(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0101429
(43) 공개일자 2022년07월19일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 21/33* (2013.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3263 (2013.01)
G06F 21/33 (2013.01)
(21) 출원번호 10-2021-0003442
(22) 출원일자 2021년01월11일
심사청구일자 2021년01월11일

(71) 출원인
서울외국어대학원대학교 산학협력단
서울특별시 서초구 남부순환로356길 85 (양재동, 서울외국어대학원대학교내)
이지스체인 주식회사
서울특별시 서초구 남부순환로356길 85 ,1408호 (양재동)
(72) 발명자
박근덕
서울특별시 송파구 삼학사로6길 9, 202호 (석촌동)
(74) 대리인
김보정

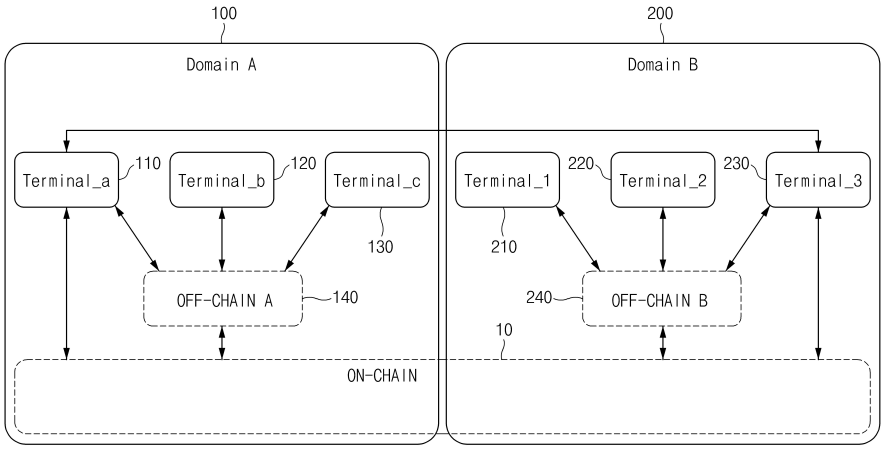
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 **무선 통신을 이용한 개인간 비대면 신원 확인 시스템**

(57) 요 약

무선 통신을 이용한 개인간 비대면 신원 확인 시스템이 개시된다. 본 발명의 비대면 신원 확인 시스템은, 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제1 증명서와 제2단말기로부터 해당 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제2 증명서를 상호 교환하고, 수신한 증명서를 온오프체인에 등록된 각 단말기의 공개키로 검증한 다음 검증한 증명서와 자체 생성한 증명서를 결합하여 통합 증명서를 생성하게 구성함으로써, 전자 서명된 확인증을 서로 교환하여 온오프체인에 등록된 공개키로 검증을 할 수 있기 때문에 비대면으로 검증된 증명서를 주고받을 수 있다.

대 표 도



(52) CPC특허분류
H04L 9/0825 (2013.01)
H04L 9/0877 (2013.01)
H04L 9/50 (2022.05)
H04L 2209/80 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711126060
과제번호	2019-0-00660-003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송표준개발지원(R&D,정보화)
연구과제명	차세대 ICT 환경에서의 보안 및 개인정보보호 기술 국제 표준화 추진
기 여 율	1/1
과제수행기관명	순천향대학교산학협력단
연구기간	2021.01.01 ~ 2021.12.31

명 세 서

청구범위

청구항 1

오프체인(OFF-CHAIN) 또는 온체인(ON-CHAIN)에 이용자 식별자, 공개키, 암호키 사본, 및 단말기 식별자를 포함하는 이용자 등록정보 중 어느 하나 이상을 등록하고, 이용자 등록정보를 등록한 단말기간에 전자서명된 증명서를 교환하도록 동작하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 있어서,

단말기 이용자의 이용자 식별자 및 개인키로 서명된 제1 증명서를 생성하여 근거리 통신을 통하여 제2단말기로 전송하고 상기 제2단말기로부터 해당 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제2 증명서를 수신하여 온오프체인에 등록된 제2단말기의 공개키로 수신한 제2 증명서를 검증하는 제1단말기;및

단말기 이용자의 이용자 식별자 및 개인키로 서명된 제2 증명서를 생성하여 근거리 통신을 통하여 제1단말기로 전송하고 제1 단말기로부터 해당 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제1 증명서를 수신하여 온오프체인에 등록된 제1단말기의 공개키로 수신한 제1 증명서를 검증하는 제2단말기;

를 포함하고,

상기 제1 단말기는 수신한 제2 증명서가 검증되면 상기 제1 증명서와 상기 검증된 제2 증명서를 결합하여 공동서명한 통합 증명서를 생성하고, 상기 제2 단말기는 수신한 제1 증명서가 검증되면 제2 증명서와 검증된 제1 증명서를 결합하여 공동서명한 통합 증명서를 생성하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템.

