 정보에 응답하여 아이덴티티 정보를 제3자에게 전송하여 상기 수신된 권한부여 정보에 따라 상기 트랜잭션을 완료하는 제어부를 포함할 수 있다.

대 표 도 - 도1



(72) 발명자

베니 웡

미국, 캘리포니아 94107, 샌프란시스코, 683 브라난 스트리트 202

뤼펭 쑤

미국, 캘리포니아 95132, 산호세, 2128 뮤리우드가

쉬공 뤼

미국, 캘리포니아 95032, 로스 가토스, 259 하우스 시티

명 세 서

청구범위

청구항 1

전자 장치에 있어서,

권한부여 서버와 광역 통신망을 통해 통신하고, 외부 전자 장치와 근거리 통신망을 통해 통신하도록 구성되는 통신부;

고유 ID 및 각각 다른 카테고리의 아이덴티티(identity) 정보를 포함하는 복수의 섹션들을 포함하는 저장부; 및

제어부를 포함하고, 상기 제어부는,

상기 통신부를 이용하여 상기 근거리 통신망을 통해 상기 외부 전자 장치로부터 트랜잭션(transaction)과 관련된 아이덴티티 정보의 요구를 수신하고,

상기 아이덴티티 정보의 요구에 응답하여, 상기 통신부를 이용하여 상기 광역 통신망을 통해 상기 아이덴티티 정보의 요구에 대응하는 트랜잭션 정보, 및 상기 전자 장치의 식별 정보를 포함하는 요청을 권한부여 서버로 전송하고,

상기 권한부여 서버로부터 권한부여 정보를 수신하고,

상기 트랜잭션을 완료하도록, 상기 수신된 권한부여 정보에 기반하여 상기 저장부에 저장되어 있는 각각 다른 카테고리의 아이덴티티 정보 중 상기 트랜잭션에 대응하는 아이덴티티 정보를 상기 외부 전자 장치에게 전송하도록 구성되고,

상기 권한부여 정보는, 상기 권한부여 서버에 의해 상기 전자 장치의 상기 식별 정보에 기반하여, 상기 전자 장치가 식별되고, 상기 전자 장치에 대응하는 목록에서 상기 외부 전자 장치의 정보가 식별되면, 상시 권한부여 서버에서 상기 전자 장치로 전송되는 전자 장치.

청구항 2

삭제

청구항 3

제1항에 있어서, 상기 제어부는,

상기 통신부를 이용하여 상기 외부 전자 장치를 통해 상기 고유 ID를 상기 권한부여 서버로 전송하도록 구성되는 전자 장치.

청구항 4

제1항에 있어서,

상기 각 섹션은 암호화되고,

상기 제어부는 상기 권한부여 정보에 포함된 복호화 키에 따라 해당 섹션을 복호화하는 전자 장치.

청구항 5

제1항에 있어서,

상기 요청은 상기 전자 장치의 고유 ID를 포함하는 전자 장치.

청구항 6

제1항에 있어서,

상기 요청은 상기 외부 전자 장치를 식별하는 정보 및 트랜잭션 타입 중 적어도 하나를 포함하는 전자 장치.

청구항 7

제1항에 있어서,

상기 저장부는 상기 고유 ID 및 상기 복수의 섹션들을 포함하는 아이덴티티 스토리지를 포함하고, 상기 고유 ID는 아이덴티티 스토리지 앞에 위치하고 뒤이어 상기 복수의 섹션이 위치하는 전자 장치.

청구항 8

제1항에 있어서, 각 섹션은 개별 아이덴티티 정보 및 관련 아이덴티티 정보 수집 중 적어도 하나를 포함하는 전자 장치.

청구항 9

전자 장치의 권한 부여 방법에 있어서,

근거리 통신망을 통해 외부 전자 장치로부터 트랜잭션(transaction)과 관련된 아이덴티티 정보의 요구를 수신하는 단계;

상기 아이덴티티 정보의 요구에 응답하여, 상기 전자 장치의 통신부를 이용하여 광역 통신망을 통해 상기 아이덴티티 정보의 요구에 대응하는 트랜잭션 정보, 상기 전자 장치의 식별 정보를 포함하는 요청을 권한부여 서버로 전송하는 단계;

상기 권한부여 서버로부터 권한부여 정보를 수신하는 단계; 및

상기 트랜잭션을 완료하도록, 상기 수신된 권한부여 정보에 기반하여 상기 전자 장치의 저장부에 저장되어 있는 각각 다른 카테고리의 아이덴티티 정보 중 상기 트랜잭션에 대응하는 아이덴티티 정보를 상기 외부 전자 장치에게 전송하는 단계를 포함하는 방법.

청구항 10

제9항에 있어서,

상기 권한부여 정보는 상기 아이덴티티 정보의 적어도 한 카테고리에 대한 복호화 키를 포함하고,

상기 복호화 키에 따라 상기 아이덴티티 정보의 적어도 한 카테고리를 복호화하는 단계를 포함하는 방법.

청구항 11

제9항에 있어서,

상기 요청은 상기 전자 장치의 고유 ID를 포함하는 방법.

청구항 12

제9항에 있어서,

상기 요청은 상기 외부 전자 장치를 식별하는 정보 및 트랜잭션 타입 중 적어도 하나를 포함하는 방법.

청구항 13

제9항에 있어서,

상기 아이덴티티 정보의 각 카테고리는 개별 아이덴티티 정보 및 관련 아이덴티티 정보의 수집 중 적어도 하나를 포함하는 방법.

청구항 14

권한부여 서버의 권한 부여 방법에 있어서,

전자 장치로부터 트랜잭션 정보, 및 상기 전자 장치의 식별 정보를 포함하는 요청을 수신하는 단계;

상기 전자 장치의 상기 식별 정보에 기반하여, 상기 전자 장치를 식별하는 단계;

상기 전자 장치에 대응하는 목록에서 트랜잭션과 관련된 외부 전자 장치의 정보를 식별하는 단계;

상기 외부 전자 장치가 아이덴티티 정보를 수신할 권한이 있는지를 판단하는 단계; 및

상기 판단 결과에 기반하여, 상기 전자 장치가 상기 외부 전자 장치에게 상기 전자 장치에 저장된 상기 아이덴티티 정보를 전송하도록, 상기 전자 장치로 권한부여 정보를 전송하는 단계를 포함하는 방법.

