(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년05월31일
(11) 등록번호 10-2538652
(24) 등록일자 2023년05월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06Q 50/10* (2012.01)
H04L 67/131 (2022.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
G06Q 50/10 (2015.01)
(21) 출원번호 10-2021-0192204
(22) 출원일자 2021년12월30일
심사청구일자 2021년12월30일
(56) 선행기술조사문헌
KR1020030035025 A
KR1020150129869 A
KR1020200100451 A
WO2011047276 A2

(73) 특허권자
(주)아톤
서울특별시 마포구 성암로 189 , 1201호(상암동, 중소기업디엠씨타워)
(72) 발명자
김종서
서울특별시 마포구 성암로 189, 12층 1201호
임형수
서울특별시 마포구 성암로 189, 12층 1201호
(뒷면에 계속)
(74) 대리인
김한솔, 김세환, 김준식, 안제성

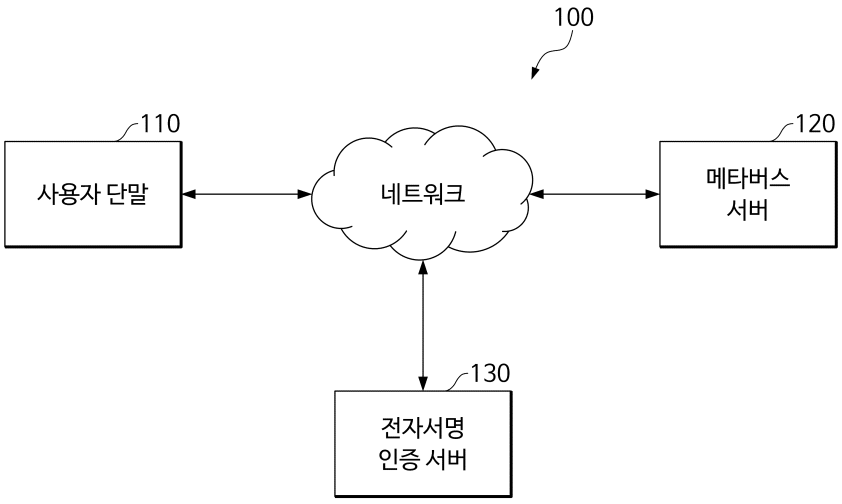
전체 청구항 수 : 총 10 항 심사관 : 양종필

(54) 발명의 명칭 **메타버스 환경에서의 전자서명 방법 및 장치**

(57) 요 약

본 개시는 적어도 하나의 프로세서에 의해 수행되는 전자서명 방법이다. 전자서명 방법은 사용자 단말로부터 메타버스 환경의 로그인을 위한 인증서와 연관된 제1 개인 식별 정보 및 메타버스 환경에서 사용하기 위한 전자서명 원문 요청 정보를 수신하는 단계, 메타버스용 개인키 및 공개키의 키 쌍(key pair)을 생성하는 단계, 제1 개인 식별 정보를 기초로 개인키를 암호화하여 저장하는 단계, 사용자 단말로 메타버스용 공개키를 포함한 전자서명 원문을 전송하는 단계 - 사용자 단말에 의해, 메타버스용 공개키를 포함한 전자서명 원문의 전자서명이 수행됨 -, 사용자 단말로부터 전자서명의 검증 요청을 수신한 메타버스 서버로부터, 전자서명의 검증 요청을 수신하는 단계, 및 전자서명의 검증을 수행하여, 전자서명의 검증 결과 및 인증서에 대응하는 고객 ID를 메타버스 서버로 전송하는 단계를 포함하고, 메타버스 환경에서 고객 ID에 대응하는 아바타가 활성화될 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 67/131 (2022.05)
H04L 9/0825 (2013.01)
H04L 9/0866 (2013.01)
H04L 9/321 (2013.01)
H04L 9/3263 (2013.01)
(72) 발명자
양성진
서울특별시 마포구 성암로 189, 12층 1201호
홍재용
서울특별시 마포구 성암로 189, 12층 1201호

명 세 서

청구범위

청구항 1

적어도 하나의 프로세서에 의해 수행되는, 메타버스 환경에서의 전자서명 방법에 있어서,

사용자 단말로부터 메타버스 환경의 로그인을 위한 인증서와 연관된 제1 개인 식별 정보 및 메타버스 환경에서 사용하기 위한 전자서명 원문 요청 정보를 수신하는 단계;

메타버스용 개인키 및 공개키의 키 쌍(key pair)을 생성하는 단계;

상기 제1 개인 식별 정보를 기초로 상기 개인키를 암호화하여 저장하는 단계;

상기 사용자 단말로 상기 메타버스용 공개키를 포함한 전자서명 원문을 전송하는 단계 - 상기 사용자 단말에 의해, 상기 메타버스용 공개키를 포함한 전자서명 원문의 전자서명이 수행됨 -;

상기 사용자 단말로부터 상기 전자서명의 검증 요청을 수신한 메타버스 서버로부터, 상기 전자서명의 검증 요청을 수신하는 단계; 및

상기 전자서명의 검증을 수행하여, 상기 전자서명의 검증 결과 및 인증서에 대응하는 고객 ID를 상기 메타버스 서버로 전송하는 단계를 포함하고,

상기 메타버스 환경에서 상기 고객 ID에 대응하는 아바타가 활성화되는,

메타버스 환경에서의 전자서명 방법.

청구항 2

제1항에 있어서,

상기 메타버스 환경의 로그인을 하기 위한 인증서는 일련번호를 포함하고,

상기 메타버스용 개인키 및 공개키의 키 쌍을 생성하는 단계는,

상기 일련번호를 이용하여 상기 인증서의 상태를 조회하는 단계;

상기 인증서의 기한이 만기되지 않은 경우, 상기 제1 개인 식별 정보를 검증하는 단계; 및

상기 제1 개인 식별 정보가 검증된 경우, 상기 메타버스용 개인키 및 상기 메타버스용 공개키의 쌍을 생성하는 단계

를 포함하는, 메타버스 환경에서의 전자서명 방법.

청구항 3

제1항에 있어서,

상기 메타버스 서버로부터, 상기 아바타가 활성화된 메타버스 환경 내에서 상기 아바타의 구매 행위로 생성된 구매 서명 원문 및 사용자 단말로부터 상기 메타버스 서버로 전송된 제2 개인 식별 정보를 수신하는 단계;

상기 메타버스용 개인키를 이용하여 상기 구매 서명 원문의 전자서명을 수행하는 단계;

상기 메타버스용 공개키를 이용하여, 상기 전자서명의 검증을 수행하는 단계; 및

상기 수행된 전자서명의 검증에 대한 결과를 상기 메타버스 서버에 전송하는 단계

를 더 포함하고,

상기 제1 개인 식별 정보 및 상기 제2 개인 식별 정보는 동일한 정보를 포함하는, 메타버스 환경에서의 전자서명 방법.

청구항 4

제3항에 있어서,

상기 메타버스용 개인키를 이용하여 상기 전자서명을 수행하는 단계는,

상기 수신된 제2 개인 식별 번호를 기초로 상기 메타버스용 개인키를 활성화하는 단계; 및

상기 활성화된 메타버스용 개인키를 이용하여, 상기 구매 서명 원문의 전자서명을 수행하는 단계

를 포함하는, 메타버스 환경에서의 전자서명 방법.

청구항 5

제1항에 있어서,

상기 고객 ID가 상기 메타버스 환경에서 로그아웃되는 경우, 상기 메타버스용 개인키 및 공개키 키 쌍을 무효화시키는 단계

를 더 포함하는, 메타버스 환경에서의 전자서명 방법.

청구항 6

제1항에 있어서,

상기 제1 개인 식별 정보 및 제2 개인 식별 정보는, PIN 번호, 패턴 정보 또는 생체 인식 정보 중 하나를 포함하는, 메타버스 환경에서의 전자서명 방법.

청구항 7

제1항에 있어서,

상기 제1 개인 식별 정보를 기초로 상기 개인키를 암호화하여 저장하는 단계는, 상기 제1 개인 식별 정보를 이용하여 상기 메타버스용 개인키를 PBKDF2(Password-Based Key Derivation Function Version 2) 방법으로 암호화하는 단계를 포함하는, 메타버스 환경에서의 전자서명 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 따른 방법을 컴퓨터에서 실행하기 위해 컴퓨터 판독 가능한 기록 매체에 저장된 컴퓨터 프로그램.

청구항 9

전자서명 인증 서버 장치로서,

통신 모듈;

메모리; 및

상기 메모리와 연결되고, 상기 메모리에 포함된 컴퓨터 판독 가능한 적어도 하나의 프로그램을 실행하도록 구성된 적어도 하나의 프로세서

를 포함하고,

상기 적어도 하나의 프로그램은,

사용자 단말로부터 메타버스 환경의 로그인을 위한 인증서와 연관된 제1 개인 식별 정보 및 메타버스 환경에서 사용하기 위한 전자서명 원문 요청 정보를 수신하고,

메타버스용 개인키 및 공개키의 키 쌍을 생성하고,

상기 제1 개인 식별 정보를 기초로 상기 개인키를 암호화하여 저장하고,

상기 전자서명 원문 요청 정보에 응답하여, 상기 사용자 단말로 상기 메타버스용 공개키를 포함한 전자서명 원문을 전송하고,

상기 사용자 단말로 상기 메타버스용 공개키를 포함한 전자서명 원문을 전송하고 - 상기 사용자 단말에 의해, 상기 메타버스용 공개키를 포함한 전자서명 원문의 전자서명이 수행됨 -,

상기 사용자 단말로부터 상기 전자서명의 검증 요청을 수신한 메타버스 서버로부터, 상기 전자서명의 검증 요청을 수신하고,

상기 전자서명의 검증을 수행하여, 상기 전자서명의 검증 결과 및 인증서에 대응하는 고객 ID를 상기 메타버스 서버로 전송하기 위한 명령어를 포함하고,

상기 메타버스 환경에서 상기 고객 ID에 대응하는 아바타가 활성화되는,

전자서명 인증 서버 장치.