청구항 2

청구항 1에 있어서,

상기 제1 또는 제2 단말기는

근거리 무선 통신을 수행하는 무선통신모듈;

해당 단말기 내 증명서, 개인키 그리고 암호키원본을 보관하고, 온오프체인에 등록된 타단말기의 공개키로 수신한 증명서를 검증하며, 해당 단말기의 이용자 식별자 및 개인키로 서명된 증명서를 상기 무선통신모듈을 통하여 타단말기로 전송하도록 동작하는 사용자앱부;및

상기 사용자앱부에서 타단말기에서 전송된 증명서가 검증되면, 해당 단말기에서 생성한 이용자 식별자 및 개인키로 서명된 증명서와 타단말기에서 수신한 검증된 증명서를 결합하여 각 단말기에서 공동 서명한 증명서를 단말기표시부에 표시하도록 제어하는 제어부;

를 포함하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템.

청구항 3

청구항 2에 있어서,

상기 사용자앱부는

암호키를 관리하는 암호키관리모듈;

상기 암호키관리모듈로부터 암호키를 제공받아 개인정보를 암호화 및 복호화하는 개인정보관리모듈;및

제1 또는 제2 증명서 생성시 개인정보관리모듈로부터 개인정보를 제공받음과 동시에 상기 암호키관리모듈로부터 개인키를 제공받아 전자서명된 증명서를 생성하고, 상기 무선통신모듈을 통하여 전자 서명된 제1 또는 제2 증명서를 수신 또는 발신하도록 동작하는 신원증명서 관리모듈;

을 포함하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템.

청구항 4

청구항 3에 있어서,

상기 통합 증명서가 수업 출석 증명서인 경우

상기 제1 단말기는 수강생이 소지하는 단말기이고, 상기 제2 단말기는 교수가 소지하는 단말기로서,

상기 제1 단말기는

과목명, 학번, 그리고 수강생 성명을 포함하는 출석확인증을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제2 단말기로 전송하고, 상기 제2 단말기에서 전자서명된 학교명, 과목명, 수업일시, 그리고 교수 성명을 포함하는 교수확인증을 수신하여 해당 교수의 공개키로 검증하고, 검증이 완료되면 상기 출석확인증에 상기 교수확인증을 결합하여 수업 출석 증명서를 생성하고,

상기 제2 단말기는

학교명, 과목명, 수업일시, 그리고 교수 성명을 포함하는 교수확인증을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제1 단말기로 전송하고, 상기 제1 단말기에서 전자서명이 첨부된 출석확인증을 수신하여 해당 수강생의 공개키로 검증하고, 검증이 완료되면 상기 출석확인증에 상기 교수확인증을 결합하여 수업 출석 증명서를 생성하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템.

청구항 5

청구항 3에 있어서,

상기 통합 증명서가 행사 참석 증명서인 경우

상기 제1 단말기는 참석자가 소지하는 단말기이고, 상기 제2 단말기는 주최자가 소지하는 단말기로서,

상기 제1 단말기는

행사명, 참석자 직장명, 그리고 참석자 성명을 포함하는 참석확인증을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제2 단말기로 전송하고, 상기 제2 단말기에서 전자서명된 행사명, 행사기간 그리고 주최자명을 포함하는 주최자 확인증을 수신하여 해당 주최자의 공개키로 검증하고, 검증이 완료되면 상기 참석확인증에 상기 주최자 확인증을 결합하여 행사 참석 증명서를 생성하고,

상기 제2 단말기는

행사명, 행사기간 그리고 주최자명을 포함하는 주최자 확인증 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제1 단말기로 전송하고, 상기 제1 단말기에서 전자서명이 첨부된 참석 확인증을 수신하여 해당 참석자의 공개키로 검증하고, 검증이 완료되면 상기 주최자 확인증에 상기 참석 확인증을 결합하여 행사 참석 증명서를 생성하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템.