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

제14항에 있어서,

상기 요청은 상기 전자 장치의 고유 ID를 포함하는 방법.

청구항 20

제14항에 있어서,

상기 요청은 상기 외부 전자 장치를 식별하는 정보 및 트랜잭션 타입 중 적어도 하나를 포함하는 방법.

청구항 21

제20항에 있어서,

상기 요청은 상기 외부 전자 장치를 통해 상기 전자 장치로부터 수신되고, 상기 외부 전자 장치를 식별하는 정보 및 트랜잭션 타입 중 적어도 하나는 상기 외부 전자 장치에 의해 공급되는 방법.

청구항 22

제14항에 있어서,

등록요구를 수신하여 상기 전자 장치를 상기 권한부여 서버에 등록하는 단계;

상기 전자 장치를 인증하는 단계;

상기 전자 장치가 인증되면 상기 전자 장치를 등록하는 단계; 및

상기 전자 장치에 해당하는 목록을 생성 및 저장하는 단계를 포함하는 방법.

청구항 23

제22항에 있어서,

상기 목록을 변경하는 요구를 수신하는 단계;

상기 목록을 변경하기 위한 상기 요구를 인증하는 단계;

상기 목록 변경에 대한 요구가 인증되면 상기 목록 변경 요구에 따라 상기 목록을 변경하는 단계를 포함하는 방법.

청구항 24

제23항에 있어서,

상기 목록을 변경하는 단계는,

상기 외부 전자 장치를 상기 목록에 추가하는 단계;

상기 목록으로부터 상기 외부 전자 장치를 삭제하는 단계; 및

상기 외부 전자 장치와 연계된 액세스 권한을 변경하는 단계 중 적어도 하나를 포함하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 다양한 실시예들은 역권한 부여 방법 및 그 전자 장치에 관한 것이다.

배 경 기 술

[0002] 전자 장치의 일환으로 사용되는 휴대 단말기는 사용자들간 무선 통신을 제공하도록 발전하고 있다. 기술이 진보함에 따라, 휴대 단말기는 현재 단순한 전화 대화를 넘어서 많은 추가적인 특징들을 제공하고 있다. 예를 들어, 휴대 단말기들은 알람, 문자 메시지(SMS), 멀티미디어 메시지(MMS), 이메일, 게임, 근거리 통신의 원격제어, 장착된 디지털 카메라를 사용하는 이미지 촬영기능, 오디오 및 비디오 콘텐츠를 제공하는 멀티미디어 기능, 스케줄링 기능 등과 같은 추가 기능을 제공할 수 있다. 휴대 단말기들은 복수의 특징들을 제공하면서 사실상 일상생활의 필수품이 되어가고 있다.

[0003] 휴대 장치들은 아이덴티티(identity) 형태로 및 트랜잭션(transaction)을 완료하는 메커니즘으로 사용되고 있다. 예를 들어, 신용카드로 식사 대금을 지불하는 대신, 식당 고객은 휴대 장치를 제시할 수 있다. 식사 대금 지불은 휴대 장치에 디스플레이된 바코드를 스캔하는 것과 같이 휴대 장치를 사용해 이뤄질 수 있다. 유사하게 휴대 장치상의 식별 정보는 제3자와의 트랜잭션을 완료할 때 액세스될 수 있다.

[0004] 그러나 해당 휴대 장치(또는 기기들)를 가진 사용자의 아이덴티티를 연계하는 기술이 현재 개발중에 있는 반면, 종래의 이런 기술들은 대부분 사용자의 아이덴티티와 휴대 장치를 신뢰할 수 있는 방식으로 페어링(pairing)하는 것과 관련될 수 있다. 이 기술들은 이 아이덴티티 정보가 제3의 요청자들에 의해 어떻게 사용되는지와는 관련이 없다. 제3자는 주어진 트랜잭션을 완료하는데 필요할 수 있는 것보다 사용자에 대한 더 많은 정보를 얻을 수 있다. 사용자들은 자신들의 개인 식별 정보를 더 보호하려하고, 이 아이덴티티 정보에 대한 제3자의 액세스를 제한하는 메커니즘을 원할 수 있다. 따라서 휴대 장치 또는 다른 아이덴티티 장치와 같은 전자 장치에서 아이덴티티 정보에 대해 사용자가 제어하도록 하는 방법이 필요하다.

발명의 내용

해결하려는 과제

[0005] 본 발명의 다양한 실시예들은 역권한 부여 방법 및 그 전자 장치를 제공할 수 있다.

과제의 해결 수단

[0006] 본 발명의 다양한 실시예에 따르면, 사용자 아이덴티티 제어를 위한 전자 장치가 제공될 수 있다. 전자 장치는 통신부, 고유 ID 및 복수의 섹션들을 포함하고, 각 섹션은 다른 아이덴티티 정보를 포함하는 저장부, 및 트랜잭션 요구에 응답하여, 상기 통신부를 통해 아이덴티티 정보에 대한 요구를 권한부여 서버로 전송하고, 상기 권한부여 서버로부터 수신된 권한부여 정보에 응답하여 아이덴티티 정보를 제3자에게 전송하여 상기 수신된 권한부여 정보에 따라 상기 트랜잭션을 완료하는 제어부를 포함할 수 있다.