청구항 10

제9항에 있어서,

상기 명령어는, 상기 고객 ID가 상기 메타버스 환경에서 로그아웃되는 경우, 상기 메타버스용 개인키 및 공개키 키 쌍을 무효화시키기 위한 명령어를 더 포함하는,

전자서명 인증 서버 장치.

발명의 설명

기 술 분 야

[0001] 본 개시는 메타버스 환경에서의 전자서명 방법 및 장치에 관한 것으로, 구체적으로, 현실 세계에서 사용자가 사용자 단말로 수행한 전자서명한 결과를 기초로 하여, 메타버스 환경에서 아바타가 안전하고 쉽게 전자서명할 수 있는 전자서명 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 온라인과 오프라인에서 하루에도 몇 번씩 본인 확인을 하고 있다. 실제 정당한 사용자인지 확인하는 사용자 인증(Authentication) 절차를 수행하고 있는 것이다. 온라인에서 PC나 스마트폰을 이용하여 은행 사이트(또는 앱)에 접속할 때 ID/패스워드나 인증서 또는 지문 등을 이용하여 본인인증하고, 회사에 출근할 때 사원증을 보여줌으로써 본인인증을 한다. 또한 운전할 때는 운전할 자격이 있음을 증명하기 위하여 운전면허증을 소지한다.

[0003] 한편, 인공지능, 사물인터넷, 블록체인 등의 새로운 IT 기술이 등장하고, 감염병의 확산 등으로 인하여, 일상의 많은 부분이 비대면 환경으로 전환되고 있는 등 서비스 환경의 변화가 급속하게 일어나고 있다. 특히, 최근에는 현실 세계에서 이루어지던 사회, 문화, 경제 활동을 온라인의 가상 환경에서 체험할 수 있는 메타버스(Metaverse) 기술이 주목받고 있다. 사용자는 가상 환경인 메타버스 상에서 아바타를 이용하여 물건을 구매하고, 콘서트에 참석하는 등 현실 세계와 같은 문화, 경제 활동을 메타버스 상에서 할 수 있다.

[0004] 다만, 현실 세계에서 문화, 경제 활동을 하는 경우, 단말 장치에 설치된 인증서 등을 이용한 전자서명을 통해 사용자 인증을 수행할 수 있으나, 메타버스와 같은 가상 환경에서는 아바타가 현실 세계와 같은 단말 장치를 사용하지 않으므로, 이를 이용한 사용자 인증 방법이 마련되어 있지 않은 실정이다. 메타버스상에서도 아바타가 안전하고 쉽게 전자서명을 할 수 있는 기술들이 절실히 필요한 상황이다.

발명의 내용

해결하려는 과제

[0005] 본 개시는 상기와 같은 문제점을 해결하기 위한 메타버스 환경에서의 전자서명 방법, 기록매체에 저장된 컴퓨터 프로그램 및 장치(시스템)를 제공한다.

과제의 해결 수단

[0006] 본 개시는 방법, 장치(시스템) 또는 판독 가능 저장 매체에 저장된 컴퓨터 프로그램을 포함한 다양한 방식으로 구현될 수 있다.

[0007] 본 개시의 일 실시예에 따르면, 적어도 하나의 프로세서에 의해 실행되는, 메타버스 환경에서의 전자서명 방법은, 사용자 단말로부터 메타버스 환경의 로그인을 위한 인증서와 연관된 제1 개인 식별 정보 및 메타버스 환경에서 사용하기 위한 전자서명 원문 요청 정보를 수신하는 단계, 메타버스용 개인키 및 공개키의 키 쌍(key pair)을 생성하는 단계, 제1 개인 식별 정보를 기초로 개인키를 암호화하여 저장하는 단계, 사용자 단말로 메타버스용 공개키를 포함한 전자서명 원문을 전송하는 단계 - 사용자 단말에 의해, 메타버스용 공개키를 포함한 전자서명 원문의 전자서명이 수행됨 -, 사용자 단말로부터 전자서명의 검증 요청을 수신한 메타버스 서버로부터, 전자서명의 검증 요청을 수신하는 단계, 및 전자서명의 검증을 수행하여, 전자서명의 검증 결과 및 인증서에 대응하는 고객 ID를 메타버스 서버로 전송하는 단계를 포함하고, 메타버스 환경에서 고객 ID에 대응하는 아바타가 활성화될 수 있다.

[0008] 본 개시의 일 실시예에 따르면, 메타버스 환경으로 로그인을 하기 위한 인증서는 일련번호를 포함하고, 메타버스용 개인키 및 공개키의 키 쌍을 생성하는 단계는, 일련번호를 이용하여 인증서의 상태를 조회하는 단계, 인증서의 기한이 만기되지 않는 경우, 제1 개인 식별 정보를 검증하는 단계, 및 제1 개인 식별 정보가 검증된 경우, 메타버스용 개인키 및 메타버스용 공개키의 쌍을 생성하는 단계를 포함할 수 있다.

[0009] 본 개시의 일 실시예에 따르면, 전자서명 방법은, 메타버스 서버로부터, 아바타가 활성화된 메타버스 환경 내에서 아바타의 구매 행위로 생성된 구매 서명 원문 및 사용자 단말로부터 메타버스 서버로 전송된 제2 개인 식별 정보를 수신하는 단계, 메타버스용 개인키를 이용하여 구매 서명 원문의 전자서명을 수행하는 단계, 메타버스용 공개키를 이용하여, 전자서명의 검증을 수행하는 단계, 및 수행된 전자서명의 검증에 대한 결과를 메타버스 서버에 전송하는 단계를 더 포함할 수 있다.

[0010] 본 개시의 일 실시예에 따르면, 제1 개인 식별 정보 및 제2 개인 식별 정보는 동일한 정보를 포함할 수 있다.

[0011] 본 개시의 일 실시예에 따르면, 메타버스용 개인키를 이용하여 전자서명을 수행하는 단계는, 수신된 제2 개인 식별 번호를 기초로 메타버스용 개인키를 활성화하는 단계, 및 활성화된 메타버스용 개인키를 이용하여, 구매 서명 원문의 전자서명을 수행하는 단계를 포함할 수 있다.

[0012] 본 개시의 일 실시예에 따르면, 전자서명 방법은, 고객 ID가 메타버스 환경에서 로그아웃되는 경우, 메타버스용 개인키 및 공개키 키 쌍을 무효화시키는 단계를 더 포함할 수 있다.

[0013] 본 개시의 일 실시예에 따르면, 제1 개인 식별 정보 및 제2 개인 식별 정보는, PIN 번호, 패턴 정보 또는 생체 인식 정보 중 하나를 포함할 수 있다.

[0014] 본 개시의 일 실시예에 따르면, 전자서명 방법은, 제1 개인 식별 정보를 기초로 개인키를 암호화하여 저장하는 단계는, 제1 개인 식별 정보를 이용하여 메타버스용 개인키를 PBKDF2(Password-Based Key Derivation Function Version 2) 방법으로 암호화하는 단계를 포함할 수 있다.

[0015] 본 개시의 일 실시예에 따른 전자서명 방법을 컴퓨터에서 실행하기 위해 컴퓨터 판독 가능한 기록 매체에 저장된 컴퓨터 프로그램이 제공된다.

[0016] 본 개시의 일 실시예에 따른 전자서명 인증 서버 장치는, 통신 모듈, 메모리, 및 메모리와 연결되고, 메모리에 포함된 컴퓨터 판독 가능한 적어도 하나의 프로그램을 실행하도록 구성된 적어도 하나의 프로세서를 포함하고, 적어도 하나의 프로그램은, 사용자 단말로부터 메타버스 환경의 로그인을 위한 인증서와 연관된 제1 개인 식별 정보 및 메타버스 환경에서 사용하기 위한 전자서명 원문 요청 정보를 수신하고, 메타버스용 개인키 및 공개키의 키 쌍을 생성하고, 제1 개인 식별 정보를 기초로 개인키를 암호화하여 저장하고, 전자서명 원문 요청 정보에 응답하여, 사용자 단말로 메타버스용 공개키를 포함한 전자서명 원문을 전송하고, 사용자 단말로 메타버스용 공개키를 포함한 전자서명 원문을 전송하고 - 사용자 단말에 의해, 메타버스용 공개키를 포함한 전자서명 원문의 전자서명이 수행됨 -, 사용자 단말로부터 전자서명의 검증 요청을 수신한 메타버스 서버로부터, 전자서명의 검증 요청을 수신하고, 전자서명의 검증을 수행하여, 전자서명의 검증 결과 및 인증서에 대응하는 고객 ID를 메타버스 서버로 전송하기 위한 명령어를 포함하고, 메타버스 환경에서 고객 ID에 대응하는 아바타가 활성화될 수 있다.

[0017] 본 개시의 일 실시예에 따르면, 명령어는, 고객 ID가 메타버스 환경에서 로그아웃되는 경우, 메타버스용 개인키 및 공개키 키 쌍을 무효화시키기 위한 명령어를 더 포함할 수 있다.

발명의 효과

[0018] 본 개시의 일부 실시예에 따르면, 현실 세계에서 사용자가 사용자 단말로 수행한 전자서명한 결과를 기초로 하여, 메타버스 환경에서 아바타가 안전하고 쉽게 전자서명할 수 있다.