청구항 6

청구항 3에 있어서,

상기 통합 증명서가 모임 참석 증명서인 경우

상기 제1 단말기는 참석자가 소지하는 단말기이고, 상기 제2 단말기는 주최자가 소지하는 단말기로서,

상기 제1 단말기는

모임명과 회원성명을 포함하는 참석확인증을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제2 단말기로 전송하고, 상기 제2 단말기에서 전자서명된 모임명, 모임일시, 그리고 주최자명을 포함하는 주최자 확인증을 수신하여 해당 주최자의 공개키로 검증하고, 검증이 완료되면 상기 참석확인증에 상기 주최자 확인증을 결합하여 모임 참석 증명서를 생성하고,

상기 제2 단말기는

모임명, 모임일시 그리고 주최자명을 포함하는 주최자 확인증 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제1 단말기로 전송하고, 상기 제1 단말기에서 전자서명이 첨부된 참석 확인증을 수신하여 해당 참석자의 공개키로 검증하고, 검증이 완료되면 상기 주최자 확인증에 상기 참석 확인증을 결합하여 모임 참석 증명서를 생성하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템.

청구항 7

청구항 3에 있어서,

상기 통합 증명서가 여행지 방문 증명서인 경우

상기 제1 단말기는 방문자가 소지하는 단말기이고, 상기 제2 단말기는 운영자가 소지하는 단말기로서,

상기 제1 단말기는

위치정보(위도/경도) 그리고 방문객 성명을 포함하는 방문 확인증을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제2 단말기로 전송하고, 상기 제2 단말기에서 전자서명된 방문장소, 방문일시, 그리고 운영자명을 포함하는 운영자 확인증을 수신하여 해당 운영자의 공개키로 검증하고, 검증이 완료되면 상기 방문확인증에 상기 운영자 확인증을 결합하여 여행지 방문 증명서를 생성하고,

상기 제2 단말기는

방문장소, 방문일시, 그리고 운영자명을 포함하는 운영자 확인증을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제1 단말기로 전송하고, 상기 제1 단말기에서 전자서명이 첨부된 방문 확인증을 수신하여 해당 방문자의 공개키로 검증하고, 검증이 완료되면 상기 운영자 확인증에 상기 방문 확인증을 결합하여 여행지 방문 증명서를 생성하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템.

청구항 8

청구항 3에 있어서,

상기 통합 증명서가 식음료 거래 증명서인 경우

상기 제1 단말기는 주문자가 소지하는 단말기이고, 상기 제2 단말기는 판매자가 소지하는 단말기로서,

상기 제1 단말기는

업소명, 주문일시/주문내역, 그리고 주문자 성명을 포함하는 주문 확인증을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제2 단말기로 전송하고, 상기 제2 단말기에서 전자서명된 업소명, 판매자 성명, 그리고 판매일시/결제금액을 포함하는 판매 확인증을 수신하여 해당 판매자의 공개키로 검증하고, 검증이 완료되면 상기 주문 확인증에 상기 판매 확인증을 결합하여 식음료 거래 증명서를 생성하고,

상기 제2 단말기는

업소명, 판매자 성명, 그리고 판매일시/결제금액을 포함하는 판매 확인증을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제1 단말기로 전송하고, 상기 제1 단말기에서 전자서명이 첨부된 주문 확인증을 수신하여 해당 주문자의 공개키로 검증하고, 검증이 완료되면 상기 판매 확인증에 상기 주문 확인증을 결합하여 식음료 거래 증명서를 생성하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템.

청구항 9

청구항 3에 있어서,

상기 통합 증명서가 디지털 명함인 경우

상기 제1 단말기와 상기 제2 단말기는 명함을 주고 받는 상대방의 단말기이고,

상기 제1 단말기는

직장명/부서명, 성명, 직장 전화번호, 휴대폰 번호, 이메일 주소 그리고 직장 주소를 포함하는 제1 디지털 명함을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제2 단말기로 전송하고, 상기 제2 단말기에서 전자서명된 직장명/부서명, 성명, 직장 전화번호, 휴대폰 번호, 이메일 주소 그리고 직장 주소를 포함하는 제2 디지털 명함을 수신하여 해당 제2 단말기 소지자의 공개키로 검증하고, 검증이 완료되면 상기 검증된 디지털 명함에 주고받은 일시를 결합하여 디지털 명함 증명서를 생성하고,