[0007] 본 발명의 다양한 실시예에 따르면, 전자 장치가 제3자와의 트랜잭션에서 아이덴티티 정보의 배포에 대한 권한을 부여하는 방법이 제공될 수 있다. 전자 장치는 트랜잭션 요구를 수신하는 단계, 상기 제3자에게 아이덴티티 정보를 전송하는 권한에 대한 요구를 권한부여 서버로 전송하는 단계, 상기 트랜잭션 정보에 응답하여 상기 권한부여 서버로부터 권한부여 정보를 수신하는 단계 및 상기 권한부여 정보가 권한부여 정보의 적어도 한 카테고리를 나타내면, 상기 아이덴티티 장치에 저장된 해당 아이덴티티 정보를 상기 제3자에게 전송하는 단계를 포함할 수 있다.

[0008] 본 발명의 다양한 실시예에 따르면, 권한부여 서버가 제3자와의 트랜잭션에서 아이덴티티 정보의 배포에 대한 권한을 부여하는 방법이 제공될 수 있다. 상기 방법은 아이덴티티 장치로부터 트랜잭션 정보를 수신하는 단계, 제3자가 아이덴티티 정보를 수신할 권한이 있는지를 판단하는 단계 및 상기 판단 결과에 따라 상기 아이덴티티 장치로 권한부여 정보를 전송하는 단계를 포함할 수 있다.

발명의 효과

[0009] 본 발명의 다양한 실시예에 따르면, 전자 장치의 사용자가 자신의 아이덴티티 정보 중 어떤 것이 어떻게 제3자들에게 배포될 것인지에 대해 더 많이 통제하게 함으로써 보안을 개선하고 원치않는 아이덴티티 정보의 배포를 제한할 수 있다.

도면의 간단한 설명

[0010] 본 발명의 예시적인 실시예들의 양상, 특징 및 장점들은 첨부된 도면을 참고한 다음의 설명으로부터 명백해질 것이다.

도 1은 본 발명의 예시적인 실시예에 따른 역권한부여 시스템을 도시한 도면이다.

도 2는 본 발명의 예시적인 실시예에 따른 역권한부여 방법에 대한 흐름도이다.

도 3은 본 발명의 예시적인 실시예에 따른 휴대 장치를 도시한 도면이다.

도 4는 본 발명의 예시적인 실시예에 따른 아이덴티티 장치에서 사용가능한 저장부를 도시한 도면이다.

도 5는 본 발명의 예시적인 실시예에 따른 화이트 리스트(white list)를 도시한 도면이다.

도면 전체에서 동일한 참고번호는 동일한 구성요소, 특징 및 구조물을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0011] 첨부된 도면을 참고한 다음의 설명은 청구범위 및 그 균등물에 의해 정의된 본 발명의 예시적인 실시예들에 대한 포괄적인 이해를 돕기 위해 제공될 수 있다. 상세한 설명은 이해를 돕기 위해 다양한 세부 사항들을 포함하지만, 이는 단지 예시적일 뿐이다. 따라서 본 발명이 속하는 기술분야의 당업자는 본 명세서에서 설명된 실시예들의 다양한 변경 및 변형이 본 발명의 범위와 기술적 사상을 벗어나지 않고 이루어질 수 있음을 인식할 것이다. 또한 명확성과 간결성을 위해 잘 알려진 기능과 구성에 대한 설명은 생략하기로 할 수 있다.

[0012] 다음의 설명과 청구범위에 사용된 용어와 단어들은 사전적인 의미에 한정되지 않으며, 단순히 본 발명에 대한 명확하고 일관성있는 이해를 위해 발명자에 의해 사용된 것이다. 따라서 본 발명의 예시적인 실시예에 대한 다음의 설명은 설명의 목적으로만 제공되며 부가된 청구범위와 그 균등물에 의해 정의된 발명을 제한할 목적으로 제공되지 않았음이 당업자에게는 명백할 것이다.

[0013] 별도로 명시되지 않았다면 단수형 표현은 복수형을 포함할 수 있다는 것이 이해되어야 할 수 있다. 따라서, 예를 들어, "하나의 구성 요소의 표면"에 대한 언급은 하나 이상의 그러한 표면들에 대한 언급을 포함할 수 있다.

[0014] 용어 "실질적으로"는 인용된 특징, 파라미터, 또는 값이 정확하게 달성될 필요는 없지만, 예를 들어, 허용치, 측정 오차, 측정 정확도 제한 및 당업자에게 알려진 다른 요소들을 포함하는 편차 또는 변이가 본 발명의 특징이 제공하려고 한 효과를 배제하지 않는 양으로 일어날 수 있다는 것을 의미할 수 있다.

[0015] 본 발명의 예시적인 실시예들은 역권한부여 방법 및 그 전자 장치를 포함할 수 있다. 본 발명의 예시적인 실시예들은 역권한 장치 및 방법을 포함할 수도 있다.

[0016] 도 1은 본 발명이 예시적인 실시예에 다른 역권한부여 시스템을 도시한 도면이다.

[0017] 도 1을 참고하면, 역권한부여 시스템은 아이덴티티 장치(100), 제3자(200) 및 권한부여 서버(300)를 포함할 수 있다. 아이덴티티 장치(100), 제3자(200) 및 권한부여 서버(300)는 동일하거나 서로 다른 네트워크를 통해 서로 통신할 수 있다. 예를 들어, 아이덴티티 장치(100)는 NFC 또는 블루투스와 같은 개인영역통신망(personal area network, PAN)을 통해 제3자(200)과 통신할 수 있는 반면, 권한부여 서버(300)는 인터넷 또는 휴대 전화망과 같은 광역 통신망(wide area network, WAN)을 통해 제3자(200) 및/또는 아이덴티티 장치(100)와 통신할 수 있다.

[0018] 아이덴티티 장치(100)는 직접 (점선으로 도시됨) 또는 제3자(200)를 통해 권한부여 서버(300)에 아이덴티티 정보를 전할 수 있다. 권한부여 서버(300)는 제3자(200)에게 아이덴티티 장치(100)에 저장된 아이덴티티 정보 중 일정 카테고리를 사용하도록 권한을 부여할 수 있다. 아이덴티티 장치(100)가 권한부여 서버(300)로부터 권한을 수신하면, 아이덴티티 장치(100)는 사용자와 제3자(200)가 트랜잭션을 완료할 수 있게 하면서 제3자(200)에게 권한이 부여된 카테고리 정보를 배포할 수 있다. 이 과정은 하기에서 도 2를 참고하며 더 자세하게 설명하기로 한다.

