(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년05월25일
(11) 등록번호 10-2402558
(24) 등록일자 2022년05월23일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 21/31* (2013.01)
H04L 9/08 (2006.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
H04L 9/3234 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2021-0050963
(22) 출원일자 2021년04월20일
심사청구일자 2021년04월20일
(56) 선행기술조사문헌
KR101711697 B1*
KR1020060105941 A*
KR1020210017432 A*
JP2006344013 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
권오경
경기도 고양시 일산동구 일산로286번길 48-5 (마두동)
(72) 발명자
권오경
경기도 고양시 일산동구 일산로286번길 48-5 (마두동)
(74) 대리인
성원찬

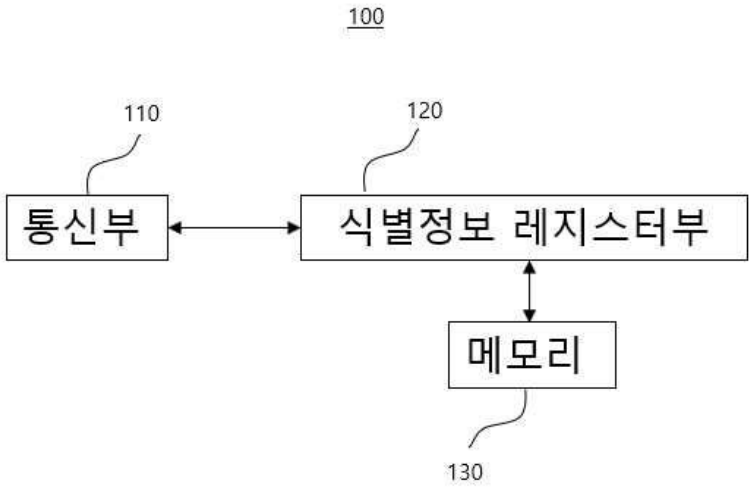
전체 청구항 수 : 총 3 항 심사관 : 나용수

(54) 발명의 명칭 **신원인증 단말장치**

(57) 요 약

신원인증 단말장치가 개시된다. 신원인증 단말장치는, 외부 장치와 통신을 수행하기 위한 통신부, 신원인증 단말장치의 식별정보를 포함하며 슬라이딩 동작이 가능한 기기 식별정보 레지스터부 및 사용자 정보를 포함하는 메모리를 포함하며, 식별정보 레지스터부는, 스위칭 동작을 통해 메모리 및 통신부의 전기적 연결을 제어한다. 이에 따라, 사용자가 물리적 버튼을 스위칭시키면서 사용자 정보 또는 암호화된 사용자 정보를 신원인증 단말장치의 식별 정보에 부가할지 여부를 선택하여 서로 다른 신원인증정보를 제공할 수 있다.

대 표 도 - 도2a



(52) CPC특허분류
H04L 63/0876 (2013.01)
H04L 9/0866 (2013.01)
H04L 9/3226 (2013.01)

명 세 서

청구범위

청구항 1

신원인증 단말장치에 있어서,

외부 장치와 통신을 수행하기 위한 통신부;

상기 신원인증 단말장치의 식별정보를 포함하며 스위칭 동작이 가능한 식별정보 레지스터부;

사용자 정보를 포함하는 메모리; 및

상기 사용자 정보를 암호화하기 위한 암호화부;를 포함하며,

상기 식별정보 레지스터부는,

상기 스위칭 동작을 통해 상기 메모리 및 통신부의 전기적 연결을 제어하며, 상기 스위칭 동작에 따라 서로 다른 신원인증정보를 상기 통신부를 통해 전송하고, 상기 스위칭 동작을 통해 상기 메모리 및 암호화부와 상기 통신부를 연결하며,

상기 식별정보 레지스터부가 상기 스위칭 동작에 따라 제1 위치에 위치하면, 상기 신원인증 단말장치의 식별번호에 기반한 제1 신원인증정보를 상기 통신부를 통해 전송하고,

상기 식별정보 레지스터부가 상기 스위칭 동작에 따라 제2 위치에 위치하면, 상기 식별정보 레지스터부, 메모리 및 통신부가 연결되며, 상기 신원인증 단말장치의 식별정보 및 사용자 정보를 포함하는 제2 신원인증정보를 상기 통신부를 통해 전송하며,

상기 식별정보 레지스터부가 상기 스위칭 동작에 따라 제3 위치에 위치하면, 상기 식별정보 레지스터부, 메모리, 암호화부 및 통신부가 연결되며, 상기 신원인증 단말장치의 식별정보 및 암호화된 사용자 정보를 포함하는 제3 신원인증정보를 상기 통신부를 통해 전송하는 것인, 신원인증 단말장치.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

제1항에 있어서,

상기 식별정보 레지스터부는,

상기 제1 신원인증정보를 상기 통신부를 통해 서버로 전송하여 상기 신원인증 단말장치의 활성화를 요청하는 것인, 신원인증 단말장치.

청구항 8

제7항에 있어서,

상기 사용자 정보는,

사용자의 생체인식정보, 금융 정보, 결제 관련 정보 중 적어도 하나를 포함하는 것인, 신원인증 단말장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 신원인증 단말 장치에 관한 것으로서, 보다 상세하게는 자기주권신원(SSI, Self-Sovereign Identity) 인증을 위한 신원인증 장치에 관한 것이다.

배 경 기 술

[0002] 기존에 신원을 인증하기 위한 기술에는 식별번호 레지스터를 활용한 인증, 종단간 암호화 인증, 공개키 기반 구조 방식의 인증 등이 사용되고 있다.

[0003] 기존의 신원인증 기술은 디지털 취약 계층이 접근하기에 장벽이 높고, 중재 기관이 암호화를 하거나 공개키를 발급 및 관리함으로써 중재기관이 개개인의 신원인증정보를 독점하고 있는 문제가 있다. 특히, 이러한 중재기관이 존재하는 경우, 개인의 권한을 검증하는 중재기관의 신뢰성에 의존해야 하는 단점이 있다.

[0004] 이에 따라, 국가나 은행 등의 초법적인 권한을 가진 중재기관이 존재하지 않는 것을 목표로 탈중앙 신원(DID, Decentralized Identifiers) 기술이 등장하고 있으나, 허위 계정 제지 불가, 물리적 인증 주체 부재, 보안 사고 시 책임 소재가 불분명하다는 한계가 있다.

[0005] 이에 따라, 하드웨어 기반의 고유번호를 활용하여 허위신원 여부를 판별하면서, 사용자가 하드웨어 기반의 고유번호와 사용자 정보를 선택적으로 결합하여 상황에 따라 신원인증정보의 보안성을 선택하여 제공할 수 있게 하는 요구가 증대되었다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 목적은 물리적 버튼을 활용하여 신원인증정보의 종류를 선택 가능한 신원인증장치를 제공함에 있다.