[0019] 본 개시의 일부 실시예에 따르면, 사용자가 메타버스에 입장 시 현실세계에서 사용하는 개인 식별 정보(예컨대, PIN 번호 등)로 전자서명을 수행하면, 이를 이용하여, 메타버스 상에서의 거래 등에 있어서도, 현실세계에서 사용하는 개인 식별 정보를 이용하여 전자서명할 수 있는 서비스를 제공할 수 있다.

[0020] 본 개시의 일부 실시예에 따르면, 개인이 메타버스에 입장할 때, 소유한 개인키로 사용자 단말을 이용하여 전자서명을 수행하면, 메타버스 상에서 사용될 개인키(예컨대, 일회용 개인키 등) 및 공개키 키 쌍을 생성함으로써, 메타버스 상에서는 개인키 및 공개키 키 쌍을 이용하여 전자 서명 및 검증을 수행할 수 있다.

[0021] 본 개시의 일부 실시예에 따르면, 현실 세계와 동일한 인증수단을 통해 메타버스 내에서 메타버스용 인증서로 구매 행위, 뱅킹, 보험, 자격증 획득, 분산신원증명 발행 등 인증이 필요한 작업 모두를 가능하게 할 수 있다.

[0022] 본 개시의 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급되지 않은 다른 효과들은 청구범위의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자(“통상의 기술자” 라 함)에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0023] 본 개시의 실시예들은, 이하 설명하는 첨부 도면들을 참조하여 설명될 것이며, 여기서 유사한 참조 번호는 유사한 요소들을 나타내지만, 이에 한정되지는 않는다.

도 1은 본 개시의 일 실시예에 따른 전자 서명 시스템의 구성도이다.

도 2 및 도 3은 본 개시의 일 실시예에 따른 메타버스 환경에서의 전자서명 방법을 나타내는 흐름도이다.

도 4 및 도 5는 본 개시의 일 실시예에 따른 메타버스 환경에서 구매를 위한 전자서명 처리 방법을 나타내는 흐름도이다.

도 6은 본 개시의 일 실시예에 따른 메타버스 환경에서의 전자서명 방법을 나타내는 흐름도이다.

도 7은 본 개시의 일 실시예에 따른 메타버스 환경 내에서 아바타의 구매 행위에 대한 구매 전자서명 방법을 나타내는 흐름도이다.

도 8은 본 개시의 일 실시예에 따른 전자서명 인증 서버의 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0024] 이하, 본 개시의 실시를 위한 구체적인 내용을 첨부된 도면을 참조하여 상세히 설명한다. 다만, 이하의 설명에서는 본 개시의 요지를 불필요하게 흐릴 우려가 있는 경우, 널리 알려진 기능이나 구성에 관한 구체적 설명은 생략하기로 한다.

[0025] 첨부된 도면에서, 동일하거나 대응하는 구성요소에는 동일한 참조부호가 부여되어 있다. 또한, 이하의 실시예들의 설명에 있어서, 동일하거나 대응되는 구성요소를 중복하여 기술하는 것이 생략될 수 있다. 그러나, 구성요소에 관한 기술이 생략되어도, 그러한 구성요소가 어떤 실시예에 포함되지 않는 것으로 의도되지는 않는다.

[0026] 개시된 실시예의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 개시는 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 개시가 완전하도록 하고, 본 개시가 통상의 기술자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것일 뿐이다.

[0027] 본 명세서에서 사용되는 용어에 대해 간략히 설명하고, 개시된 실시예에 대해 구체적으로 설명하기로 한다. 본 명세서에서 사용되는 용어는 본 개시에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 관련 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 발명의 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서, 본 개시에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 개시의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0028] 본 명세서에서의 단수의 표현은 문맥상 명백하게 단수인 것으로 특정하지 않는 한, 복수의 표현을 포함한다. 또한, 복수의 표현은 문맥상 명백하게 복수인 것으로 특정하지 않는 한, 단수의 표현을 포함한다. 명세서 전체에서 어떤 부분이 어떤 구성요소를 포함한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다.

[0029] 또한, 명세서에서 사용되는 '모듈' 또는 '부'라는 용어는 소프트웨어 또는 하드웨어 구성요소를 의미하며, '모듈' 또는 '부'는 어떤 역할들을 수행한다. 그렇지만, '모듈' 또는 '부'는 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. '모듈' 또는 '부'는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서, '모듈' 또는 '부'는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 또는 변수들 중 적어도 하나를 포함할 수 있다. 구성요소들과 '모듈' 또는 '부'들은 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 '모듈' 또는 '부'들로 결합되거나 추가적인 구성요소들과 '모듈' 또는 '부'들로 더 분리될 수 있다.

[0030] 본 개시의 일 실시예에 따르면, '모듈' 또는 '부'는 프로세서 및 메모리로 구현될 수 있다. '프로세서'는 범용 프로세서, 중앙 처리 장치(CPU), 마이크로프로세서, 디지털 신호 프로세서(DSP), 제어기, 마이크로제어기, 상태 머신 등을 포함하도록 넓게 해석되어야 한다. 몇몇 환경에서, '프로세서'는 주문형 반도체(ASIC), 프로그램가능 로직 디바이스(PLD), 필드 프로그램가능 게이트 어레이(FPGA) 등을 지칭할 수도 있다. '프로세서'는, 예를 들어, DSP와 마이크로프로세서의 조합, 복수의 마이크로프로세서들의 조합, DSP 코어와 결합한 하나 이상의 마이크로프로세서들의 조합, 또는 임의의 다른 그러한 구성들의 조합과 같은 처리 디바이스들의 조합을 지칭할 수도 있다. 또한, '메모리'는 전자 정보를 저장 가능한 임의의 전자 컴포넌트를 포함하도록 넓게 해석되어야 한다. '메모리'는 임의 액세스 메모리(RAM), 판독-전용 메모리(ROM), 비-휘발성 임의 액세스 메모리(NVRAM), 프로그램가능 판독-전용 메모리(PROM), 소거-프로그램가능 판독 전용 메모리(EPROM), 전기적으로 소거가능 PROM(EEPROM), 플래쉬 메모리, 자기 또는 광학 데이터 저장장치, 레지스터들 등과 같은 프로세서-판독가능 매체의 다양한 유형들을 지칭할 수도 있다. 프로세서가 메모리로부터 정보를 판독하고/하거나 메모리에 정보를 기록할 수 있다면 메모리는 프로세서와 전자 통신 상태에 있다고 불린다. 프로세서에 집적된 메모리는 프로세서와 전자 통신 상태에 있다.

[0031] 본 개시에서, '시스템'은 서버 장치와 클라우드 장치 중 적어도 하나의 장치를 포함할 수 있으나, 이에 한정되는 것은 아니다. 예를 들어, 시스템은 하나 이상의 서버 장치로 구성될 수 있다. 다른 예로서, 시스템은 하나 이상의 클라우드 장치로 구성될 수 있다. 또 다른 예로서, 시스템은 서버 장치와 클라우드 장치가 함께 구성되어 동작될 수 있다.

[0032] 본 개시에서, '디스플레이'는 컴퓨팅 장치와 연관된 임의의 디스플레이 장치를 지칭할 수 있는데, 예를 들어, 컴퓨팅 장치에 의해 제어되거나 컴퓨팅 장치로부터 제공된 임의의 정보/데이터를 표시할 수 있는 임의의 디스플레이 장치를 지칭할 수 있다.

[0033] 본 개시에서, '복수의 A의 각각' 또는 '복수의 A 각각'은 복수의 A에 포함된 모든 구성 요소의 각각을 지칭하거나, 복수의 A에 포함된 일부 구성 요소의 각각을 지칭할 수 있다.

[0034] 도 1은 본 개시의 일 실시예에 따른 전자 서명 시스템(100)의 구성도이다. 도시된 바와 같이, 전자 서명 시스템(100)은 사용자 단말(110), 메타버스 서버(120) 및/또는 전자서명 인증 서버(130)를 포함할 수 있다. 전자 서명 시스템(100)은 네트워크를 통해 메타버스 환경에서의 전자서명 서비스를 제공할 수 있는 시스템(들)을 포함할 수 있다. 일 실시예에서, 전자 서명 시스템(100)은 메타버스 환경에서의 전자서명 서비스와 관련된 컴퓨터 실행 가능한 프로그램(예를 들어, 다운로드 가능한 어플리케이션) 및 데이터를 저장, 제공 및 실행할 수 있는 하나 이상의 서버 장치 및/또는 데이터베이스, 또는 클라우드 컴퓨팅 서비스 기반의 하나 이상의 분산 컴퓨팅 장치 및/또는 분산 데이터베이스를 포함할 수 있다. 예를 들어, 전자 서명 시스템(100)은 메타버스 환경에서의 전자서명 서비스를 제공하기 위한 별도의 시스템(예를 들어, 서버)들을 포함할 수 있다. 일 실시예에서, 전자 서명 시스템(100)은 메타버스 환경에서 전자서명을 할 수 있는 메타버스 플랫폼이 구현된 서버의 일부일 수 있다. 또한, 일 실시예에서, 전자 서명 시스템(100)은 메타버스 환경에서의 전자서명 서비스를 제공할 수 있으며, 메타버스 환경에서의 전자서명 인증 동작이 구현된 서버의 일부일 수 있다.

[0035] 일 실시예에서, 전자서명 인증 서버(130)에 의해 제공되는 전자서명 인증 동작은 사용자 단말(110)에 설치된 메타버스 플랫폼 어플리케이션, 상점 서비스 어플리케이션, 금융 플랫폼 어플리케이션, 웹 브라우저 어플리케이션

등을 통해 사용자에게 제공될 수 있다.