[0019] 본 발명의 예시적인 실시예에 따르면, 아이덴티티 장치(100)는 휴대폰, 스마트폰, 태블릿, 개인정보단말(PDA) 등과 같은 사용자의 휴대 장치일 수 있다. 그러나 아이덴티티 장치(100)는 아이덴티티 정보 및 통신 메커니즘이 저장된 아이덴티티 카드 형태일 수 있다. 아이덴티티 카드는 NFC 또는 아이덴티티 카드에 설치된 무선 주파수 식별 (RFID) 태그를 통해 제3자(200) 및 권한부여 서버(300)와 통신할 수 있다. 아이덴티티 장치(100)가 휴대 장치라면, 그 휴대 장치는 또한 NFC 및 RFID 외에 블루투스, 와이파이(Wi-Fi), 셀룰러(cellar) 등과 같은 다른 통신 기술을 통해 통신할 수 있다.

[0020] 제3자(200)는 아이덴티티 장치(100)의 사용자와 트랜잭션을 수행할 수 있다. 예를 들어, 트랜잭션은 상품 또는 서비스 판매일 수 있다. 그러나 트랜잭션은 판매에 한정될 필요는 없다. 트랜잭션은 사용자의 아이덴티티 또는 사용자에 대한 정보가 필요한 임의의 종류의 트랜잭션일 수 있다. 제3자(200)는 웹사이트 또는 다른 온라인 서

비스일 수 있고, 식당 또는 오프라인 상점(brick-and-mortar store)과 같이 물리적인 존재를 가질 수 있다.

[0021] 권한부여 서버(300)는 사용자에 의해 정의된 화이트 리스트에 따라 특별한 아이덴티티 정보 카테고리를 수신하도록(제3자(200)와 같은) 제3자들에게 권한을 부여한 공개(public) 서버일 수 있다. 보안을 높이기 위해, 권한부여 서버(300)는 제3자들에 독립적일 수 있다.

[0022] 권한부여 서버(300)는 사용자가 아이덴티티 장치를 권한부여 서버(300)에 등록하고, 각 등록된 아이덴티티 장치와 연계된 화이트 리스트를 만들도록 인터페이스를 제공할 수 있다. 권한부여 서버(300)는 저장된 화이트 리스트들을 변경하게 하는 인터페이스를 제공할 수 있다. 각 화이트 리스트는 해당 제3자들이 액세스할 권한을 부여받는 아이덴티티 정보 카테고리를 포함할 수 있다. 이 카테고리들은 은행계좌 정보(예를 들어, 계좌번호), 정부 관련 정보(사회보장번호), 금융정보(예를 들어, 모기지 정도, 이자율 등)와 같은 특별 목적에 사용되는 정보를 포함할 수 있다. 이 카테고리들은 또한 주소 정보, 나이 등과 같은 다른 종류의 개인 정보를 포함할 수 있다. 제3자(200)가 요구하는 정보 카테고리가 화이트 리스트에 존재하는 해당 카테고리와 매칭되면, 권한부여 서버(300)는 트랜젝션에 권한을 부여하고 권한부여 정보를 아이덴티티 장치(100)로 전송해, 아이덴티티 장치(100)가 아이덴티티 정보를 배포하게하여 그 트랜잭션을 완료하게 할 수 있다. 화이트 리스트는 도 5를 참고하여 하기에서 더 자세히 설명하기로 하고, 제3자(200)에게 권한을 부여하여 아이덴티티 정보를 수신하게 하는 과정은 도 2를 참고해 하기에서 설명하기로 한다.

[0023] 도 2는 본 발명의 예시적인 실시예에 따른 역권한부여 방법에 대한 흐름도이다.

[0024] 도 2를 참고하면, 210단계에서 사용자는 제3자(200)와 트랜잭션을 시작할 수 있다. 온라인상에서 이것은 사용자가 체크아웃 과정을 시작할 때 일어날 수 있지만, 사용자가 제3자 사이트 혹은 다른 곳을 처음 방문할 때와 같이 다른 포인트에서 일어날 수 있다. 유사하게, 물리적인 존재의 경우 트랜잭션은 매장에서 일어날 수 있다. 그러나, 트랜잭션의 시작은 사용자와 제3자(200)가 상호 작용하는 동안 언제라도 일어날 수 있다. 예를 들어, 210단계에서 트랜잭션의 시작은 제3자(200)가 사용자에게 아이덴티티 정보를 요구할 때 일어날 수 있다.

[0025] 220단계에서, 아이덴티티 장치(100)는 권한부여 서버(300)에 아이덴티티 정보를 전송할 수 있다. 아이덴티티 요구는, 예를 들어, 아이덴티티 장치(100)에 저장된 보안 ID, 사용자에 의해 제공된 사용자 패스워드, 및 다른 정보를 포함할 수 있다. 요구는 또한 트랜잭션 타입과 제3자(200)의 아이덴티티와 같은 트랜잭션에 대한 트랜잭션 정보를 포함할 수 있다. 도 1에 도시된 바와 같이, 정보의 전부 또는 일부가 아이덴티티 장치(100)로부터 권한부여 서버(300)로 직접 또는 제3자(200)를 통해 전송될 수 있다. 트랜잭션 정보는 제3자(200)에 의해 제공될 수 있다. 이 경우, 요구는 아이덴티티 장치(100)로부터 제3자(200)에게 전송될 수 있고, 제3자(200)는 트랜잭션 정보를 요구에 조합하고 그 요구를 권한부여 서버(300)로 전달할 수 있다. 예를 들어, 사용자가 와인 한 병을 구입할 수 있다면, 그 정보는 그 구입이 술 음료 구입임을 나타낸 것을 포함할 수 있다.