과제의 해결 수단

[0007] 이러한 목적을 달성하기 위한 본 발명의 일 실시 예에 따른 신원인증 단말장치는, 외부 장치와 통신을 수행하기 위한 통신부, 상기 신원인증 단말장치의 식별정보를 포함하며 슬라이딩 동작이 가능한 식별정보 레지스터부 및 사용자 정보를 포함하는 메모리를 포함하며, 상기 식별번호 레지스터부는, 상기 스위칭 동작을 통해 상기 메모리 및 통신부의 전기적 연결을 제어할 수 있다.

[0008] 또한, 본 발명의 일 실시 예에 따른 신원인증 단말장치는, 상기 사용자 정보를 암호화하기 위한 암호화부를 더 포함하며, 상기 식별정보 레지스터부는 상기 스위칭 동작을 통해 상기 메모리 및 암호화부와 상기 통신부를 연결할 수 있다.

[0009] 또한, 상기 식별정보 레지스터부는, 상기 스위칭 동작에 따라 서로 다른 신원인증정보를 상기 통신부를 통해 전송할 수 있다.

[0010] 또한, 상기 식별정보 레지스터부가 상기 스위칭 동작에 따라 제1 위치에 위치하면, 상기 식별정보 레지스터부는, 상기 신원인증 단말장치의 식별번호에 기반한 제1 신원인증정보를 상기 통신부를 통해 전송할 수 있다.

[0011] 또한, 상기 식별정보 레지스터부가 상기 스위칭 동작에 따라 제2 위치에 위치하면, 상기 식별정보 레지스터부, 메모리 및 통신부가 연결되며, 상기 식별정보 레지스터부는, 상기 신원인증 단말장치의 식별정보 및 사용자 정보를 포함하는 제2 신원인증정보를 상기 통신부를 통해 전송할 수 있다.

[0012] 또한, 상기 식별정보 레지스터부가 상기 스위칭 동작에 따라 제3 위치에 위치하면, 상기 식별정보 레지스터부, 메모리, 암호화부 및 통신부가 연결되며, 상기 식별정보 레지스터부는, 상기 신원인증 단말장치의 식별정보 및 암호화된 사용자 정보를 포함하는 제3 신원인증정보를 상기 통신부를 통해 전송할 수 있다.

[0013] 또한, 상기 식별정보 레지스터부는, 상기 제1 신원인증정보를 상기 통신부를 통해 서버로 전송하여 상기 신원인증 단말장치의 활성화를 요청할 수 있다.

[0014] 또한, 상기 사용자 정보는, 사용자의 생체인식정보, 금융 정보, 결제 관련 정보 중 적어도 하나를 포함할 수 있다.

발명의 효과

[0015] 이상과 같은 본 발명의 다양한 실시 예에 따르면, 사용자가 물리적 버튼을 스위칭시키면서 사용자 정보 또는 암호화된 사용자 정보를 신원인증 단말장치의 식별 정보에 부가할지 여부를 선택하여 서로 다른 신원인증정보를 제공할 수 있다.

도면의 간단한 설명

[0016] 도 1은 종래 기술을 설명하기 위한 도면이다.

도 2a는 본 발명의 일 실시 예에 따른 신원인증 단말장치의 구성을 도시한 블럭도이다.

도 2b는 본 발명의 다른 실시 예에 따른 신원인증 단말장치의 구성을 도시한 블록도이다.

도 3a는 본 발명의 일 실시 예에 따른 신원인증 단말장치의 식별정보 레지스터부의 스위칭 동작에 따라 서로 다른 신원인증정보를 선택하는 구성에 대한 도면이다.

도 3b는 본 발명의 다른 실시 예에 따른 신원인증 단말장치의 식별정보 레지스터부의 스위칭 동작에 따라 서로 다른 신원인증정보를 선택하는 구성에 대한 도면이다.

도 4는 본 발명의 일 실시 예에 따른 신원인증정보의 데이터 구성을 도시한 도면이다.

도 5는 본 발명의 일 실시 예에 따른 신원인증 단말장치와 외부 장치들간의 데이터 전송 과정을 설명하기 위한 도면이다.

도 6은 본 발명의 다른 실시 예에 따른 신원인증 단말장치와 외부 장치들간의 데이터 전송 과정을 설명하기 위한 도면이다.

도 7은 본 발명의 일 실시 예에 따른 메쉬 네트워크와 복수의 신원인증 단말장치 간의 관계를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하에서는 도면을 참조하여 본 발명을 더욱 상세하게 설명한다. 그리고, 본 발명을 설명함에 있어서, 관련된 공지기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단된 경우 그 상세한 설명은 생략한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관계 등에 따라 달라질 수 있다. 그러므로, 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0018] 도 1은 종래 기술을 설명하기 위한 도면이다.

[0019] 도 1을 참조하면, 종래에는 등록기관(RA, Registration Authorities) 및 인증기관(CA, Certification Authority)이라는 개념을 도입하여 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하기 위한 복합적인 보안 시스템 환경을 구축하였다.

[0020] 구체적으로, 암호화와 복호화키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 시스템이며, 이를 위해 인증기관 및 등록기관이 필요하다.

[0021] 이러한 인증기관 및 등록기관이 도입된 보안 시스템 환경은 중앙서버(10)를 대상으로 사용자 개개인이 직접 사용자 정보를 등록하고, 등록된 사용자 정보에 대한 검증이 중앙서버(10)에 의해 완료되면, 이에 관한 디지털 인증서를 발급받아 필요한 기관에 인증서를 등록하여 사용한다.

[0022] 그러나, 이러한 경우 중앙서버(10)에 대한 해킹이 이루어질 경우 대량의 개인 정보가 제3자에 의해 탈취될 수

있고, 이러한 과정에서 사용자 개개인은 아무런 조취를 취할 수 없다는 문제점이 항상 존재한다.

[0023] 이에 따라, 등록 및 인증을 관리하는 중앙서버(10)의 존재를 없애고, 사용자 개개인이 각각 자기의 신원인증정보를 관리할 수 있도록 하는 필요성이 크게 대두되었으며, 이러한 필요성에 대응하여 등장한 기술이 바로 탈중앙 신원(DID, Decentralized Identifiers) 개념이다.

[0024] 이러한 탈중앙 신원과 관련하여 함께 언급되는 개념이 자기주권신원(SSI, Self Sovereign Identity)이 있으며, 개인의 정보는 개인 스스로 통제하고 제어할 수 있으며, 기존의 IP 제공 역할을 자처하는 IT 대기업과 같은 제3자의 중재나 개입없이도 신뢰 네트워크 기반에서 충분히 높은 보안성을 유지하면서, 독립적인 일회성 채널을 통해 서비스에 필요한 신원 정보만을 선택적으로 제출할 수 있고, 제출된 정보에 대한 신뢰성 역시 제 3자 개입 없이도 증명할 수 있는 시스템을 의미한다.

[0025] 상술한 중앙서버(10)에 의한 인증 및 등록의 경우, 서비스 제공자가 모든 개인 데이터를 직접 소유 및 사용하는 방법으로서, 사용자는 ID/Password 기반의 인증 정보를 입력하여 회원가입 및 로그인함으로써 해당 서비스의 이용이 가능하게 한다.