상기 제2 단말기는

직장명/부서명, 성명, 직장 전화번호, 휴대폰 번호, 이메일 주소 그리고 직장 주소를 포함하는 제2 디지털 명함을 생성하고 전자서명한 다음 상기 무선통신모듈을 통하여 상기 제1 단말기로 전송하고, 상기 제1 단말기에서 전자서명이 첨부된 제1 디지털 명함을 수신하여 해당 제1 단말기 소지자의 공개키로 검증하고, 검증이 완료되면 상기 검증된 디지털 명함에 주고받은 일시를 결합하여 디지털 명함 증명서를 생성하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 신원확인 시스템에 관한 것으로, 온오프 체인에 개인정보는 등록하지 않고 검증에 필요한 정보만 등록하여 개인의 단말기에서 각각의 공개키로 증명서를 검증하여 통합 증명서를 생성하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 관한 것이다.

배 경 기 술

[0002] 글로벌 블록체인 기반 신원 인증 시장은 2021년 101억달러(12조원)에서 2025년 252억달러(30조원) 규모로 2.5배 성장이 예상된다(출처: 헤럴드 경제).

[0003] 통상 신원인증의 4가지 범주는 간편인증, 본인인증, 자격증명, 사물인증으로 구별되는 데 간편인증은 현행 복잡한 인증 단계를 1~2단계로 간소화하는 것이며, 본인인증은 디지털 신분증처럼 플라스틱증명서 없이 신원확인 및 제출을 하는 것이고, 자격증명은 학생의 성적증명이나 직장인의 재직증명을 종이 서류없이 제출하는 것을, 그리고 사물인증은 항만컨테이너, 유기농 식품 등 사물에 ID를 부여해 원스톱 관리하는 것을 말한다.

[0004] 특히 탈중앙화 신원증명(DID;Decentralized Identifier)은 개인들이 본인 정보를 직접관리하고, 인증에 필요한 정보만 선택해 제출 가능하다는 점과 해킹을 통한 개인정보유출을 최소화한다는 점 그리고 기업들의 무단 개인정보 사용을 원천차단한다는 점에서 여러가지 장점이 있다.

[0005] Peer DID는 Pairwise DID 또는 N-wise DID를 의미하는 것으로서, Anywise DID처럼 불특정 다수를 대상으로 하는 공용(Global public) 신원 확인 목적이 아니기 때문에 특정 개인 간 신원 확인 및 프라이버시 보호에 유리하다.

[0006] 한편, 분산 ID나 사설 및 공동 인증서 등은 사업자가 발행하고 인터넷을 이용하여 원거리 비대면으로 증명서를 제출하는 방식이나, 법규정에 근거한 본인 실명확인이 필요한 분야 즉 금융 및 공공 서비스 등에 활용이 가능하기 때문에 개인 간 비대면 신원 확인 시스템에는 여러 가지 불편함으로 사용하지 못하는 문제점이 있다.

[0007] 즉, 특정 장소에 모인 다수의 사람들이 명함 교환 시 많은 시간이 소요되고, 명함 소진이나 명함 미지참 등 사유로 원활한 교환이 이루어지지 않는다는 문제점도 있고, 각종 행사(행사/워크샵/컨퍼런스/전시회) 및 모임(동호회/동문회/회의) 등에서 주최자가 다수 참석자의 현장 참석 여부를 확인하는데 많은 시간이 소요되고 줄서기 등이 불편하다는 문제점이 있다.

[0008] 또한, 학교 및 학원 등에서 교수가 다수 수강생의 대면 수업 출석 여부를 확인하는데 많은 시간이 소요되고, 식음료 매장에서 판매자가 다수 구매자의 주문/결제/픽업 여부를 확인하는데도 많은 시간이 소요된다.

[0009] 또한, 개인 간 신원 확인 시 포스트 코로나 시대에 맞는 사회적 거리 두기 (예: 개인 간 2M 이상 거리 두기) 실천이 어렵다는 문제점이 있다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) KR 공개특허공보 제10-2006-0032888호(2006.04.18)

발명의 내용

해결하려는 과제

[0011] 이러한 문제점을 해결하기 위한 본 발명은 무선통신을 이용하여 근거리에서 개인 간 신원을 확인할 수 있는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템을 제공하는 것을 목적으로 한다.