[0026] 230단계에서 권한부여 서버(300)는 보안 ID 및/또는 패스워드와 같은 수신된 정보에 따라 아이덴티티 장치(100)를 인증할 수 있다. 아이덴티티 장치(100)가 확인되면, 권한부여 서버(300)는 240단계에서 아이덴티티 장치(100)에 대응하는 화이트 리스트에서 제3자(200)를 찾고 제3자(200)가 화이트 리스트에 존재하는지를 판단할 수 있다.

[0027] 제3자(200)가 화이트 리스트에 존재하지 않는다면, 권한부여 서버(300)는 270단계에서 트랜잭션을 부정할 수 있다. 권한부여 서버(300)는 아이덴티티 장치(100) 및 제3자(200) 중 하나 또는 둘 다에 대한 거부를 전송할 수 있다. 또한 권한부여 서버(300)는 '화이트 리스트에 존재하지 않는 제3자'와 같은 거부 이유에 대한 정보를 전송할 수 있다. 이는 사용자에게 제3자(200)를 화이트리스트에 추가하여 트랜잭션을 다시 시도할 기회를 제공할 수 있다.

[0028] 제3자(200)가 화이트 리스트에 존재한다면, 권한부여 서버(300)는 250단계에서 화이트 리스트를 분석하여 제3자(200)와의 트랜잭션이 허가될 수 있는지를 판단할 수 있다. 제3자(200)가 허가되었는지에 대한 판단은 트랜잭션 타입에 따라 좌우될 수 있다. 예를 들어, 와인 구입의 경우, 화이트 리스트 정보는 제3자(200)가 와인을 구입할 권한이 없다는 것을 나타낼 수 있다.

[0029] 제3자(200)가 트랜잭션에 대한 권한이 없다면, 권한부여 서버(300)는 270단계에서 상술한 바와 같이 그 트랜잭션을 거부할 수 있다. 권한부여 서버(300)가 거부 이유에 대한 정보를 전송하면, 권한부여 서버(300)는 이 경우 제3자(200)가 특별한 트랜잭션에 대해 권한이 없음을 나타내는 정보를 전송할 수 있다. 와인 구입의 경우, 예를 들어, 제3자(200)가 술 구입 권한이 없다면, 권한부여 서버(300)는 '제3자는 술 구입에 대한 권한이 없다'와 같

은 정보를 전송할 수 있다. 그런 다음, 상술한 바와 같이 사용자는 화이트 리스트를 갱신하여 제3자(200)로부터의 술 구입을 허가하고 트랜잭션을 다시 시도하게 할 수 있다.

[0030] 제3자(200)는 트랜잭션에 대한 권한이 부여되면, 권한부여 서버(300)는 260단계에서 트랜잭션을 허가하고 아이덴티티 장치(100)에 정보를 전송하여 아이덴티티 장치(100)가 제3자(200)에 아이덴티티 정보를 배포하여 트랜잭션을 완료할 수 있게 할 수 있다. 예를 들어, 권한부여 서버(300)는 권한이 부여된 아이덴티티 정보를 포함하는 아이덴티티 장치(100)에 저장된 해당 정보에 대한 복호화키(decryption key)를 전송할 수 있다. 와인 구입의 경우, 권한이 부여된 아이덴티티 정보는 나이 정보뿐만 아니라 신용카드 정보를 포함해 사용자가 술을 구입할 합법적 나이인지를 확인할 수 있다.

[0031] 권한부여 서버(300)의 관점에서 트랜잭션이 허가될 수 있다면(즉, 권한부여 서버(300)는 제3자(200)가 어떤 아이덴티티 정보 카테고리에 액세스하도록 권한이 부여된 것으로 판단할 수 있다.), 허가된 아이덴티티 정보가 제3자(200)의 트랜잭션 승인에 불충분하다면 그 트랜잭션은 여전히 실패할 수 있다. 예를 들어, 권한부여 서버(300)는 제3자(200)가 신용카드 정보를 수신할 권한은 갖지만, 수신할 권한이 없는 주소 정보도 또한 요구했던 것으로 판단할 수 있다. 이 경우, 사용자는 화이트 리스트를 갱신하고 트랜잭션을 다시 시도할 수 있다(예를 들어, 화이트 리스트를 갱신하여 제3자(200)가 주소 정보를 수신하게 할 수 있다.).

[0032] 아이덴티티 정보에 대한 다중 요구가 사용자와 제3자간 동일한 트랜잭션 내에서 이뤄질 수 있다. 예를 들어, 제3자(200)가 배관공이라면, 그 배관공은 먼저 주소 정보를 요구할 수 있고, 그런 다음 나중에 (작업이 완료됐을 때) 신용카드 정보를 요구할 수 있다.

[0033] 상술한 바와 같이, 화이트 리스트는 사용자에게 사용자의 아이덴티티 정보에 대한 더 많은 통제를 허가할 수 있다. 예를 들어, 사용자는 어떤 제3자들이 신용카드 정보를 수신하고 트랜잭션을 처리하게 할 수 있지만 주소정보나 전화번호 정보는 허가하지 않을 수 있다. 온라인 소매상 또는 서비스 제공자들(배관공, 전기기사, 청부업자 등)과 같은 다른 제3자들은 (예를 들어, 배달이나 약속을 하기 위해) 주소 정보를 수신하도록 허가될 수 있다.

[0034] 도 3은 본 발명의 예시적인 실시예들에 따른 아이덴티티 장치를 도시한 도면이다.

[0035] 도 3을 참고하면, 아이덴티티 장치(100)는 저장부(110), 제어부(120) 및 통신부(130)를 포함할 수 있다. 도 1과 관련해 상술한 바와 같이, 아이덴티티 장치(100)는 아이덴티티 카드이고, 제어부(120) 및 통신부(130)의 기능은 하나의 구성요소로 통합될 수 있다.

[0036] 아이덴티티 장치(100)는 또한 도시되지 않은 추가 구성요소들을 포함할 수 있다. 이 추가 구성요소들은 휴대 장치의 추가 기능들에 따라 달라질 수 있다. 예를 들어, 휴대 장치(100)는 디스플레이부, 입력부, 카메라, 위치부 등을 포함할 수 있다.