[0026] 또한, 서비스 제공자가 데이터를 직접 소유하는 대신 구글, 페이스북 등과 같은 IP 제공업체들이 개인 정보를 보유하고 서비스 제공자는 이러한 IP 제공업체를 통해 사용자가 허용한 개인정보에 한해서 엑세스가 가능한 연합 방식의 인증 시스템도 있다.

[0027] 그러나, 이러한 중앙서버(10)에 의한 인증 및 등록 방식은 이미 설명한 바와 같이, 보안적인 리스크가 존재하고 사용자의 편의성이 떨어진다는 문제점이 있다.

[0028] 이에 비해, 자기주권신원 기술의 경우 분산원장 기법을 사용하는 신뢰 기반의 네트워크 상에서 사용자와 서비스 제공자는 중재자나 중앙서버(10) 등과 같은 제어 기관의 개입없이 사용자 각자가 본인의 데이터를 소유하고 관리하는 시스템이며, 서비스를 요청하거나 서비스 제공이 필요할 때만 일회성 P2P 통신으로 데이터를 교환하게 되어, 사용자가 직접 본인의 신원인증정보를 관리하고 보안이슈가 줄어든다는 점에서 장점이 있다.

[0029] 한편, 이러한 자기주권신원 기술과 관련하여, 사용자가 서비스에 필요한 신원 정보만을 선택적으로 제출하도록 하도록 하면서 사용자 편의성을 고려한 신원인증 단말장치에 대한 필요성이 증대되었으며, 이러한 신원인증 단말장치에 대해 본 명세서를 통해 설명하기로 한다.

[0030] 도 2a는 본 발명의 일 실시 예에 따른 신원인증 단말장치의 구성을 도시한 블럭도이다.

[0031] 도 2a를 참조하면, 본 발명의 일 실시 예에 따른 신원인증 단말장치(100)는 통신부(110), 식별정보 레지스터부(120) 및 메모리(130) 를 포함한다.

[0032] 여기서, 신원인증 단말장치(100)는 전자신분증과 같은 카드 형태로 구현될 수도 있고, USB나 OTP 등과 같은 별도의 메모리 장치로 구현될 수도 있으며, 형태와 상관없이 통신 모듈 및 슬라이딩 기능이 가능한 버튼이 구비되도록 구현된다.

[0033] 통신부(110)는 서버, 노드, 사용자 단말장치 등과 같은 외부 장치와 통신을 수행할 수 있다. 여기서, 통신부(110)는 외부 장치와 통신을 수행할 수 있으며, BT(BlueTooth), WI-FI(Wireless Fidelity), Zigbee, IR(Infrared), Serial Interface, USB(Universal Serial Bus), NFC(Near Field Communication) 등과 같은 다양한 통신 방식을 통해 외부 장치와 통신을 수행할 수 있다.

[0034] 또한, 식별정보 레지스터부(120)는 신원인증 단말장치(100)의 식별정보를 포함하며 스위칭 동작이 가능하다. 여기서, 스위칭 동작은 사용자 터치 조작에 따라 상이한 기능을 구현하는 물리적 버튼, 사용자 조작에 따라 기능이 상이하게 변경되도록 하는 토글이나 휠 형태의 버튼 또는 사용자 조작에 따라 식별정보 레지스터부(120)의 위치가 변경되면서 상이한 기능을 구현하도록 슬라이딩 기능을 수행하는 슬라이딩 버튼 등과 같이 다양한 형태의 입력부를 통해 구현될 수 있다.

[0035] 한편, 스위칭 동작이 슬라이딩 기능을 수행하는 슬라이딩 버튼으로 구현되는 경우를 가정하고 설명하면, 식별정보 레지스터부(120)는 신원인증 단말장치(100)의 외부에 노출되어 사용자가 직접 터치 또는 조작하여 슬라이딩 동작이 가능하다.

[0036] 구체적으로, 식별정보 레지스터부(120)는 슬라이딩 동작이 가능한 물리적인 버튼 또는 토글 형태로 구현될 수 있으며, 물리적인 버튼 또는 토글 내부에는 신원인증 단말장치(100)의 식별정보가 포함된 메모리가 위치할 수 있다.

[0037] 그리고, 신원인증 단말장치(100)의 식별정보는 신원인증 단말장치(100) 각각에 부여되는 식별번호(EIR, Equipment Identity Register)를 포함하며, 이러한 신원인증 단말장치(100) 각각에 부여되는 식별번호를 모든 신원인증정보에 동일하게 부여함으로써, 서로 다른 신원인증정보 간의 일관성을 획득할 수 있고, 신원인증정보의 허위성 여부를 검증할 수 있다.

[0038] 한편, 신원인증 단말장치(100)는 직접 공용서버와 접속하거나 스마트폰, PC 등을 통해 공용서버에 접속하여 상술한 고유번호 기반의 신원인증 단말장치(100)임을 확인할 수 있고, 이와 동시에 사용자 개인의 위치 정보 또는 동선 정보의 익명 제공 여부를 결정할 수 있다.

[0039] 또한, 고유번호 기반의 신원인증 단말장치(100)임이 확인되는 경우, 이러한 고유번호에 기반하여 신원인증 단말장치(100)의 전자 신분증 기능이 활성화될 수 있다.

[0040] 여기서, 신원인증 단말장치(100)가 고유번호 기반의 신원인증 단말장치(100)임을 확인하면서 사용자 개인의 위치 정보 또는 동선 정보의 익명 제공 여부를 결정하는 이유는, 위치 정보 또는 동선 정보를 통해 실제로 존재하는 실존 인물인지 여부를 검증할 수 있어, 신원인증정보에 대한 허위성 여부 판별이 가능하기 때문이다.

[0041] 이와 같이, 신원인증 단말장치(100)의 식별정보(Identification Information)가 포함된 메모리가 구비된 물리적인 버튼 또는 토글은 사용자 조작에 따라 슬라이딩 동작을 수행하면서, 사용자 정보가 포함된 메모리와 접촉할 수 있다.

[0042] 물론, 상술한 바와 같이, 식별정보 레지스터부(120)는 슬라이딩 동작이 아닌, 사용자의 터치 조작에 따라 사용자 정보가 포함된 메모리와 접촉될 수도 있고, 사용자의 스위칭 동작 또는 토글 동작에 따라 사용자 정보가 포함된 메모리와 접촉될 수도 있다.

[0043] 메모리(130)는 사용자 정보를 포함하며, 이러한 사용자 정보는 사용자의 CI(Connecting Information)나 DI(Duplication Information) 수단으로 활용할 수 있는 생체인식정보, 금융 정보, 결제 관련 정보, SNS 정보 중 적어도 하나를 포함한다.