[0036] 사용자 단말(110)은 네트워크를 통해 메타버스 서버(120) 및 전자서명 인증 서버(130)와 통신할 수 있다. 네트워크는 사용자 단말(110), 메타버스 서버(120) 및 전자서명 인증 서버(130) 사이의 통신이 가능하도록 구성될 수 있다. 네트워크는 설치 환경에 따라, 예를 들어, 이더넷(Ethernet), 유선 홈 네트워크(Power Line Communication), 전화선 통신 장치 및 RS-serial 통신 등의 유선 네트워크, 이동통신망, WLAN(Wireless LAN), Wi-Fi, Bluetooth 및 ZigBee 등과 같은 무선 네트워크 또는 그 조합으로 구성될 수 있다. 통신 방식은 제한되지 않으며, 네트워크가 포함할 수 있는 통신망(일례로, 이동통신망, 유선 인터넷, 무선 인터넷, 방송망, 위성망 등)을 활용하는 통신 방식뿐 아니라 사용자 단말(110) 사이의 근거리 무선 통신 역시 포함될 수 있다.

[0037] 사용자 단말(110)은 휴대폰 단말, 태블릿 단말 및 PC 단말 등의 사용자 단말일 수 있으나, 이에 한정되지 않는다. 사용자 단말(110)은 유선 및/또는 무선 통신이 가능한 임의의 컴퓨팅 장치일 수 있다. 예를 들어, 사용자 단말(110)은, 스마트폰, 휴대폰, 내비게이션, 컴퓨터, 노트북, 디지털방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC, 게임 콘솔(game console), 웨어러블 디바이스(wearable device), IoT(internet of things) 디바이스, VR(virtual reality) 디바이스, AR(augmented reality) 디바이스 등을 포함할 수 있다.

[0038] 일 실시예에서, 전자서명 인증 서버(130)는 사용자 단말(110)로부터 메타버스 환경의 로그인을 위한 인증서와 연관된 제1 개인 식별 정보 및 메타버스 환경에서 사용하기 위한 전자서명 원문 요청 정보를 수신하고, 메타버스용 개인키 및 공개키의 키 쌍을 생성하고, 제1 개인 식별 정보를 기초로 개인키를 암호화하여 저장하고, 사용자 단말(110)로 메타버스용 공개키를 포함한 전자서명 원문을 전송하고, 사용자 단말(110)로부터 전자서명의 검증 요청을 수신한 메타버스 서버(120)로부터, 전자서명의 검증 요청을 수신하고, 전자서명의 검증을 수행하여 전자서명의 검증이 정상적으로 완료되면, 전자서명의 검증 결과 및 인증서에 대응하는 고객 ID를 메타버스 서버(120)로 전송할 수 있다. 이와 같은 동작을 거쳐, 메타버스 환경에서 고객 ID에 대응하는 아바타가 활성화될 수 있다.

[0039] 도 2 및 도 3은 본 개시의 일 실시예에 따른 메타버스 환경에서 전자서명을 위한 개인키-공개키 키쌍 생성 방법을 나타내는 흐름도이다. 일 실시예에서, 메타버스 환경에서 전자서명을 위한 개인키-공개키 키쌍 생성 방법은 사용자 단말(420), 보안 모듈(430), 메타버스 서버(440), 아바타(450) 및 전자서명 인증 서버(460)에 의해 수행될 수 있다. 도 2에 도시된 바와 같이, 메타버스 환경에서 전자서명을 위한 개인키-공개키 키쌍 생성 방법은 사용자(410)가 사용자 단말(420)에 인증서 로그인을 요청함으로써 개시될 수 있다(412).

[0040] 사용자 단말(420)은 인증서 로그인을 요청한 사용자(410)에게 개인 식별 정보 입력 화면을 디스플레이할 수 있다(422). 사용자(410)는 인증서 기반 로그인을 위해, 디스플레이된 개인 식별 정보 입력 화면을 통해 개인 식별 정보를 입력할 수 있다(414). 여기서, 개인 식별 정보 입력 동작(414)은 인증서 일련번호 요청 동작(424) 이후에 수행될 수 있다. 예를 들어, 사용자(410)는 인증서 기반 로그인을 위해 인증서의 PIN(Personal Identification Number) 번호를 입력할 수 있다. 여기서, 개인 식별 정보는 PIN 번호로 한정되지 않으며, PIN 번호, 패턴 정보 또는 생체 인식 정보 등을 포함할 수 있다. 여기서, 생체 인식 정보는 지문 정보, 얼굴 정보, 홍채 정보, 망막 정보 및 정맥 정보를 포함할 수 있다.

[0041] 사용자 단말(420)은 사용자 단말(420) 내의 보안 모듈(430)에 인증서 일련번호를 요청할 수 있다(424). 여기서, 인증서 일련번호 요청 동작(424)은 사용자 단말(420) 내에 존재하는 하나 이상의 인증서를 조회하는 동작을 나타낼 수 있다. 보안 모듈(430)은 요청된 하나 이상의 인증서의 일련번호를 사용자 단말(420)로 전송할 수 있다(432). 예를 들어, 사용자 단말(420)은 사용자 단말에 설치된 보안 모듈(430)을 이용하여 인증서의 일련번호를 획득할 수 있다.

[0042] 사용자 단말(420)은 전자서명 인증 서버(460)에 전자서명 원문을 요청할 수 있다(426). 여기서, 사용자 단말(420)은 전자서명 원문의 요청 시, 인증서 일련번호 및 사용자(410)가 입력한 개인 식별 정보(예컨대, PIN 번호 등)를 전자서명 원문 요청 정보와 함께 전송할 수 있다. 이 경우, 사용자 단말(420)은 인증서 일련번호 및 개인 식별 정보(예컨대, PIN 번호 등)와 대응되는 해시(Hash) 정보를 생성하여 전자서명 인증 서버(460)로 전송하고, 구간 암호화를 적용함으로써 인증서 일련번호와 개인 식별 정보를 안전하게 전송할 수 있다.

[0043] 전자서명 인증 서버(460)는 수신한 인증서 일련번호를 기초로 해당 인증서 일련번호의 상태를 조회할 수 있다(462). 그 후, 전자서명 인증 서버(460)는 사용자 단말(420)로부터 수신한 개인 식별 정보를 검증할 수 있다(464). 검증이 완료된 경우, 전자서명 인증 서버(460)는 사용자(410)가 메타버스 환경에 로그인하는 동안 사용

할 수 있는 개인키 및 공개키의 키 쌍을 생성할 수 있다(466). 여기서, 개인키 및 공개키의 키 쌍은 사용자(410)가 메타버스 환경에 로그인하는 동안만 유효하고, 로그아웃 하는 경우 무효화되는 일회용 개인키 및 공개키의 키 쌍을 지칭할 수 있으나, 이에 한정되지 않는다.

[0044] 이후, 전자서명 인증 서버(460)는 사용자(410)가 입력한 개인 식별 정보를 이용하여 개인키를 암호화하여 안전하게 저장할 수 있다(468). 여기서, 전자서명 인증 서버(460)는 암호화 표준인 PBKDF2 기반으로 개인키를 암호화할 수 있으나, 이에 한정되지 않는다. 즉, 암호화 방법은 다양하게 적용될 수 있다. 예를 들어, 전자서명 인증 서버(460)는 개인키를 HSM(Hardware Security Module) 하드웨어 장비에 저장하거나, 블록체인에 저장할 수 있다.

[0045] 그리고 전자서명 인증 서버(460)는 전자서명 원문인 공개키와 인증서의 일련번호 상태 정보를 사용자 단말(420)로 전송할 수 있다(470).

[0046] 이와 같이, 도 2는 사용자(410)가 메타버스 서버(440)에 로그인을 하기 위하여 입력하는 개인 식별 정보를 이용하여, 전자서명 인증 서버(460)가 메타버스에서 사용할 개인키-공개키 키쌍을 생성하는 동작을 설명하였다. 이하에서는, 사용자 단말(420)이 메타버스에서 사용할 공개키에 전자서명하고, 전자서명 인증 서버(460)가 해당 전자서명을 검증한 후, 검증 결과를 사용자 단말(420) 및 메타버스 서버(440)로 전송하는 동작을 설명한다.

[0047] 도 3에 도시된 바와 같이, 사용자 단말(420)은 사용자 단말에 설치된 보안 모듈(430)로 전자서명 원문인 공개키에 대한 전자서명 요청을 전송할 수 있다(522). 보안 모듈(430)은 전자서명 원문인 공개키에 대한 전자서명 값을 사용자 단말(420)로 리턴할 수 있다(532). 여기서, 전자서명 값은 PKCS#7 전자서명 표준 값을 지칭할 수 있으나, 이에 한정되지 않는다. 예를 들어, 전자서명 값은 JWT(JSON Web Token) 방식을 이용하여 전자적으로 서명될 수 있다.

[0048] 사용자 단말(420)은 메타버스 서버(440)로 전자서명 값을 전송하여 검증을 요청할 수 있다(524). 메타버스 서버(440)는 사용자 단말(420)로부터 수신한 전자서명 값을 전자서명 인증 서버(460)로 전송하여 전자서명의 검증을 요청할 수 있다(542).

[0049] 전자서명 인증 서버(460)는 수신한 전자서명 값을 검증할 수 있다(562). 검증이 완료된 경우, 전자서명 인증 서버(460)는 전자서명 값에 대한 검증 결과 및 인증서에 해당하는 고객ID를 메타버스 서버(440)로 전송할 수 있다(564). 메타버스 서버(440)는 수신한 전자서명에 대한 검증 결과를 사용자 단말(420)로 전송할 수 있다(544). 상술한 바와 같이, 전자서명 인증 서버(460)에 의한 전자서명 검증 동작이 수행될 수 있다. 전자서명 검증 동작은 전자서명 인증 서버(460)가 미리 발급한 개인키가 사용자 단말(420)에 존재하는 사실 및 발급된 개인키를 이용하여 전자서명 원문(예, 공개키)을 전자서명한 사실을 검증하는 동작을 나타낼 수 있다. 전자서명 검증이 완료되면, 사용자 단말(420)은 전자서명 인증 서버(460)로부터 수신한 전자서명의 검증 결과 및 고객ID를 메타버스 서버(440)로 전송할 수 있다.