[0037] 제어부(120)는 아이덴티티 장치(100)의 전체적인 동작을 제어할 수 있다. 특히 제어부(120)는 통신부가 권한부여를 위해 아이덴티티 정보를 권한부여 서버(300)로 전송하도록 제어할 수 있다. 아이덴티티 정보를 제3자에 배포하도록 권한을 부여받으면, 제어부(120)는 저장부(110)로부터 적절한 아이덴티티 정보를 검색하고 통신부(130)가 그 아이덴티티 정보는 제3자에게 전송해 트랜잭션을 완료(또는 시작)하도록 제어할 수 있다. 아이덴티티 정보가 암호화되면, 제어부(120)는 이동 기기에 저장되거나 권한부여 서버(300)로부터 수신된 복호화 키를 사용하여 아이덴티티 정보를 복호화할 수 있다.

[0038] 통신부(130)는 제어부(120)의 제어하에서, 예를 들어, 제3자(200) 및 권한부여 서버(300)를 포함한 다른 기기들과 통신할 수 있다. 통신부(130)는 다양한 프로토콜 및 방법 중 어느 것에 따라 (제3자(200) 및 권한부여 서버(300)를 포함한) 다른 기기들과 통신할 수 있다. 예를 들어, 통신부(130)는 NFC 또는 다른 근거리 통신 방법을 통해 통신할 수 있다. 그러나 통신부(130)는 이 프로토콜들에 한정되지 않고 장치의 설계에 따라 다른 프로토콜들을 사용할 수 있다.

[0039] 저장부(110)는 아이덴티티 정보를 저장할 수 있다. 아이덴티티 정보는 사용자에 의해 정의된 다양한 카테고리의 아이덴티티 정보뿐만 아니라 고유 ID를 포함할 수 있다. 저장부(110)의 예는 도 4를 참고하여 하기에서 설명하기로 할 수 있다.

[0040] 도 4는 본 발명의 예시적인 실시예에 다른 아이덴티티 장치에서 사용가능한 저장부를 도시한 도면이다.

[0041] 도 4를 참고하면, 저장부(110)는 고유 ID 및 섹션 1 내지 섹션 N을 포함할 수 있다. 고유 ID는 저장부(110)의 첫 M개 바이트에 저장될 수 있다. 그러나, 고유 ID는 저장부(110)의 다른 위치에 저장될 수 있음이 이해되어야 할 수 있다. 고유 ID는 서명된(signed) 고유 ID일 수 있다.

[0042] 섹션 1 내지 섹션 N의 각각은 다른 카테고리의 아이덴티티 정보를 포함할 수 있다. 카테고리들은 주소 정보, 전화번호 정보, 이메일 주소, 개인 정보(예를 들어, 나이, 키, 성별 등), 및 다른 종류의 정보와 같은 개인의 아이덴티티 정보를 포함할 수 있다. 그 카테고리들은 (신용카드 번호, 계좌 번호, 송금번호와 같은) 은행계좌 관련 정보, (사회 보장 번호, 납세자 번호와 같은) 정부 정보, (이름, 나이, 체중과 같은) 개인 정보, 및 다른 관련 아이덴티티 정보 수집과 같은 아이덴티티 정보의 수집을 포함할 수 있다. 카테고리들은 사용자에 의해 정의되거나 개발자 또는 제조업자에 의해 미리 설정될 수 있다.

[0043] 섹션 1 내지 섹션 N은 개별적으로 추가 보안을 위해 암호화될 수 있다. 이 경우, 각 섹션은 연계된 공개 키 또는 다른 암호화 키를 가질 수 있다. 복호화 키는 해당 섹션의 비암호화 부분에 저장되거나 저장부(도시되지 않음)의 다른 영역에 저장될 수 있다. 또는 복호화 키는 권한부여 서버(300)에 의해 보유되어 트랜잭션에 대한 권한 부여시 휴대 장치로 전송될 수 있다.

[0044] 사용자는 권한부여 서버(300)에 의해 저장된 화이트 리스트를 통해 저장부(110)에 저장된 아이덴티티 정보에 대한 액세스를 제어할 수 있다. 화이트 리스트의 예는 도 5를 참고하여 아래에서 설명하기로 할 수 있다.

[0045] 도 5는 본 발명의 예시적인 실시예에 다른 화이트 리스트를 도시한 도면이다.

[0046] 도 5를 참고하면, 화이트 리스트는 회사들(이 예에서 회사 1 내지 회사 X)의 리스트 및 해당 액세스 권한을 포함할 수 있다. 화이트 리스트가 회사들에 관해 도 5의 예에 설명되어 있지만, 화이트 리스트는 사용자가 아이덴티티 정보를 제공하기를 원하는 임의의 제3자에 대한 액세스 권한을 포함할 수 있음이 이해되어야 한다. 권한부여 서버(300)는 복수의 화이트 리스트들을 저장하고, 각 아이덴티티 장치(100)에 대해 하나가 권한부여 서버(300)에 등록될 수 있다. 권한 부여 서버(300)는 다양한 포맷 중 하나로 화이트 리스트를 저장할 수 있다.

[0047] 각 액세스 권한은 해당 회사가 수신 권한을 갖는 아이덴티티 정보 카테고리 리스트를 포함할 수 있다. 아이덴티티 정보 이외에, 액세스 권한은 또한 트랜잭션 타입을 포함할 수 있다. 트랜잭션 타입은 특별한 구입이 허가되거나 되지 않음을 나타낼 수 있다. 예를 들어, 도 2를 참고해 설명한 와인 구입 예를 다시 참고하면, 액세스 권한은 특별한 제3자가 와인 구입에 대한 권한이 없다는 것을 특정할 수 있다. (다른 카테고리뿐만 아니라) 이 트랜잭션 타입들은 사용자에 의해 정의될 수 있다. 제조업자들 및/또는 개발자들 또한 디폴트 트랜잭션 또는 미리 정의된 트랜잭션 타입을 제공할 수 있다.