[0044] 여기서 식별 정보는 공개 키(Public Key), 인증서(Certificate), NFT(Non-Fungible Token) 등에 관한 정보를 포함할 수 있고, 생체인식정보는 사용자의 홍채, 지문, 얼굴, 정맥 등에 관한 정보를 포함하고, 금융 정보는 사용자가 가입한 금융 상품 또는 은행 등에 관한 정보를 포함하며, 결제 관련 정보는 사용자의 신용 카드나 다양한 결제 방식 등에 관한 정보를 포함한다. 또한, SNS 정보는 사용자가 사용하는 소셜 네트워크 서비스의 명칭, 종류, 계정 등에 관한 정보를 포함할 수 있다.

[0045] 그리고, 암호화부(140)는 상술한 사용자 정보를 암호화하며, 이러한 암호화 과정에서 암호화 알고리즘이 사용될 수 있으며, 주로 "해시함수", “다변수함수”, “아이소제니”, “격자 계산”, “선형코드” 등을 활용한 방식으로 암호화가 이루어진다.

[0046] 한편, 본 발명의 일 실시 예에 따른 식별정보 레지스터부(120)는 스위칭 동작을 통해 메모리(130) 및 통신부(110)의 전기적 연결을 제어할 수 있다.

[0047] 구체적으로, 식별정보 레지스터부(120)는 스위칭 동작을 통해 메모리(130) 및 통신부(110)가 서로 전기적으로 연결되거나 또는 해제되도록 할 수 있으며, 예를 들어, 식별정보 레지스터부(120)가 스위칭 동작을 통해 메모리(130) 및 통신부(110) 간의 전기적 연결을 해제하면 식별정보 레지스터부(120)만 통신부(110)에 연결되어 식별정보 레지스터부(120)에 포함된 신원인증 단말장치(100)의 식별정보를 통신부(110)를 통해 외부 장치로 제공할 수 있다. 또한, 식별정보 레지스터부(120)가 스위칭 동작을 통해 메모리(130) 및 통신부(110)를 전기적으로 연결하면 식별정보 레지스터부(120)에 포함된 신원인증 단말장치(100)의 식별정보 및 메모리(130)에 포함된 사용자 정보를 결합하여 통신부(110)를 통해 외부 장치로 제공할 수 있다.

[0048] 한편, 본 발명의 다른 실시 예에 따른 신원인증 단말장치(100)는 사용자 정보를 암호화하기 위한 구성을 더 포함할 수 있다.

[0049] 도 2b는 본 발명의 다른 실시 예에 따른 신원인증 단말장치의 구성을 도시한 블록도이다.

[0050] 도 2b를 참조하면, 본 발명의 다른 실시 예에 따른 신원인증 단말장치(100)는 통신부(110), 식별정보 레지스터부(120), 메모리(130) 및 암호화부(140)를 포함할 수 있다.

[0051] 여기서, 암호화부(140)는 사용자 정보를 암호화하며, 이때, 식별정보 레지스터부(120)는 스위칭 동작을 통해 메

모리(130) 및 암호화부(140)와 통신부(110)를 연결할 수 있다.

[0052] 신원인증 단말장치(100)가 암호화부(140)를 포함하는 경우, 식별정보 레지스터부(120)는 스위칭 동작을 통해 도 2a와 같이 암호화부(140)를 포함하지 않는 신원인증 단말장치(100)에 비해 다양한 신원인증정보를 제공할 수 있다.

[0053] 예를 들어, 식별정보 레지스터부(120)는 스위칭 동작을 통해 메모리(130)와 통신부(110)를 연결시키거나, 메모리(130), 암호화부(140) 및 통신부(110)를 연결시킬 수 있으며, 아무것도 연결시키지 않은채 식별정보 레지스터부(120)만 통신부(110)에 연결될 수도 있다.

[0054] 그리고, 식별정보 레지스터부(120)는 이러한 스위칭 동작에 따라 서로 다른 신원인증정보를 통신부(110)를 통해 전송할 수 있다. 구체적으로, 식별정보 레지스터부(120)가 스위칭 동작에 따라 메모리(130)와 통신부(110)를 연결시키는 경우, 도 2a에서 상술한 바와 같이, 식별정보 레지스터부(120)에 포함된 신원인증 단말 장치(100)의 식별정보 및 메모리(130)에 포함된 사용자 정보를 결합하여 통신부(110)를 통해 외부 장치로 제공할 수 있다.

[0055] 또한, 식별정보 레지스터부(120)가 스위칭 동작에 따라 메모리(130), 암호화부(140) 및 통신부(110)를 연결시키는 경우, 식별정보 레지스터부(120)에 포함된 신원인증 단말장치(100)의 식별정보 및 메모리(130)에 포함된 사용자 정보가 암호화부(140)를 통해 암호화된 사용자 정보를 결합하여 통신부(110)를 통해 외부 장치로 제공할 수 있다.

[0056] 또한, 식별정보 레지스터부(120)가 스위칭 동작에 따라 아무것도 연결시키지 않아 식별정보 레지스터부(120)만 통신부(110)에 연결되는 경우, 식별정보 레지스터부(120)에 포함된 신원인증 단말장치(100)의 식별정보만을 통신부(110)를 통해 외부 장치로 제공할 수 있다.

[0057] 도 3a는 본 발명의 일 실시 예에 따른 신원인증 단말장치의 식별정보 레지스터부의 스위칭 동작에 따라 서로 다른 신원인증정보를 선택하는 구성에 대한 도면이다.

[0058] 도 3a를 참조하면, 신원인증 단말장치(100)가 전자 신분증 또는 전자 카드 형태로 구현되어 있으며, 식별정보 레지스터부(120)가 슬라이딩 동작이 가능한 버튼 형태로 구현되어 있다.

[0059] 또한, 식별정보 레지스터부(120)는 슬라이딩 동작이 가능한 슬라이딩 영역에서 사용자 조작에 따라 움직일 수 있으며, 신원인증 단말장치(100)를 턴오프 시키는 off 위치, A 위치, B 위치로 이동할 수 있다.

[0060] 식별정보 레지스터부(120)가 슬라이딩 동작에 따라 제1 위치에 위치하면 식별정보 레지스터부(120)는 통신부(110)와 연결되며, 신원인증 단말장치(100)의 식별정보에 기반한 제1 신원인증정보를 통신부(110)를 통해 전송할 수 있다. 여기서, 식별정보는 상술한 바와 같이 신원인증 단말장치(100)에 고유하게 부여된 식별번호를 포함할 수 있다.

[0061] 예를 들어, 식별정보 레지스터부(120)가 슬라이딩 동작에 따라 A 위치에 위치하면, 식별정보 레지스터부(120)는 신원인증 단말장치(100)의 식별번호 자체 또는 식별번호에 기반하여 생성된 별도의 코드를 포함하는 제1 신원인증정보를 통신부(110)를 통해 사용자 단말 장치 또는 PC 등과 같은 노드(200)로 전송할 수 있다.

[0062] 즉, 제1 신원인증정보는 신원인증 단말장치(100)에 고유하게 부여된 식별번호에 기반하여 생성된 것으로서, 신원인증 단말장치(100) 별로 고유한 속성을 포함하는 제1 신원인증정보는 서로 다른 신원인증정보의 허위신원 여부를 판별하는데 사용될 수 있다.