[0050] 이와 같이, 도 3은 사용자 단말(420) 및 보안 모듈(430)이 메타버스에 사용할 공개키에 전자서명을 하고, 전자서명 인증 서버(460)가 전자서명을 검증한 후, 검증 결과를 사용자 단말(420) 및 메타버스 서버(440)로 전송하는 동작을 설명하였다.

[0051] 도 2 및 도 3에 도시된 412 내지 546 동작을 통해, 사용자(410)는 메타버스 서버에 로그인을 완료할 수 있다. 예를 들어, 사용자(410)가 개인 식별 정보(예컨대, PIN 입력)를 입력하면, 사용자 단말(420), 전자서명 인증 서버(460) 및 메타버스 서버(440) 간의 로그인 동작 프로세스가 수행될 수 있다. 사용자(410)는 도 2 및 도 3에 도시된 412 내지 544 동작을 통해 로그인 동작을 완료할 수 있다.

[0052] 그리고 메타버스 서버(440)는 인증서 기반 로그인에 성공하였으므로 사용자(410)의 아바타(450)를 활성화하여 사용자 단말(420)을 통해 보여줄 수 있다(546). 사용자(410)는 546 동작을 통해 아바타(450)를 생성 또는 활성화할 수 있다.

[0053] 도 4 및 도 5는 본 개시의 일 실시예에 따른 메타버스 환경에서의 전자서명 처리 방법을 나타내는 흐름도이다. 일 실시예에서, 메타버스 환경에서의 전자서명 처리 방법은 메타버스 서버(440) 및 전자서명 인증 서버(460)에 의해 수행될 수 있다. 도 4에 도시된 바와 같이, 메타버스 환경에서의 전자서명 처리 방법은 메타버스 환경 상의 아바타(450)가 메타버스의 상점에서 물건을 구매하기 위해 상점(670)으로 전자서명을 요청을 전송함으로써 개시될 수 있다(652).

[0054] 상점(670)은 수신한 구매 서면 요청을 기초로 구매 서명 원문을 생성할 수 있다(672). 그 후, 상점(670)은 생

성된 구매 서명 원문을 아바타(450)에게 전송할 수 있다(674). 그리고 나서, 아바타(450)는 수신한 구매 서명 원문을 메타버스 서버(440)로 전송하여 구매 전자서명을 요청할 수 있다(654). 여기서, 상점(670)은 메타버스 환경 내에서 아바타(450)에게 물건(또는 아이템)을 판매할 수 있는 가상의 상점을 지칭할 수 있으며, 상점(670)은 메타버스 환경 내에서 물건 등을 판매 서비스를 제공하는 현실 세계의 서비스 제공자와 연관될 수 있다.

[0055] 메타버스 서버(440)는 사용자(410)에게 개인 식별 정보 입력 화면을 제공할 수 있다(642). 사용자(410)는 제공받은 개인 식별 정보 입력 화면을 통해 개인 식별 정보를 입력하여 메타버스 서버(440)로 전송할 수 있다(612). 여기서, 개인 식별 정보 입력 방식은 도 2에서 사용된 로그인 방식과 동일한 인증 방식이 적용될 수 있다. 예를 들어, 도 2에서 개인 식별 정보로 PIN 번호가 사용되었다면 도 4에서도 동일한 PIN 번호의 인증 방식이 적용될 수 있다.

[0056] 도 5에 도시된 바와 같이, 메타버스 서버(440)는 구매 서명 원문과 개인 식별 정보를 전자서명 인증 서버(460)로 전송하여 전자서명을 요청할 수 있다(742).

[0057] 전자서명 인증 서버(460)는 개인 식별 정보를 이용하여 메타버스용 개인키를 활성화할 수 있다(762). 전자서명 인증 서버(460)는 활성화된 메타버스용 개인키로 구매 서명 원문에 서명하여(764), 전자서명 값을 생성할 수 있다. 전자서명 인증 서버(460)는 메타버스용 공개키를 이용하여 생성된 전자서명 값을 검증할 수 있다(766). 검증이 완료되면, 전자서명 인증 서버(460)는 전자서명 결과를 메타버스 서버(440)로 전송할 수 있다(768).

[0058] 메타버스 서버(440)는 전자서명 결과를 아바타(450)에 전달할 수 있다(742). 구매를 위한 전자서명 값의 검증 결과가 정상일 경우, 아바타(450)가 구매를 위한 전자서명이 성공하였음을 표현할 수 있다(752).

[0059] 이와 같이, 사용자(410)는 아바타(450)를 이용하여 메타버스 상에서 구매 행위를 하는 경우, 전자서명을 이용하여 본인 인증을 수행할 수 있다.

[0060] 도 4 및 도 5는 메타버스 환경에서의 전자서명 처리 방법이 상점(670)으로 물품 구매를 위한 전자서명의 요청에 의해 개시된 것으로 도시되었으나, 이에 한정되지 않는다. 예를 들어, 메타버스 환경에서의 전자서명 은 메타버스 환경 내에서 보험 상품의 구매, 뱅킹 업무와 연관된 계좌조회, 출금 및 이체 등과 같은 사용자 인증이 필요한 작업에 적용될 수 있다. 일 실시예에서, 메타버스 환경에서의 전자서명 방법은 메타버스 환경에서 사용자와 연관된 아바타가 취득한 자격증을 증명하기 위한 인증서에 적용될 수 있다. 구체적으로, 도 2의 466 동작에서 생성된 메타버스용 개인키 및 공개키의 키 쌍을 이용하여, 메타버스용 공개키를 블록체인에 저장하고, 분산 신원증명(DID)을 발급받음으로써 자격증을 취득한 것을 등록할 수 있다. 일 실시예에서, 전자서명 처리 방법은 금융 분야에도 적용될 수 있다. 예를 들어, 가상의 메타버스 환경에서 실제(real) 계좌를 조회하고 메타버스 내 계좌로 이체를 수행할 수 있으며, 이 경우, 메타버스 환경에서의 전자서명 방법을 이용하여 전자서명을 이용한 사용자 인증을 수행할 수 있다.

[0061] 도 6은 본 개시의 일 실시예에 따른 메타버스 환경에서의 전자서명 방법(600)을 나타내는 흐름도이다. 일 실시예에서, 메타버스 환경에서의 전자서명 방법(600)은 프로세서(예를 들어, 전자 서명 시스템의 적어도 하나의 프로세서)에 의해 수행될 수 있다.

[0062] 도시된 바와 같이, 전자서명 방법(600)은 프로세서가 사용자 단말로부터 메타버스 환경의 로그인을 위한 인증서와 연관된 제1 개인 식별 정보 및 메타버스 환경에서 사용하기 위한 전자서명 원문 요청 정보를 수신함으로써 개시될 수 있다(S610). 여기서, 메타버스 환경으로 로그인하기 위한 인증서는 일련번호를 포함할 수 있으며, 제1 개인 식별 정보는 PIN 번호, 패턴 정보 또는 생체 인식 정보 중 하나를 포함할 수 있다.

[0063] 그리고 나서, 프로세서는 메타버스용 개인키 및 공개키의 키 쌍(key pair)을 생성할 수 있다(S620). 구체적으로, 프로세서는 일련번호를 이용하여 인증서의 상태를 조회할 수 있다. 인증서의 기한이 만기되지 않은 경우, 프로세서는 제1 개인 식별 정보를 검증할 수 있다. 제1 개인 식별 정보가 검증된 경우, 프로세서는 메타버스용 개인키 및 메타버스용 공개키의 쌍을 생성할 수 있다. 그 후, 프로세서는 제1 개인 식별 정보를 기초로 개인키를 암호화하여 저장할 수 있다(S630). 여기서, 프로세서는 제1 개인 식별 정보를 이용하여 메타버스용 개인키를 PBKDF2 방법으로 암호화할 수 있다.

[0064] 그 후, 프로세서는 사용자 단말로 메타버스용 공개키를 포함한 전자서명 원문을 전송할 수 있다(S640). 이 경우, 사용자 단말은 메타버스용 공개키를 포함한 전자서명 원문의 전자서명을 수행할 수 있다. 사용자 단말에 의해, 전자서명이 완료된 이후, 프로세서는 사용자 단말로부터 전자서명의 검증 요청을 수신한 메타버스 서버로부터, 전자서명의 검증 요청을 수신할 수 있다(S650).

[0065] 프로세서는 전자서명의 검증을 수행하여, 전자서명의 검증 결과 및 인증서에 대응하는 고객 ID를 메타버스 서버로 전송할 수 있다(S660). 이 때, 메타버스 환경에서 고객 ID에 대응하는 아바타가 활성화될 수 있다. 이 후, 고객 ID가 메타버스 환경에서 로그아웃되는 경우, 프로세서는 메타버스용 개인키 및 공개키 키 쌍을 무효화시킬 수 있다.

[0066] 도 7은 본 개시의 일 실시예에 따른 메타버스 환경 내에서 아바타의 구매 행위에 대한 구매 전자서명 방법(700)을 나타내는 흐름도이다. 일 실시예에서, 메타버스 환경 내에서 아바타의 구매 행위에 대한 구매 전자서명 방법(700)은 프로세서(예를 들어, 전자 서명 시스템의 적어도 하나의 프로세서)에 의해 수행될 수 있다.