[0012] 또한, 본 발명은 이용자가 직접 필수 정보를 입력하여 생성된 증명서를 온오프체인상에 등록되어 있는 정보를 이용하여 검증할 수 있는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템을 제공하는 것을 다른 목적으로 한다.

[0013] 또한, 본 발명은 개인간 신원 확인 후 전자 서명된 증명서를 서로 발급 교환할 수 있는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템을 제공하는 것을 또 다른 목적으로 한다.

[0014] 그리고 본 발명은 온오프 체인에 개인정보는 등록하지 않고 이용자 식별자, 공개키, 암호키사본 및 단말기 식별자를 저장하고, 개인의 단말기에서 각각의 공개키로 증명서를 검증하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템을 제공하는 것을 또 다른 목적으로 한다.

과제의 해결 수단

[0015] 이러한 과제를 해결하기 위한 본 발명의 오프체인(OFF-CHAIN) 또는 온체인(ON-CHAIN)에 이용자 식별자, 공개키, 암호키 사본, 및 단말기 식별자를 포함하는 이용자 등록정보 중 어느 하나 이상을 등록하고, 이용자 등록정보를 등록한 단말기간에 서명된 증명서를 교환하도록 동작하는 무선 통신을 이용한 개인간 비대면 신원 확인 시스템은, 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제1 증명서를 생성하여 근거리 통신을 통하여 제2단말기로 전송하고 상기 제2단말기로부터 해당 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제2 증명서를 수신하여 온오프체인에 등록된 제2단말기의 공개키로 수신한 제2 증명서를 검증하는 제1단말기와, 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제2 증명서를 생성하여 근거리 통신을 통하여 제1단말기로 전송하고 제1단말기로부터 해당 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제1 증명서를 수신하여 온오프체인에 등록된 제1단말기의 공개키로 수신한 제1 증명서를 검증하는 제2단말기를 포함하고, 상기 제1 단말기는 수신한 제2 증명서가 검증되면 상기 제1 증명서와 상기 검증된 제2 증명서를 결합하여 공동서명한 통합 증명서를 생성하고, 상기 제2 단말기는 수신한 제1 증명서가 검증되면 제2 증명서와 검증된 제1 증명서를 결합하여 공동서명한 통합 증명서를 생성하게 구성함으로써 달성될 수 있다.

[0016] 상기 제1 또는 제2 단말기는 근거리 무선 통신을 수행하는 무선통신모듈과, 해당 단말기 내 증명서, 개인키 그리고 암호키원본을 보관하고, 온오프체인에 등록된 타단말기의 공개키로 수신한 증명서를 검증하며, 해당 단말기의 이용자 식별자 및 개인키로 서명된 증명서를 상기 무선통신모듈을 통하여 타단말기로 전송하도록 동작하는 사용자앱부, 및 상기 사용자앱부에서 타단말기로부터 전송된 증명서가 검증되면, 해당 단말기에서 생성한 이용자 식별자 및 개인키로 서명된 증명서와 타단말기로부터 수신한 검증된 증명서를 결합하여 각 단말기에서 공동서명한 증명서를 단말기표시부에 표시하도록 제어하는 제어부가 포함되게 구성할 수 있다.

[0017] 또한, 상기 사용자앱부는 암호키를 관리하는 암호키관리모듈과 상기 암호키관리모듈로부터 암호키를 제공받아 암호화 및 복호화하는 개인정보관리모듈, 및 제1 또는 제2 증명서 생성시 개인정보관리모듈로부터 개인정보를 제공받음과 동시에 상기 암호키관리모듈로부터 개인키를 제공받아 전자서명된 증명서를 생성하고, 상기 무선통신모듈을 통하여 전자 서명된 제1 또는 제2 증명서를 수신 또는 발신하도록 동작하는 신원증명서 관리모듈을 포함한다.

[0018] 그리고 상기 통합 증명서는 수업 출석 증명서, 행사 참석 증명서, 모임 참석 증명서, 여행지 방문 증명서, 식음료 거래 증명서 또는 디지털 명함 중 어느 하나인 것을 특징으로 한다.

발명의 효과

[0019] 따라서, 본 발명의 일실시예에 의한 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 의하면, 전자 서명된 확인증을 서로 교환하여 온오프체인에 등록된 공개키로 검증을 할 수 있기 때문에 비대면으로 검증된 증명서를 주고받을 수 있다.