[0063] 이에 따라, 제1 신원인증정보는 신원인증 단말장치(100) 각각에 대해 모두 상이하게 생성된다.

[0064] 또한, 식별정보 레지스터부(120)가 슬라이딩 동작에 따라 제2 위치에 위치하면, 식별정보 레지스터부(120), 메모리(130) 및 통신부(110)가 연결되며, 식별정보 레지스터부(120)는 신원인증 단말장치(100)의 식별정보 및 사용자 정보를 포함하는 제2 신원인증정보를 통신부(110)를 통해 전송할 수 있다.

[0065] 예를 들어, 식별정보 레지스터부(120)가 슬라이딩 동작에 따라 B 위치에 위치하면, 식별정보 레지스터부(120)와 메모리(130)가 연결되면서, 식별정보 레지스터부(120)에 저장된 신원인증 단말장치(100)의 식별정보와 메모리(130)에 저장된 사용자 정보가 결합되어 제2 신원인증정보가 생성되고, 식별정보 레지스터부(120)는 생성된 제2 신원인증정보를 통신부(110)를 통해 사용자 단말 장치 또는 PC 등과 같은 노드(200)로 전송할 수 있다.

[0066] 여기서, 상술한 바와 같이 제1 신원인증정보는 신원인증 단말장치(100)의 식별번호 자체 또는 식별번호에 기반하여 생성된 별도의 코드를 포함할 수 있으며, 이에 따라, 식별정보 레지스터부(120)에 저장된 식별정보가 메모

리(130)에 저장된 사용자 정보와 결합되어 제2 신원인증정보가 생성될 수도 있으나, 식별번호에 기반하여 생성된 별도의 코드가 메모리(130)에 저장된 사용자 정보와 결합되어 제2 신원인증정보가 생성될 수도 있다.

[0067] 즉, 식별정보 또는 식별정보에 기반하여 생성된 별도의 코드가 사용자 정보와 결합되어 제2 신원인증정보가 생성될 수 있으며, 결과적으로 제1 신원인증정보에 사용자 정보가 결합되어 제2 신원인증정보가 생성되는 것으로 정리된다.

[0068] 한편, 식별정보 레지스터부(120)가 슬라이딩 동작에 따라 제3 위치에 위치하면, 식별정보 레지스터부(120), 메모리(130), 암호화부(140) 및 통신부(110)가 연결되며, 식별정보 레지스터부(120)는 신원인증 단말장치(100)의 식별정보 및 암호화된 사용자 정보를 포함하는 제3 신원인증정보를 통신부(110)를 통해 전송할 수 있다.

[0069] 도 3b는 본 발명의 다른 실시 예에 따른 신원인증 단말장치의 식별정보 레지스터부의 스위칭 동작에 따라 서로 다른 신원인증정보를 선택하는 구성에 대한 도면이다.

[0070] 여기서, 식별정보 레지스터부(120)가 A 위치 또는 B 위치에 위치하는 경우 생성되는 신원인증정보에 대해서는 도 3a에서 이미 설명하였으며 도 3b에도 동일하게 적용된다. 이에 따라, 도 3b와 같이 신원인증 단말장치(100)가 암호화부(140)를 더 포함하는 경우 발생할 수 있는, 식별정보 레지스터부(120)가 C 위치에 위치하는 경우에 대해 상세히 설명하기로 한다.

[0071] 예를 들어, 식별정보 레지스터부(120)가 슬라이딩 동작에 따라 C 위치에 위치하면, 식별정보 레지스터부(120)와 암호화부(140) 및 메모리(130)가 연결되면서, 식별정보 레지스터부(120)에 저장된 신원인증 단말장치(100)의 식별정보 또는 식별정보에 기반하여 생성된 별도의 코드와, 메모리(130)에 저장된 사용자 정보가 암호화부(140)에 의해 암호화된 사용자 정보가 결합되어 제3 신원인증정보가 생성되고, 식별정보 레지스터부(120)는 생성된 제3 신원인증정보를 통신부(110)를 통해 사용자 단말 장치 또는 PC 등과 같은 노드(200)로 전송할 수 있다.

[0072] 이에 따라, 도 3b와 같이, 신원인증 단말장치(100)가 통신부(110), 식별정보 레지스터부(120), 메모리(130) 및 암호화부(140)를 포함하는 경우, 식별정보 레지스터부(120)는 슬라이딩 동작에 따라 서로 다른 제1 신원인증정보, 제2 신원인증정보, 제3 신원인증정보를 통신부(110)를 통해 전송할 수 있다.

[0073] 이를 통해, 사용자는 상황에 맞는 보안성을 선택하여 이에 적합한 신원인증정보를 선택하여 전송할 수 있다.

[0074] 예를 들어, 제1 신원인증정보는 하드웨어 기반의 고유번호 속성을 포함하는 것으로 익명정보에 활용될 수 있고, 제2 신원인증정보는 고유번호 속성과 사용자 정보가 결합된 것으로 별명정보에 활용될 수 있고, 제3 신원인증정보는 사용자 정보가 암호화되어 고유번호 속성과 결합된 것으로 실명정보에 활용될 수 있다.

[0075] 즉, 높은 보안성이 요구될 수록 사용자 정보를 암호화하여 식별정보에 부가하고, 중간정도의 보안성이 요구되면 사용자 정보를 암호화하지 않고 식별정보에 부가하며, 낮은 정도의 보안성이 요구되면 식별정보만을 제공할 수 있다.

[0076] 한편, 도 3a 및 도 3b에서, 식별정보 레지스터부(120)가 슬라이딩 동작에 따라 off 위치에 위치하면, 신원인증 단말장치(100)는 턴오프될 수 있다.

[0077] 도 4는 본 발명의 일 실시 예에 따른 신원인증정보의 데이터 구성을 도시한 도면이다.

[0078] 도 4를 참조하면, 식별정보 레지스터부(120)의 위치별로 생성되는 신원인증정보에 포함되는 데이터 정보를 도시하고 있다.

[0079] 구체적으로, 식별정보 레지스터부(120)가 A 위치에 있을 때, 제1 신원인증정보(410)는 신원인증 단말장치(100)의 식별정보를 포함한다. 상술한 바와 같이, 제1 신원인증정보(410)는 신원인증 단말장치(100)의 식별정보에 기반하여 생성된 별도의 코드를 포함할 수도 있다.

[0080] 또한, 식별정보 레지스터부(120)가 B 위치에 있을 때, 제2 신원인증정보(420)는 신원인증 단말장치(100)의 식별정보 및 사용자 정보를 포함한다.

[0081] 또한, 식별정보 레지스터부(120)가 C 위치에 있을 때, 제3 신원인증정보(430)는 신원인증 단말장치(100)의 식별정보 및 암호화된 사용자 정보를 포함한다.

[0082] 한편, 식별정보 레지스터부(120)는 제1 신원인증정보를 통신부(110)를 통해 서버로 전송하여 신원인증 단말장치(100)의 활성화를 요청할 수 있다.