[0067] 도시된 바와 같이, 구매 전자서명 방법(700)은 프로세서가 메타버스 서버로부터, 아바타가 활성화된 메타버스 환경 내에서 아바타의 구매 행위로 생성된 구매 서명 원문 및 사용자 단말로부터 메타버스 서버로 전송된 제2 개인 식별 정보를 수신함으로써 개시될 수 있다(S710). 여기서, 제2 개인 식별 정보는 PIN 번호, 패턴 정보 또는 생체 인식 정보 중 하나를 포함할 수 있다.

[0068] 제2 개인 식별 정보를 수신한 이후, 프로세서는 메타버스용 개인키를 이용하여 구매 서명 원문의 전자서명을 수행할 수 있다(S720). 구체적으로, 프로세서는 수신된 제2 개인 식별 번호를 기초로 메타버스용 개인키를 활성화할 수 있다. 이후, 활성화된 메타버스용 개인키를 이용하여, 프로세서는 구매 서명 원문의 전자서명을 수행할 수 있다.

[0069] 그리고 나서, 프로세서는 메타버스용 공개키를 이용하여, 전자서명의 검증을 수행하고(S730), 수행된 전자서명의 검증에 대한 결과를 메타버스 서버에 전송할 수 있다(S740).

[0070] 도 8은 본 개시의 일 실시예에 따른 전자서명 인증 서버 장치(800)의 구성도이다. 여기서, 전자서명 인증 서버 장치(800)는 하나 이상의 프로세서(810), 버스(830), 통신 인터페이스(840), 프로세서(810)에 의해 수행되는 컴퓨터 프로그램(860)을 로드(load)하는 메모리(820) 및 컴퓨터 프로그램(860)을 저장하는 저장 모듈(850)을 포함할 수 있다. 다만, 도 8에는 본 개시의 실시예와 관련 있는 구성요소들만이 도시되어 있다. 따라서, 본 개시가 속한 기술분야의 통상의 기술자라면 도 8에 도시된 구성요소들 외에 다른 범용적인 구성 요소들이 더 포함될 수 있음을 알 수 있다.

[0071] 프로세서(810)는 전자서명 인증 서버 장치(800)의 각 구성의 전반적인 동작을 제어한다. 프로세서(810)는 CPU(Central Processing Unit), MPU(Micro Processor Unit), MCU(Micro Controller Unit), GPU(Graphic Processing Unit) 또는 본 개시의 기술 분야에 잘 알려진 임의의 형태의 프로세서를 포함하여 구성될 수 있다. 또한, 프로세서(810)는 본 개시의 실시예들에 따른 방법을 실행하기 위한 적어도 하나의 애플리케이션 또는 프로그램에 대한 연산을 수행할 수 있다. 전자서명 인증 서버 장치(800)는 하나 이상의 프로세서를 구비할 수 있다.

[0072] 메모리(820)는 각종 데이터, 명령 및/또는 정보를 저장할 수 있다. 메모리(820)는 본 개시의 다양한 실시예들에 따른 방법/동작을 실행하기 위하여 저장 모듈(850)로부터 하나 이상의 컴퓨터 프로그램(860)을 로드할 수 있다. 메모리(820)는 RAM과 같은 휘발성 메모리로 구현될 수 있으나, 본 개시의 기술적 범위는 이에 한정되지 아니한다.

[0073] 버스(830)는 전자서명 인증 서버 장치(800)의 구성 요소 간 통신 기능을 제공할 수 있다. 버스(830)는 주소 버스(Address Bus), 데이터 버스(Data Bus) 및 제어 버스(Control Bus) 등 다양한 형태의 버스로 구현될 수 있다.

[0074] 통신 인터페이스(840)는 전자서명 인증 서버 장치(800)의 유무선 인터넷 통신을 지원할 수 있다. 또한, 통신 인터페이스(840)는 인터넷 통신 외의 다양한 통신 방식을 지원할 수도 있다. 이를 위해, 통신 인터페이스(840)는 본 개시의 기술 분야에 잘 알려진 통신 모듈을 포함하여 구성될 수 있다.

[0075] 저장 모듈(850)은 하나 이상의 컴퓨터 프로그램(860)을 비임시적으로 저장할 수 있다. 저장 모듈(850)은 ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리 등과 같은 비휘발성 메모리, 하드 디스크, 착탈형 디스크, 또는 본 개시가 속하는 기술 분야에서 잘 알려진 임의의 형태의 컴퓨터로 읽을 수 있는 기록 매체를 포함하여 구성될 수 있다.

[0076] 컴퓨터 프로그램(860)은 메모리(820)에 로드될 때 프로세서(810)로 하여금 본 개시의 다양한 실시예들에 따른 동작/방법을 수행하도록 하는 하나 이상의 인스트럭션들(instructions)을 포함할 수 있다. 즉, 프로세서(810)는 하나 이상의 인스트럭션들을 실행함으로써, 본 개시의 다양한 실시예들에 따른 동작/방법들을 수행할 수 있

다.

[0077] 예를 들어, 컴퓨터 프로그램(860)은 사용자 단말로부터 메타버스 환경의 로그인을 위한 인증서와 연관된 제1 개인 식별 정보 및 메타버스 환경에서 사용하기 위한 전자서명 원문 요청 정보를 수신하는 동작, 메타버스용 개인키 및 공개키의 키 쌍을 생성하는 동작, 제1 개인 식별 정보를 기초로 개인키를 암호화하여 저장하는 동작, 사용자 단말로 메타버스용 공개키를 포함한 전자서명 원문을 전송하는 동작, 사용자 단말로부터 전자서명의 검증 요청을 수신한 메타버스 서버로부터, 전자서명의 검증 요청을 수신하는 동작, 전자서명의 검증을 수행하여, 전자서명의 검증 결과 및 인증서에 대응하는 고객 ID를 메타버스 서버로 전송하는 동작 등을 수행하도록 하는 하나 이상의 인스트럭션들을 포함할 수 있다. 해당 동작이 완료되면, 메타버스 환경에서 고객 ID에 대응하는 아바타가 활성화될 수 있다. 이와 같은 경우, 전자서명 인증 서버 장치(800)를 통해 본 개시의 몇몇 실시예들에 따른 메타버스 환경에서의 전자서명하는 시스템이 구현될 수 있다.

[0078] 본 개시의 앞선 설명은 통상의 기술자들이 본 개시를 행하거나 이용하는 것을 가능하게 하기 위해 제공된다. 본 개시의 다양한 수정예들이 통상의 기술자들에게 쉽게 자명할 것이고, 본원에 정의된 일반적인 원리들은 본 개시의 취지 또는 범위를 벗어나지 않으면서 다양한 변형예들에 적용될 수도 있다. 따라서, 본 개시는 본원에 설명된 예들에 제한되도록 의도된 것이 아니고, 본원에 개시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위가 부여되도록 의도된다.

[0079] 비록 예시적인 구현예들이 하나 이상의 독립형 컴퓨터 시스템의 맥락에서 현재 개시된 주제의 양태들을 활용하는 것을 언급할 수도 있으나, 본 주제는 그렇게 제한되지 않고, 오히려 네트워크나 분산 컴퓨팅 환경과 같은 임의의 컴퓨팅 환경과 연계하여 구현될 수도 있다. 또 나아가, 현재 개시된 주제의 양상들은 복수의 프로세싱 칩들이나 디바이스들에서 또는 그들에 걸쳐 구현될 수도 있고, 스토리지는 복수의 디바이스들에 걸쳐 유사하게 영향을 받게 될 수도 있다. 이러한 디바이스들은 PC들, 네트워크 서버들, 및 핸드헬드 디바이스들을 포함할 수도 있다.

[0080] 본 명세서에서는 본 개시가 일부 실시예들과 관련하여 설명되었지만, 본 발명이 속하는 기술분야의 통상의 기술자가 이해할 수 있는 본 개시의 범위를 벗어나지 않는 범위에서 다양한 변형 및 변경이 이루어질 수 있다는 점을 알아야 할 것이다. 또한, 그러한 변형 및 변경은 본 명세서에서 첨부된 특허 청구의 범위 내에 속하는 것으로 생각되어야 한다.