[0020] 또한, 본 발명의 일실시예에 의한 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 의하면, 온오프체인상에 검증에 필요한 최소 정보만 등록하고, 개인정보가 저장된 개인 단말기를 이용하여 증명서를 발급하기 때문에 필수 정보만 입력하여 검증된 증명서를 주고 받을 수 있다.

[0021] 또한, 본 발명의 일실시예에 의한 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 의하면, 출석확인을 위한 수업출석 증명서를 생성할 수 있기 때문에 교수는 강의실 내 위치한 다수의 수강생들의 수업 출석 여부를 동시에 빠르고 정확하게 확인할 수 있는 효과가 있다.

[0022] 또한, 본 발명의 일실시예에 의한 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 의하면, 행사 참석여부를 확인할 수 있는 행사 참석 증명서를 생성할 수 있기 때문에 행사, 워크샵, 컨퍼런스, 전시회 또는 회의 주최자는 행사장에 위치한 다수의 참석자들의 행사 참석 여부를 동시에 빠르고 정확하게 확인할 수 있다.

[0023] 또한, 본 발명의 일실시예에 의한 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 의하면, 모임 참석여부를 확인할 수 있는 모임 참석 증명서를 생성할 수 있기 때문에, 동호회/동문회/동아리 주최자는 모임 장소에 위치한 다수의 회원들의 참석 여부를 동시에 빠르고 정확하게 확인할 수 있다.

[0024] 또한, 본 발명의 일실시예에 의한 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 의하면, 여행지 방문 유무를 확인할 수 있는 여행지 방문 증명서를 생성할 수 있기 때문에 유명 여행지 (유적지/관광지) 운영자는 방문 장소에 위치한 다수의 손님들의 방문 여부를 동시에 빠르고 정확하게 확인할 수 있다.

[0025] 또한, 본 발명의 일실시예에 의한 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 의하면, 식음료 거래 증명서를 생성할 수 있기 때문에 식음료 판매자는 매장 내 위치한 다수의 손님들의 주문을 동시에 빠르고 정확하게 처리할 수 있다.

[0026] 그리고 본 발명의 일실시예에 의한 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 의하면, 검증된 디지털 명함을 생성하고 교환할 수 있기 때문에 행사, 워크샵, 컨퍼런스, 전시회 또는 회의장에 위치한 다수의 사람들이 동시에 디지털 명함을 빠르고 정확하게 교환할 수 있는 효과가 있다.

도면의 간단한 설명

[0027] 도 1은 본 발명의 무선 통신을 이용한 개인간 비대면 신원 확인 시스템의 기능을 설명하기 위한 도면,

도 2는 본 발명의 무선 통신을 이용한 개인간 비대면 신원 확인 시스템의 주요 구성도,

도 3은 본 발명 앱의 주요 기능을 설명하기 위한 참고 도면,

도 4는 오프 체인을 이용한 증명서 검증 방법을 설명하기 위한 흐름도,

도 5는 일례로 실제 운영자와 방문객 간이 주고 받는 증명서 발급 과정을 설명하기 위한 흐름도,

도 6은 본 발명의 일실시예에 의한 수업출석 증명서를 발급하는 과정을 설명하기 위한 참고 도면,

도 7은 본 발명의 다른 실시예에 의한 행사 참석 증명서를 발급하는 과정을 설명하기 위한 참고 도면,

도 8은 본 발명의 또 다른 실시예에 의한 모임참석 증명서를 발급하는 과정을 설명하기 위한 참고 도면,

도 9는 본 발명의 또 다른 실시예에 의한 여행지 방문 증명서를 발급하는 과정을 설명하기 위한 참고 도면,

도 10은 본 발명의 또 다른 실시예에 의한 거래 증명서를 발급하는 과정을 설명하기 위한 참고 도면,

그리고

도 11은 본 발명의 또 다른 실시예에 의한 디지털 명함을 주고받는 과정을 설명하기 위한 참고 도면이다.

발명을 실시하기 위한 구체적인 내용

[0028] 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정 해석되지 아니하며, 발명자

는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다.

[0029] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈", "장치" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 및/또는 소프트웨어의 결합으로 구현될 수 있다.

[0030] 명세서 전체에서 "및/또는"의 용어는 하나 이상의 관련 항목으로부터 제시 가능한 모든 조합을 포함하는 것으로 이해되어야 한다. 예를 들어, "제1 항목, 제2 항목 및/또는 제3 항목"의 의미는 제1, 제2 또는 제3 항목뿐만 아니라 제1, 제2 또는 제3 항목들 중 2개 이상으로부터 제시될 수 있는 모든 항목의 조합을 의미한다.