[0083] 도 5는 본 발명의 일 실시 예에 따른 신원인증 단말장치와 외부 장치들간의 데이터 전송 과정을 설명하기 위한

도면이다.

[0084] 도 5를 참조하면, 식별번호가 부여된 신원인증 단말장치(510)는 직접 서버(520)로 식별번호 확인 및 활성화를 요청할 수 있다(S510).

[0085] 서버(520)는 식별번호 확인을 통해 고유의 식별번호가 부여된 신원인증 단말장치(510)를 확인하고, 신원인증 단말장치(510)를 활성화시킬 수 있다(S520).

[0086] 이때, 도 5에 도시되지 않았으나, 서버(520)는 신원인증 단말장치(510)로 개인 동선 정보 또는 위치 정보의 익명 제공 동의를 요청할 수도 있다.

[0087] 또한, 신원인증 단말장치(510)는 서버(520)에 접속하여 사용자 정보를 등록할 수 있다(S530).

[0088] 그리고, 신원인증 단말장치(510)는 사용자 정보를 자체 메모리에 저장한다(S540).

[0089] 이후, 신원인증 단말장치(510)는 사용자 정보와 식별번호 정보를 선택적으로 결합 또는 암호화된 사용자 정보와 식별번호 정보를 선택적으로 결합하여 생성된 서로 다른 신원인증정보를 선택적으로 PC, 키오스크 등과 같은 노드(530)에 제공할 수 있다(S550).

[0090] 한편, 도 5와 같이, 신원인증 단말장치(510)가 서버(520)에 직접 식별번호 확인 및 활성화를 요청할 수도 있으나, 전용 어플리케이션을 통해 식별번호 확인 및 활성화를 요청할 수도 있다.

[0091] 도 6은 본 발명의 다른 실시 예에 따른 신원인증 단말장치와 외부 장치들간의 데이터 전송 과정을 설명하기 위한 도면이다.

[0092] 도 6을 참조하면, 식별번호가 부여된 신원인증 단말장치(610)는 사용자 단말장치(620)로 식별번호 전송을 요청할 수 있다(S610).

[0093] 그리고, 사용자 단말장치(620)는 신원인증 단말장치(610)의 요청에 따라 신원인증 단말장치(610)에 부여된 식별번호 확인 및 활성화를 서버(630)로 요청할 수 있다(S620).

[0094] 서버(630)는 식별번호 확인을 통해 고유의 식별번호가 부여된 신원인증 단말장치(610)를 확인하고, 신원인증 단말장치(610)를 활성화시킬 수 있다(S630).

[0095] 이때, 도 6에 도시되지 않았으나, 서버(630)는 신원인증 단말장치(610) 또는 사용자 단말장치(620)로 개인 동선 정보 또는 위치 정보의 익명 제공 동의를 요청할 수도 있다.

[0096] 또한, 신원인증 단말장치(610)는 서버(630)에 접속하여 사용자 정보를 등록할 수 있다(S640).

[0097] 그리고, 신원인증 단말장치(610)는 사용자 정보를 자체 메모리에 저장한다(S650).

[0098] 이후, 신원인증 단말장치(610)는 사용자 정보와 식별번호 정보를 선택적으로 결합 또는 암호화된 사용자 정보와 식별번호 정보를 선택적으로 결합하여 생성된 서로 다른 신원인증정보를 선택적으로 사용자 단말장치(620)로 전송할 수 있고, 사용자 단말장치(620)는 수신된 서로 다른 신원인증정보를 PC, 키오스크 등과 같은 노드(640)로 선택적으로 제공할 수 있다(S670).

[0099] 도 7은 본 발명의 일 실시 예에 따른 메쉬 네트워크와 복수의 신원인증 단말장치 간의 관계를 도시한 도면이다.

[0100] 도 7을 참조하면, 복수의 신원인증자가 각각의 노드를 통해 공용서버에 식별 번호 확인 및 활성화 요청을 통한 인증 확인 절차를 수행하고, 노드와 노드 간의 P2P 연결을 통해 각각의 신원인증장치 내에 저장된 서로 다른 신원인증정보가 선택적으로 제공될 수 있으며, 이러한 노드와 노드 간의 P2P 연결이 거대해지면서 메쉬 네트워크가 형성됨을 설명하고 있다.

[0101] 이러한 메쉬 네트워크에서도 복수의 신원인증 단말장치는 노드를 통해 공용서버에 식별번호 확인 및 활성화 요청을 통한 인증 확인 절차를 수행하고, 신원인증정보를 사용자 조작에 따라 선택적으로 제공할 수 있다.

[0102] 이에 따라, 사용자는 버튼의 간단한 슬라이딩 조작만으로 보안성에 따라 적절한 신원인증정보를 선택하여 제공할 수 있어, 사용자 편의성이 증대되고 사용자가 본인의 신원인증정보를 관리할 수 있게 된다.

[0103] 또한, 이상에서는 본 발명의 바람직한 실시 예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의

기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

[0104] 또한, 도면에 도시된 구성 요소들 간의 연결 선들 또는 연결 부재들은 기능적 연결, 물리적 연결 또는 회로적 연결들을 예시적으로 나타낸 것으로서, 실제 장치에서는 대체 가능하거나 추가의 다양한 상기 연결들로 나타내질 수 있다. 또한, 구성요소에 대한 기재에 있어서 특별히 필수적이라는 별도의 언급이 없다면 본원발명의 적용을 위하여 반드시 필요한 구성요소가 아닐 수 있다.