부호의 설명

[0081] 100: 전자 서명 시스템

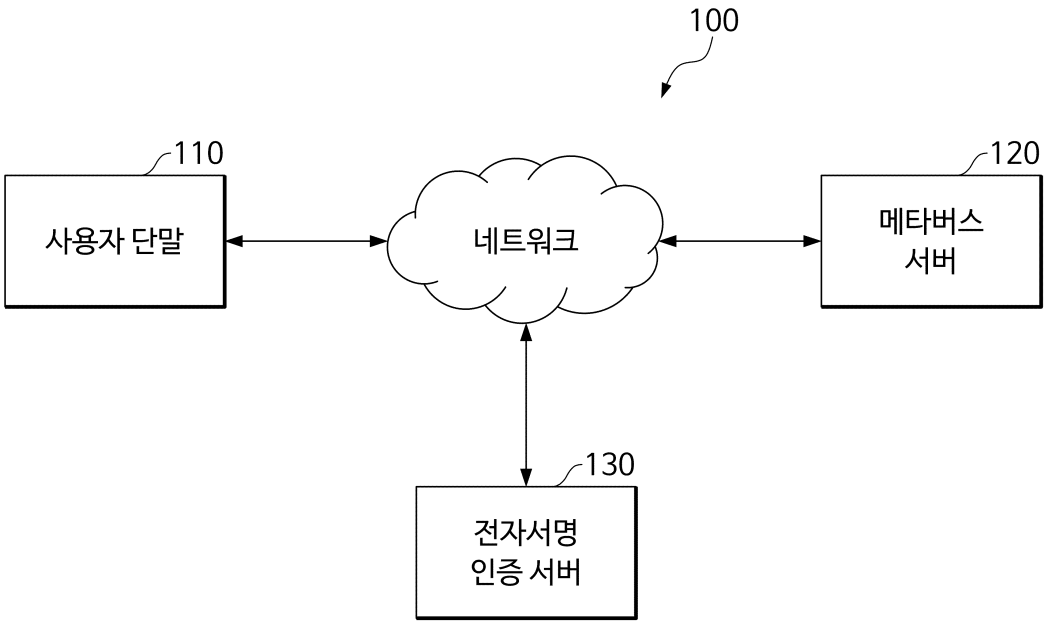
110: 사용자 단말

120: 메타버스 서버

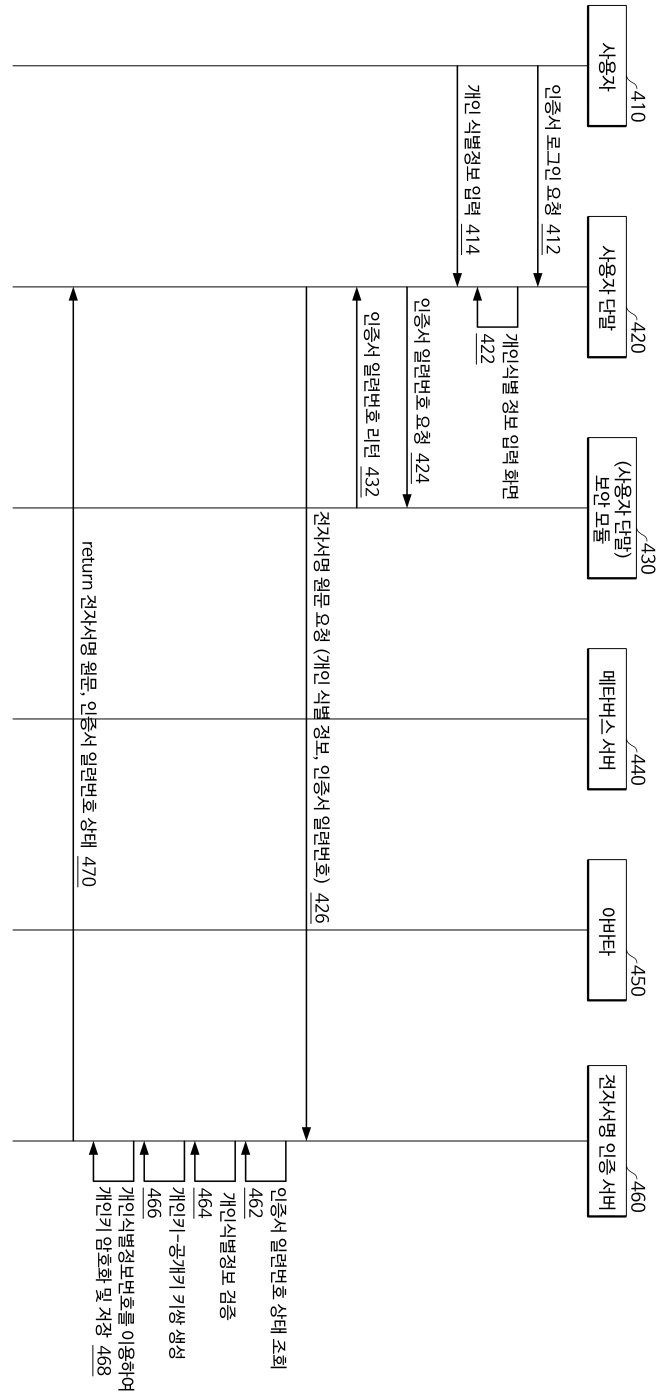
130: 전자서명 인증 서버

도면

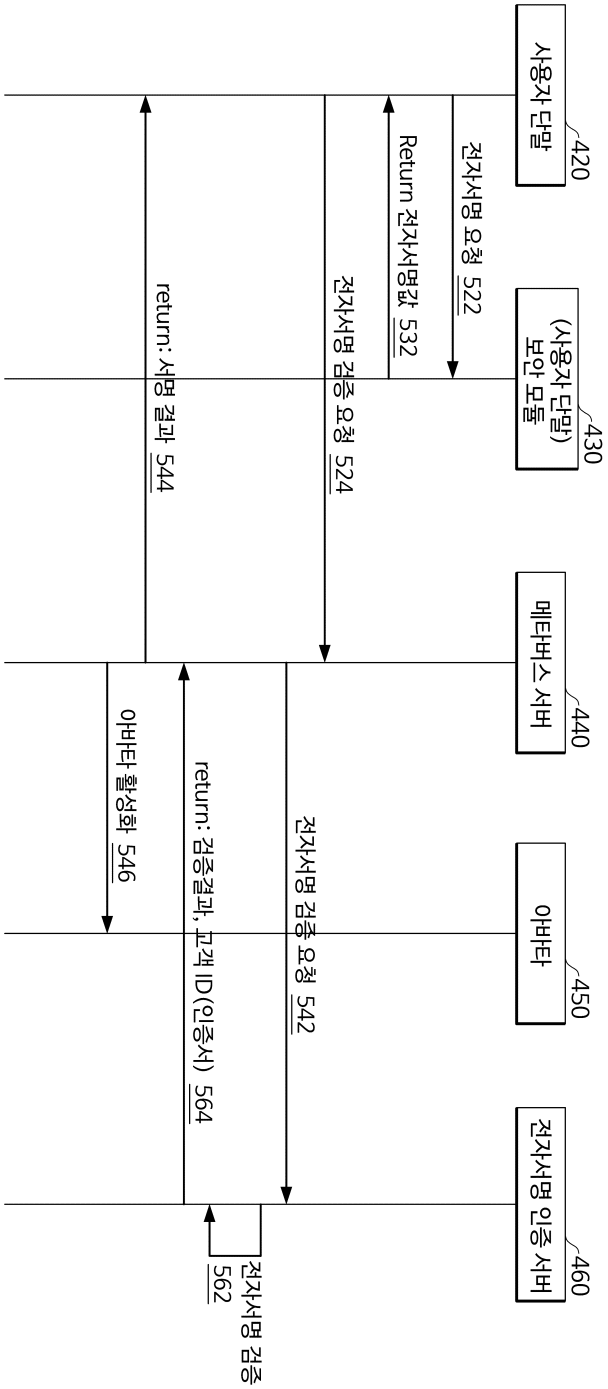
도면1



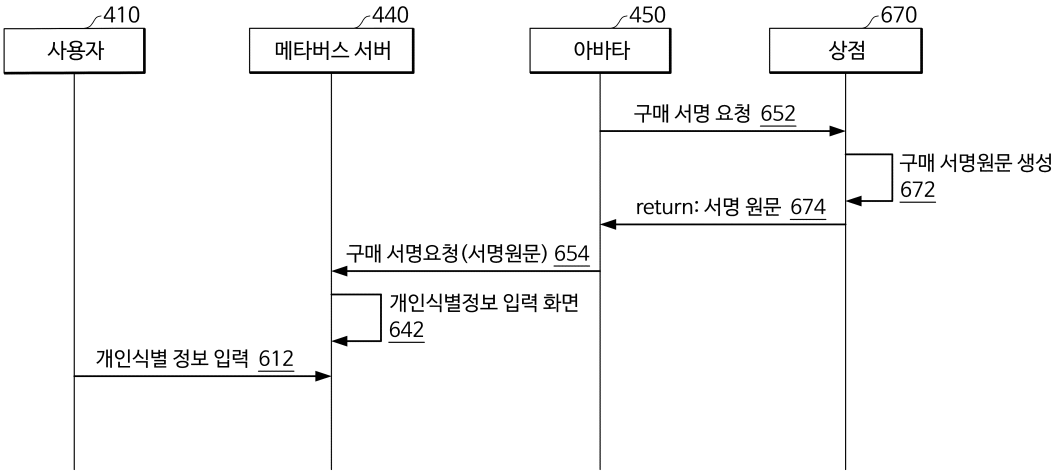
도면2


사용자 410
사용자 단말 420
(사용자 단말) 보안 모듈 430
메타버스 서버 440
아바타 450
전자서명 인증 서버 460
인증서 로그인 요청 412
개인 식별정보 입력 414
개인식별 정보 입력 화면 422
인증서 일련번호 요청 424
인증서 일련번호 리턴 432
전자서명 원문 요청 (개인 식별 정보, 인증서 일련번호) 426
return 전자서명 원문, 인증서 일련번호 상태 470
인증서 일련번호 상태 조회 462
개인식별정보 검증 464
개인키-공개키 키쌍 생성 466
개인식별정보번호를 이용하여 개인키 암호화 및 저장 468