[0048] 회사와 관련된 특별한 액세스 권한이 사용자의 정의에 따라 달라질 수 있다. 예를 들어, 식당이 (사용자가 술을 구입할 수 있는 충분한 나이임을 확인하기 위해) 사용자의 나이 및 (식사 대금 지불을 처리하기 위해) 사용자의 신용카드 정보와 관련된 아이덴티티 정보에 액세스하도록 유일하게 권한이 주어졌을 수 있다. 배관공은 (배관공이 사용자의 집을 찾을 수 있도록) 주소 정보뿐만 아니라 (지불을 처리하기 위한) 사용자의 신용카드 정보를 수신하도록 권한이 주어졌을 수 있다. 온라인 상점은 사용자의 신용카드 정보 및 (적절한 배달을 보증하기 위한) 주소정보에 대한 권한이 주어졌을 수 있다. 따라서, 특별한 회사와 관련된 정보는 사용자가 얼마나 많은 정보를 제공하고자 하는가에 따라 달라질 수 있다. 유사하게, 주어진 제3자는 특별한 트랜잭션 타입에 기초해 어떤 정보 카테고리를 수신하도록 허가될 수 있다.

[0049] 또한 액세스 권한은 회사가 액세스하도록 허가된 아이덴티티 정보를 포함하는 저장부의 해당 섹션들에 대한 복호화 키 정보를 포함할 수 있다. 이 정보는 복호화 키 자체를 포함할 수 있다. 복호화 키가 다른 곳에 저장될 수 있다면, 화이트 리스트는 복호화 키의 위치에 대한 포인터 또는 다른 참고를 포함할 수 있다.

[0050] 도 2와 관련한 상술한 설명에서, 권한부여 서버(300)는 화이트 리스트를 참고해 제3자가 (있다면) 어느 아이덴티티 정보를 수신하도록 허가할 것인가를 판단할 수 있다. 권한부여 서버(300)는 화이트 리스트에 포함된 정보에 따라 권한을 전송할 수 있다.

[0051] 화이트 리스트에 저장된 특별한 회사 및 해당 액세스 권한은 사용자에 의해 정의될 수 있다. 권한부여 서버(300)는 사용자가 제3자들을 화이트 리스트에 추가, 화이트 리스트로부터 제3자들을 삭제, 또는 특별한 제3자들과 연계된 액세스 권한을 수정하게 하는 인터페이스를 제공할 수 있다. 이 인터페이스는 아이덴티티 장치(100)

를 요구하거나 (예를 들어, 사용자가 화이트 리스트를 편집하게 하는 권한은 아이덴티티 장치(100)에 포함된 고유 ID와 같은 정보를 필요로 할 수 있다), 별도의 인증 절차를 가질 수 있다.

[0052] 권한부여 서버(300)는 또한 사용자가 아이덴티티 장치(100)를 권한부여 서버(300)에 등록하게 하는 인터페이스를 제공할 수 있다. 한번 등록되면, 권한부여 서버(300)는 또한 사용자가 화이트 리스트를 변경하거나 수정하게 하는 인터페이스를 제공할 수 있다. 그러한 변경은 제3자가 수신하도록 허가된 아이덴티티 정보 카테고리를 변경하는 것뿐만 아니라 리스트에 포함된 제3자들의 추가 또는 삭제를 포함할 수 있다.

[0053] 본 발명의 청구항 및/또는 명세서에 기재된 실시 예들에 따른 방법들은 하드웨어, 소프트웨어, 또는 하드웨어와 소프트웨어의 조합의 형태로 구현될(implemented) 수 있다.

[0054] 소프트웨어로 구현하는 경우, 하나 이상의 프로그램(소프트웨어 모듈)을 저장하는 컴퓨터 판독 가능 저장 매체가 제공될 수 있다. 컴퓨터 판독 가능 저장 매체에 저장되는 하나 이상의 프로그램은, 전자 장치(device) 내의 하나 이상의 프로세서에 의해 실행 가능하도록 구성된다(configured for execution). 하나 이상의 프로그램은, 전자 장치로 하여금, 본 발명의 청구항 및/또는 명세서에 기재된 실시 예들에 따른 방법들을 실행하게 하는 명령어(instructions)를 포함한다.

[0055] 이러한 프로그램(소프트웨어 모듈, 소프트웨어)은 랜덤 액세스 메모리 (random access memory), 플래시(flash) 메모리를 포함하는 불휘발성(non-volatile) 메모리, 롬(ROM, Read Only Memory), 전기적 삭제가능 프로그램가능 롬(EEPROM, Electrically Erasable Programmable Read Only Memory), 자기 디스크 저장 장치(magnetic disc storage device), 컴팩트 디스크 롬(CD-ROM, Compact Disc-ROM), 디지털 다목적 디스크(DVDs, Digital Versatile Discs) 또는 다른 형태의 광학 저장 장치, 마그네틱 카세트(magnetic cassette)에 저장될 수 있다. 또는, 이들의 일부 또는 전부의 조합으로 구성된 메모리에 저장될 수 있다. 또한, 각각의 구성 메모리는 다수개 포함될 수도 있다.

[0056] 또한, 전자 장치에 인터넷(Internet), 인트라넷(Intranet), LAN(Local Area Network), WLAN(Wide LAN), 또는 SAN(Storage Area Network)과 같은 통신 네트워크, 또는 이들의 조합으로 구성된 통신 네트워크를 통하여 접근(access)할 수 있는 부착 가능한(attachable) 저장 장치(storage device)에 저장될 수 있다. 이러한 저장 장치는 외부 포트를 통하여 전자 장치에 접속할 수 있다.

[0057] 또한, 통신 네트워크상의 별도의 저장장치가 휴대용 전자 장치에 접속할 수도 있다.