부호의 설명

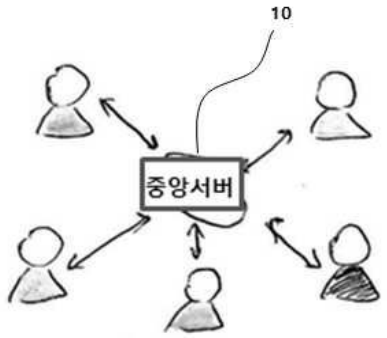
[0105] 100: 신원인증 단말장치 110: 통신부

120: 식별정보 레지스터부 130: 메모리

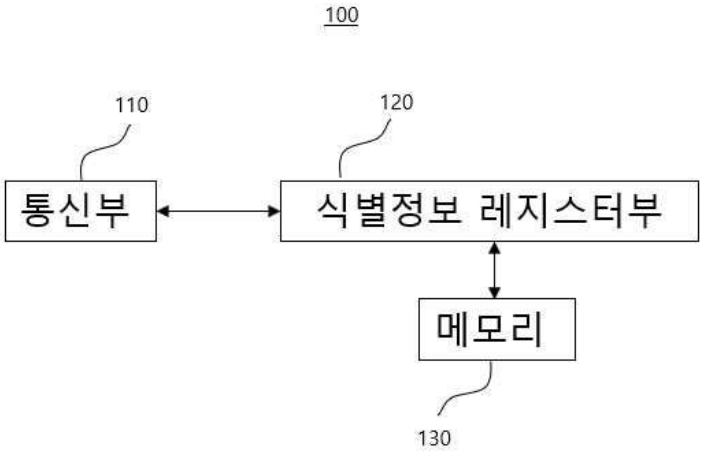
140: 암호화부

도면

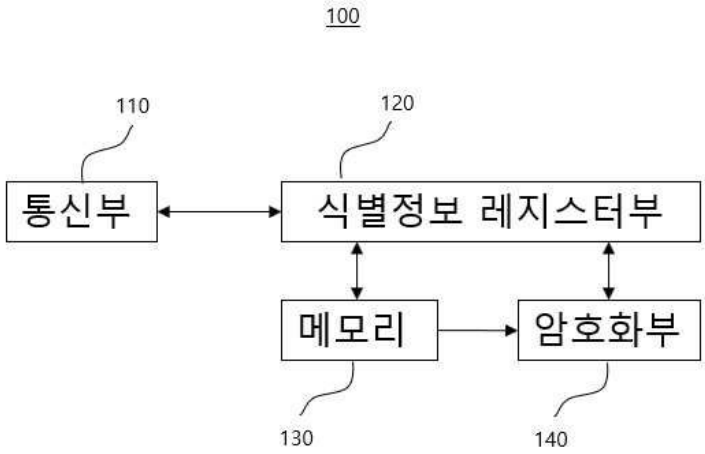
도면1



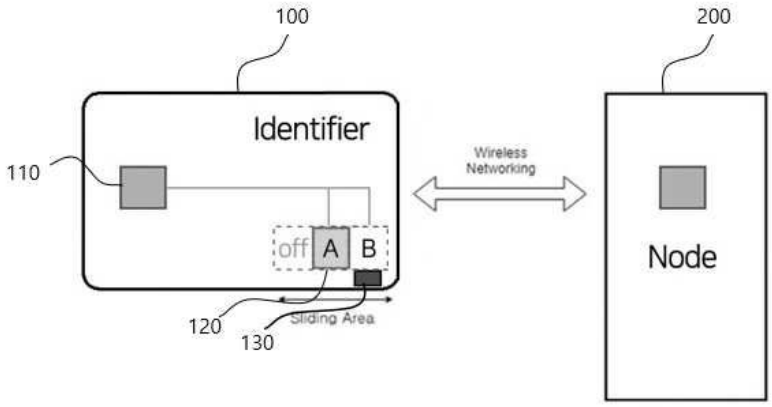
도면2a



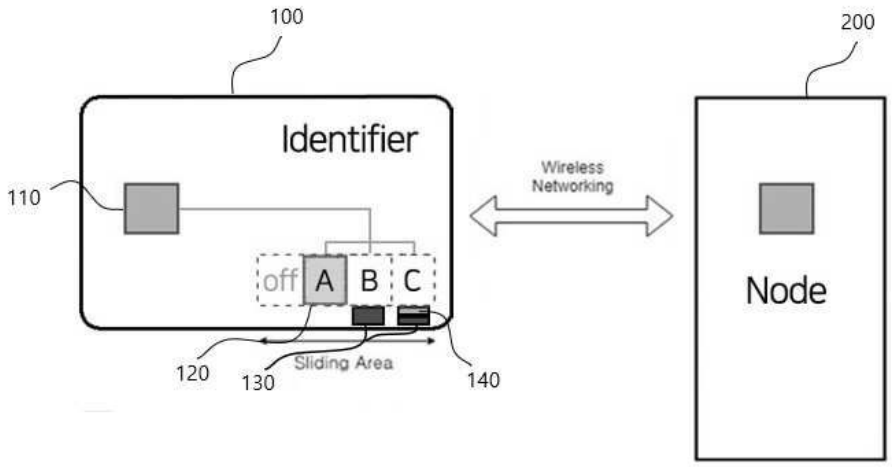
도면2b



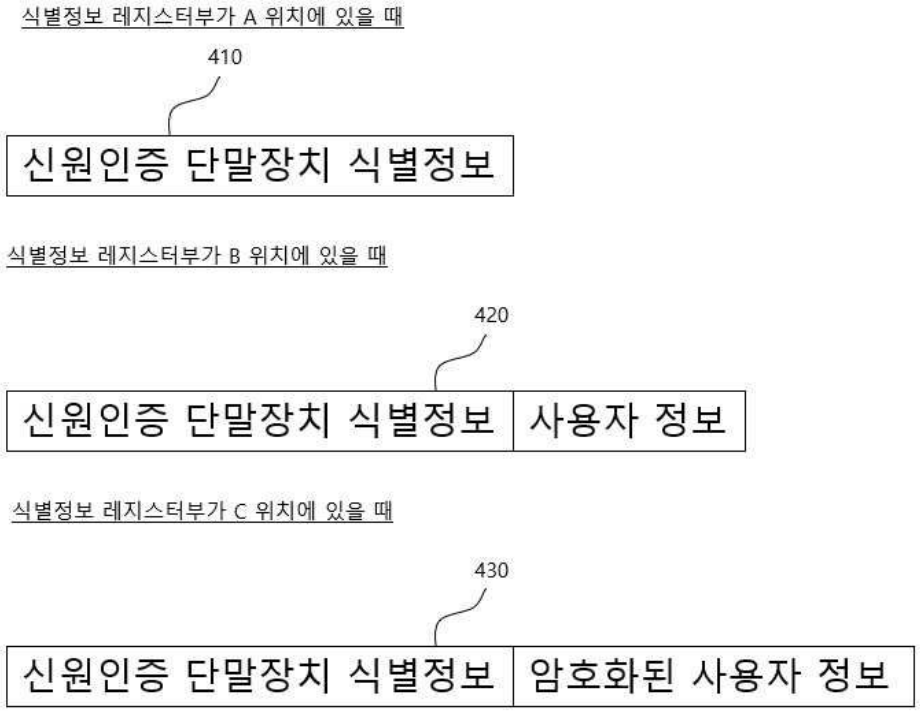
도면3a



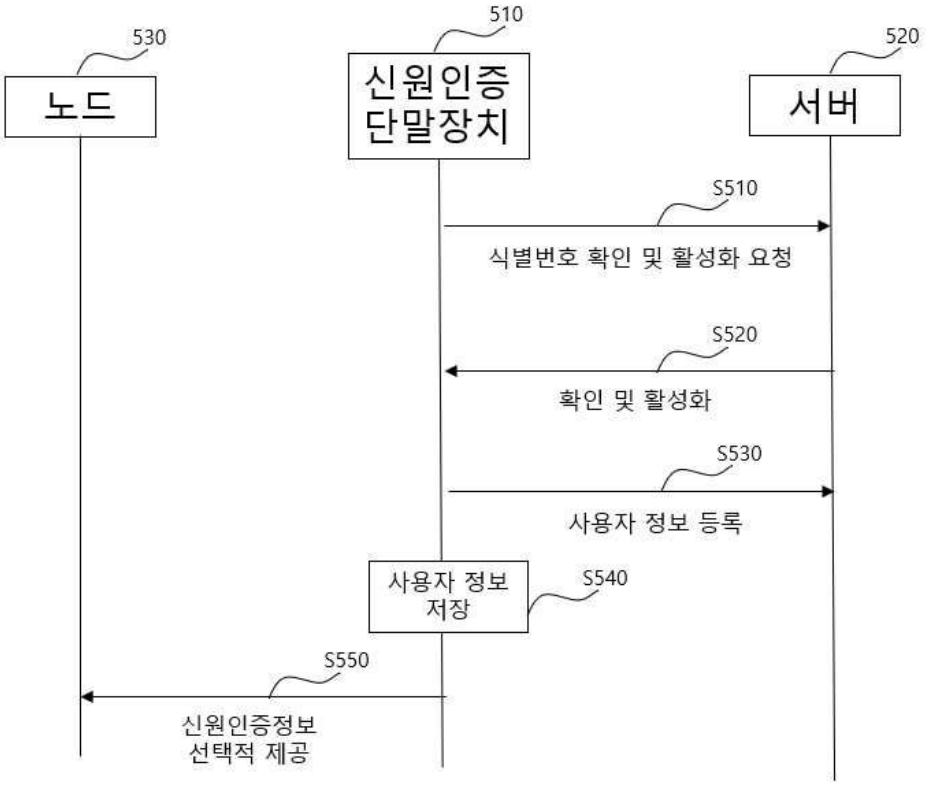
도면3b



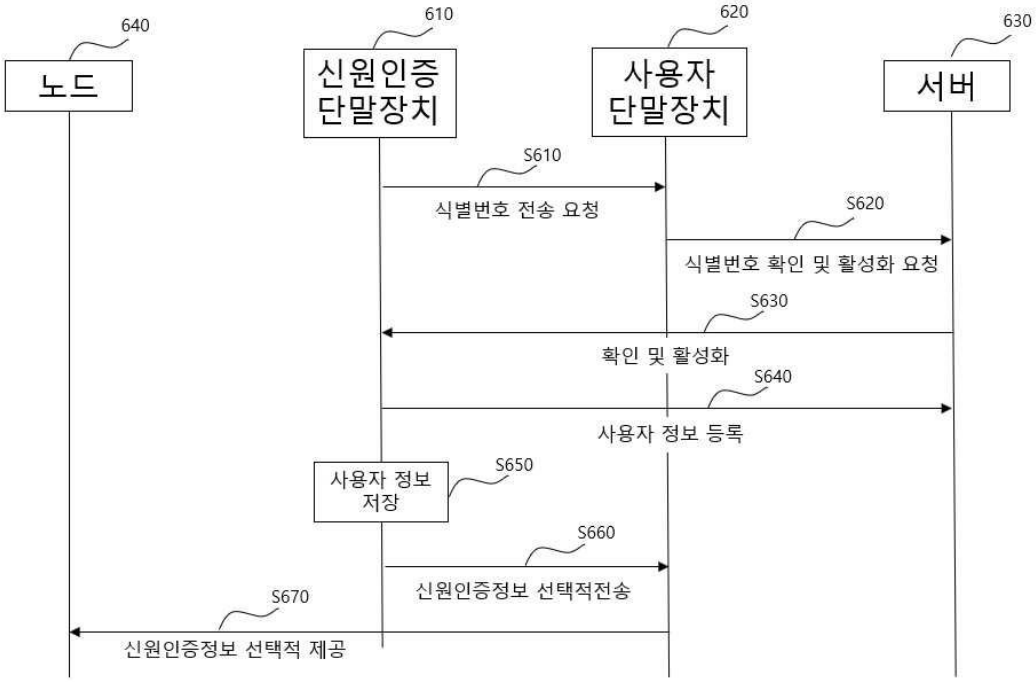
도면4


식별정보 레지스터부가 A 위치에 있을 때
410
신원인증 단말장치 식별정보
식별정보 레지스터부가 B 위치에 있을 때