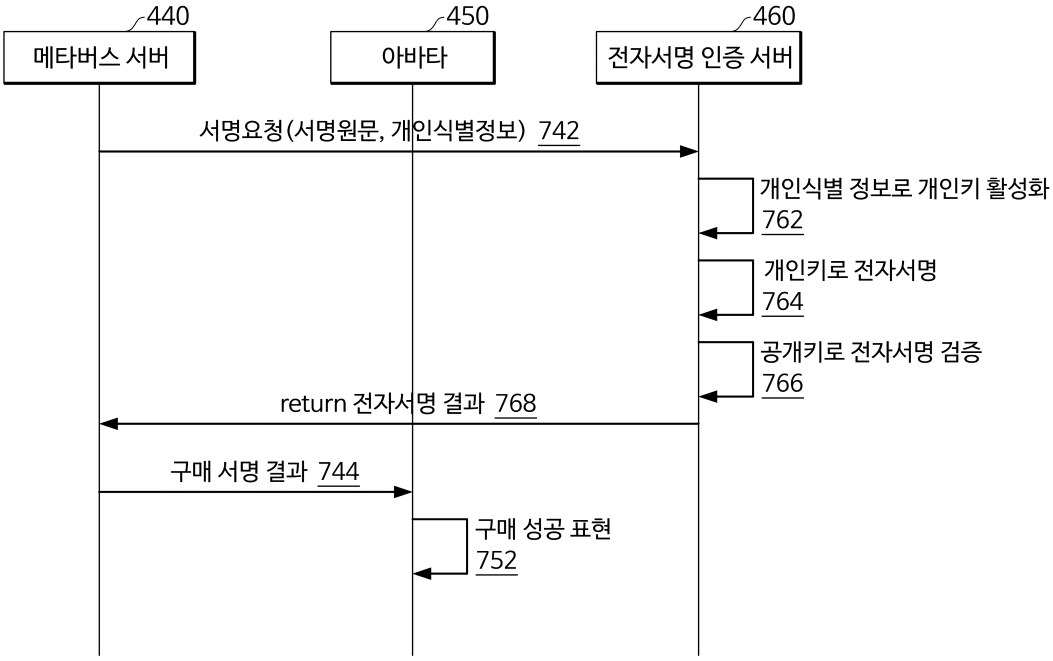
도면3


사용자 단말
420
(사용자 단말) 보안 모듈
430
메타버스 서버
440
아바타
450
전자서명 인증 서버
460
전자서명 요청 522
Return 전자서명값 532
전자서명 검증 요청 524
return: 서명 결과 544
아바타 활성화 546
전자서명 검증 요청 542
return: 검증결과, 고객 ID(인증서) 564
전자서명 검증 562

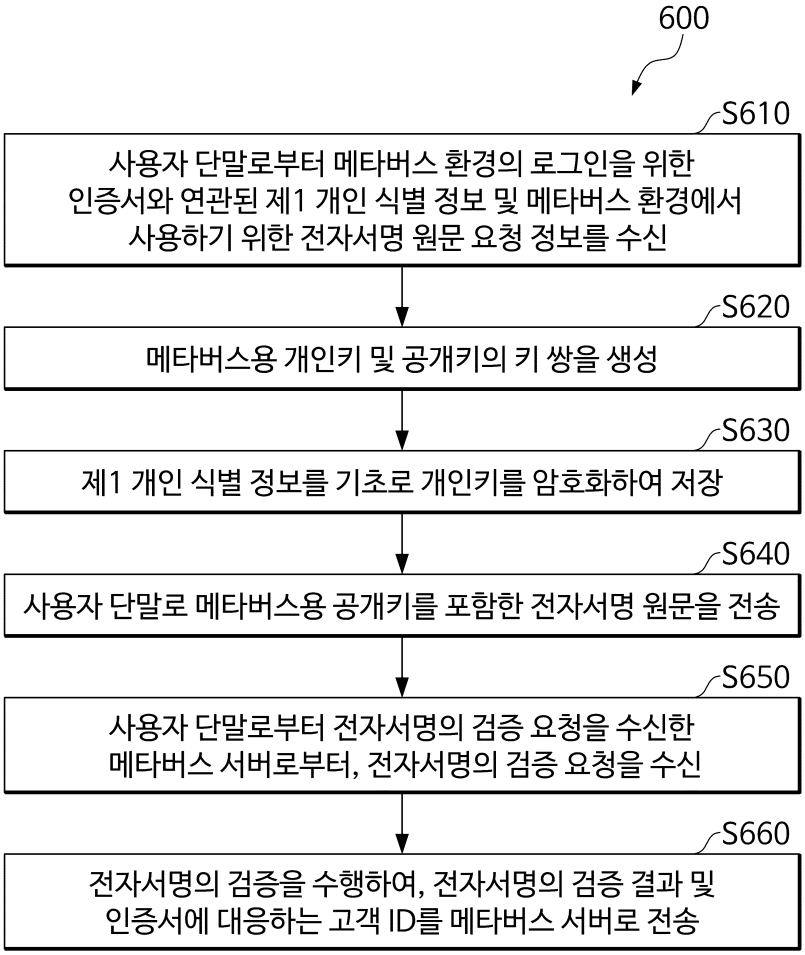
도면4


410
사용자
440
메타버스 서버
450
아바타
670
상점
구매 서명 요청 652
구매 서명원문 생성
672
return: 서명 원문 674
구매 서명요청(서명원문) 654
개인식별정보 입력 화면
642
개인식별 정보 입력 612

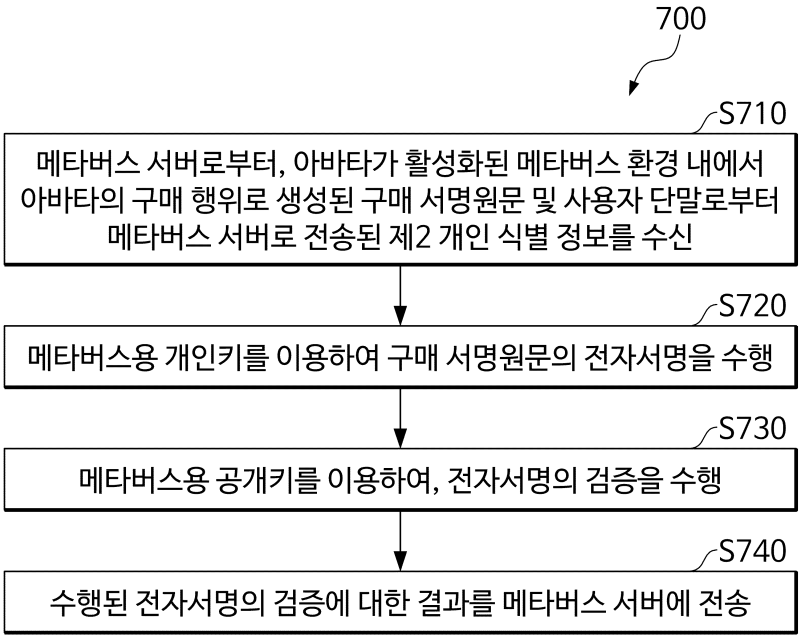
도면5


440
메타버스 서버
450
아바타
460
전자서명 인증 서버
서명요청(서명원문, 개인식별정보) 742
개인식별 정보로 개인키 활성화
762
개인키로 전자서명
764
공개키로 전자서명 검증
766
return 전자서명 결과 768
구매 서명 결과 744
구매 성공 표현
752

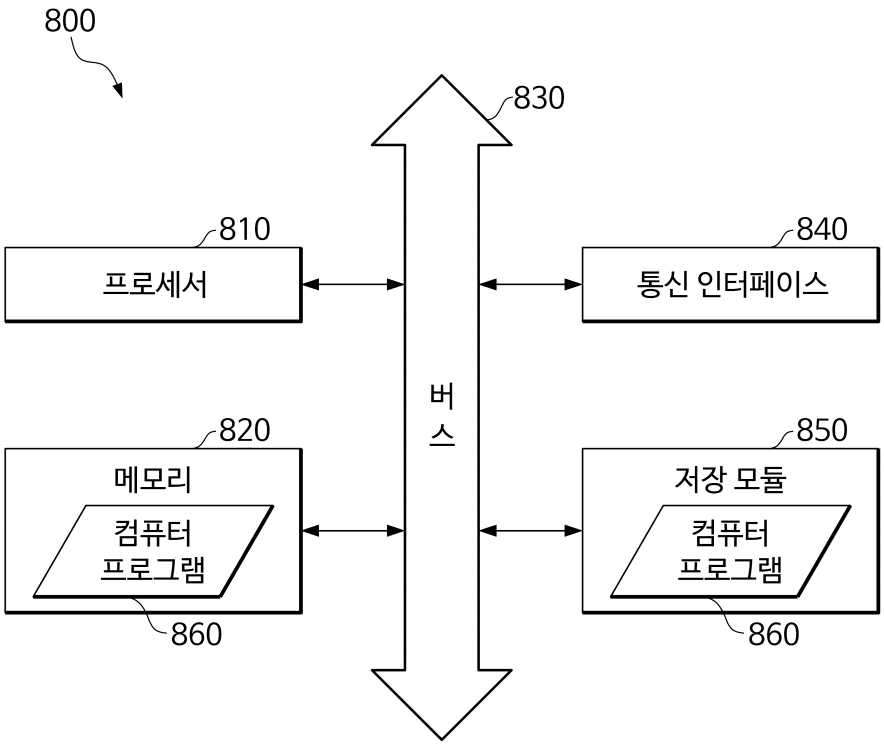
도면6


600
S610
사용자 단말로부터 메타버스 환경의 로그인을 위한 인증서와 연관된 제1 개인 식별 정보 및 메타버스 환경에서 사용하기 위한 전자서명 원문 요청 정보를 수신
S620
메타버스용 개인키 및 공개키의 키 쌍을 생성
S630
제1 개인 식별 정보를 기초로 개인키를 암호화하여 저장
S640
사용자 단말로 메타버스용 공개키를 포함한 전자서명 원문을 전송
S650
사용자 단말로부터 전자서명의 검증 요청을 수신한 메타버스 서버로부터, 전자서명의 검증 요청을 수신
S660
전자서명의 검증을 수행하여, 전자서명의 검증 결과 및 인증서에 대응하는 고객 ID를 메타버스 서버로 전송

도면7


700
S710
메타버스 서버로부터, 아바타가 활성화된 메타버스 환경 내에서 아바타의 구매 행위로 생성된 구매 서명원문 및 사용자 단말로부터 메타버스 서버로 전송된 제2 개인 식별 정보를 수신
S720
메타버스용 개인키를 이용하여 구매 서명원문의 전자서명을 수행
S730
메타버스용 공개키를 이용하여, 전자서명의 검증을 수행
S740
수행된 전자서명의 검증에 대한 결과를 메타버스 서버에 전송

도면8


800
830
810
프로세서
840
통신 인터페이스
버
스
820
메모리
컴퓨터
프로그램
860
850
저장 모듈
컴퓨터
프로그램
860