[0058] 본 발명은 예시적인 실시예를 참고하여 도시되고 설명되었으며, 형태와 세부사항들의 다양한 변화가 첨부된 청구범위와 그 균등물에 의해 정의된 바와 같이 본 발명의 사상과 범위를 벗어나지 않고 그 안에서 이루어질 수 있음을 당업자는 이해해야 할 것이다.

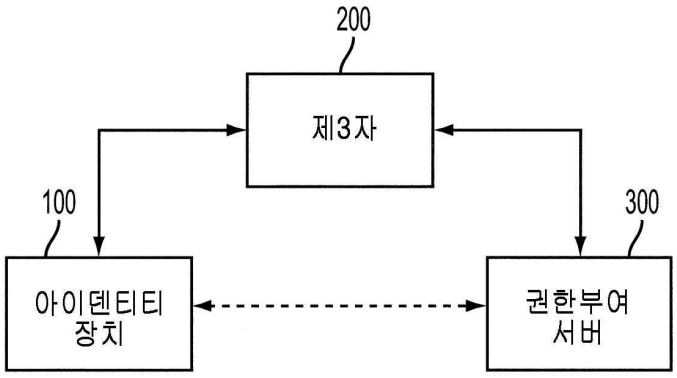
부호의 설명

[0059] 100: 아이덴티티 장치 200: 제3자

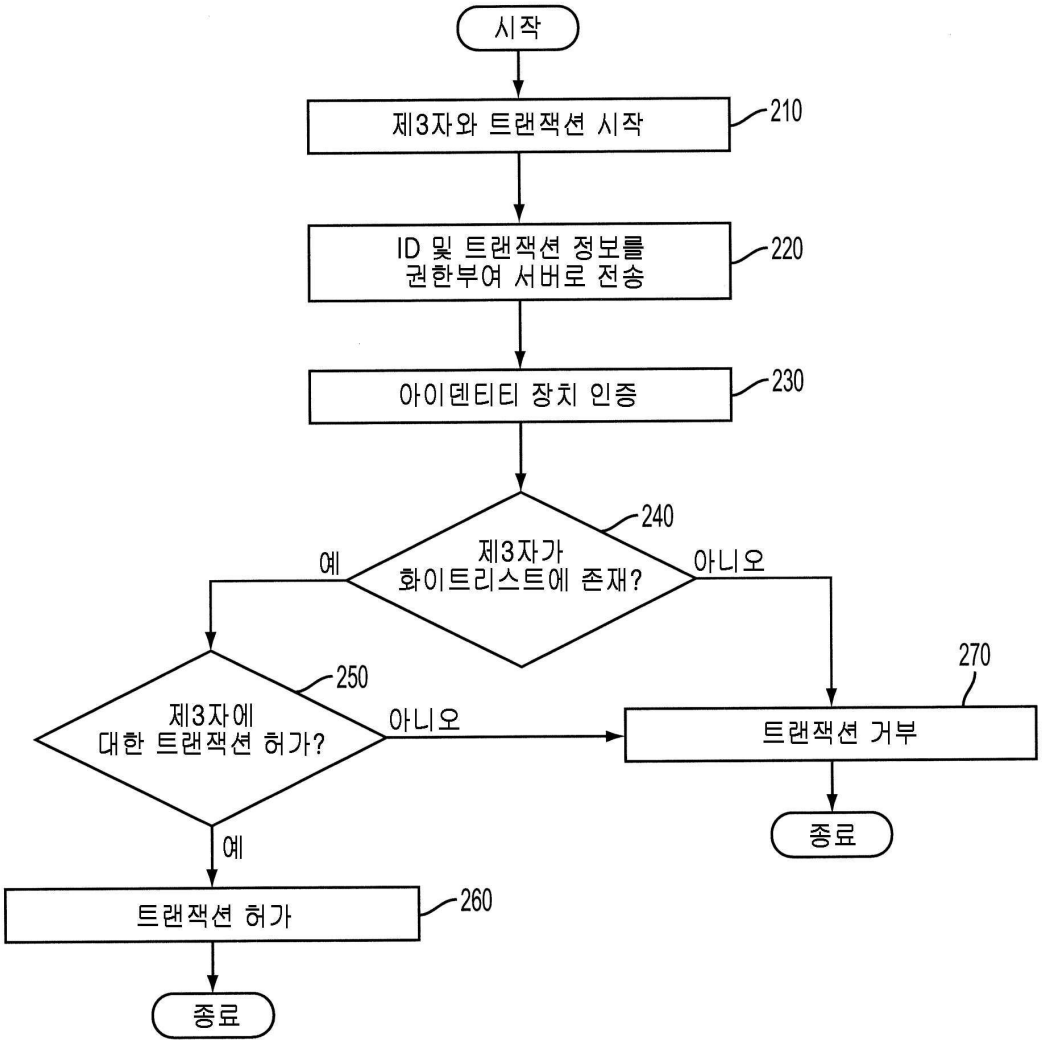
300: 권한부여 서버

도면

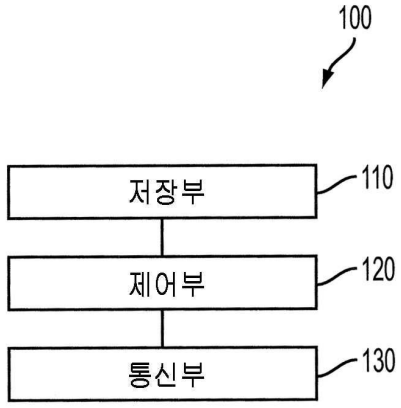
도면1


200
제3자
100
300
아이덴티티 장치
권한부여 서버

도면2


시작
제3자와 트랜잭션 시작
210
ID 및 트랜잭션 정보를 권한부여 서버로 전송
220
아이덴티티 장치 인증
230
240
제3자가 화이트리스트에 존재?
예
아니오
250
제3자에 대한 트랜잭션 허가?
아니오
270
트랜잭션 거부
종료
예
트랜잭션 허가
260
종료

도면3



도면4

도면5

회사 1	액세스 정보
회사 2	액세스 정보
⋮	⋮
회사 X	액세스 정보