420
신원인증 단말장치 식별정보
사용자 정보
식별정보 레지스터부가 C 위치에 있을 때
430
신원인증 단말장치 식별정보
암호화된 사용자 정보

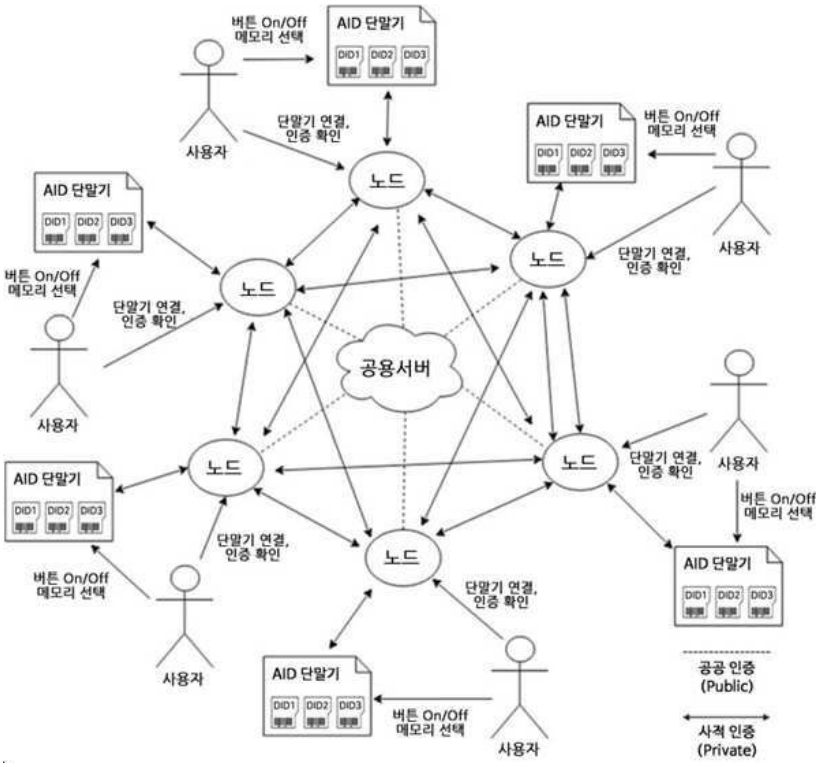
도면5


530
노드
510
신원인증 단말장치
520
서버
S510
식별번호 확인 및 활성화 요청
S520
확인 및 활성화
S530
사용자 정보 등록
사용자 정보 저장
S540
S550
신원인증정보 선택적 제공

도면6


640
노드
610
신원인증 단말장치
620
사용자 단말장치
630
서버
S610
식별번호 전송 요청
S620
식별번호 확인 및 활성화 요청
S630
확인 및 활성화
S640
사용자 정보 등록
사용자 정보 저장
S650
S660
신원인증정보 선택적전송
S670
신원인증정보 선택적 제공

도면7


버튼 On/Off 메모리 선택
AID 단말기
DID1
DID2
DID3
사용자
단말기 연결, 인증 확인
노드
공용서버
공공 인증 (Public)
사적 인증 (Private)