[0031] 명세서 전체에서 각 단계들에 있어 식별부호(예를 들어, a, b, c, ...)는 설명의 편의를 위하여 사용되는 것으로 식별부호는 각 단계들의 순서를 한정하는 것이 아니며, 각 단계들은 문맥상 명백하게 특정 순서를 기재하지 않은 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 단계들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0032] 먼저, 본 발명에서 사용되는 용어는 다음과 같은 의미를 갖는 것으로 정의한다.

[0033] "오프 체인(OFF-CHAIN)"이란 블록체인 시스템과 관련되어 있지만, 블록체인 시스템 외부에 위치하여 동작하는 것으로, 오프체인에 저장된 데이터는 동일한 사법관할에 속한 참여노드에게만 공유되며, 블록체인 네트워크 외부에서 트랜잭션(Transaction)이 기록된다는 뜻으로 트랜잭션은 거래뿐만 아니라 여러 액션(Actions)이 포함되어 있는 것을 의미한다.

[0034] "온체인(On-Chain)"이란 블록체인 시스템 내부에 거래 내역(데이터)등을 기록하는 방식을 의미하며 온체인에 저장된 데이터는 모든 참여 노드가 공유하는 것을 의미한다.

[0035] 이하, 도면을 참고하여 본 발명의 일실시예에 대하여 설명한다.

[0036] 도 1은 본 발명의 무선 통신을 이용한 개인간 비대면 신원 확인 시스템의 기능을 설명하기 위한 도면으로 도시된 바와 같이, 본 발명은 오프체인(OFF-CHAIN) 또는 온체인(ON-CHAIN)에 이용자 식별자, 공개키, 암호키 사본, 및 단말기 식별자를 포함하는 이용자 등록정보 중 어느 하나 이상을 등록하고, 이용자 등록정보를 등록한 단말기간에 전자서명된 증명서를 교환하여 최종 통합 증명서를 생성하도록 동작한다.

[0037] 도면을 참고하면, 제1 단말기(Terminal_a;110), 제2 단말기(Terminal_b;120), 제3 단말기(Terminal_c;130)는 도메인 A(100)로 명명되는 영역에서 동작하며, OFF-CHAIN A(140)와 ON-CHAIN(10)상에 이용자 식별자, 공개키, 암호키 사본, 및 단말기 식별자를 포함하는 이용자 등록정보를 등록하고, 등록한 단말기간에 전자서명된 증명서를 주고받고 해당 온오프 체인상에서 공개키를 이용하여 증명서를 검증하도록 구성되어 있다.

[0038] 즉, 본 발명은 이용자 등록정보를 온오프체인상에 등록한 단말기간에 서명된 증명서를 교환하도록 동작하는 것을 하나의 특징으로 한다.

[0039] 또한, 제4 단말기(Terminal_1;210), 제5 단말기(Terminal_2;220), 제6 단말기(Terminal_3;330)는 도메인 B(200)로 명명되는 영역에서 동작하며, OFF-CHAIN (240)과 ON-CHAIN(10)상에 이용자 식별자, 공개키, 암호키 사본, 및 단말기 식별자를 포함하는 이용자 등록정보를 등록하고, 등록한 단말기간에 전자서명된 증명서를 주고받고 해당 온오프 체인상에서 공개키를 이용하여 증명서를 검증하도록 구성되어 있다.

[0040] 도메인 A에 포함되어 있는 단말기가 도메인 B에 포함된 단말기와 정보를 송수신할 경우에는 온체인(10)을 이용하여 소통하며, 도면에서는 제1단말기(110)와 제6단말기(230)가 서로 정보를 주고 받을 수 있게 연결되어 있음을 알 수 있다.

[0041] 즉, OFF-CHAIN상에만 정보를 등록한 경우는 해당 도메인 내에서만 서로 정보의 교환이 가능하고, 타 도메인에 소속된 단말기와 정보를 교환하고자 할 경우는 온체인을 이용하여 교환하는 것이다.

[0042] 도 3의 본 발명 앱의 주요 기능을 설명하기 위한 참고 도면을 보면, 단말기(110)에서 OFF-CHAIN(140)에 등록하는 정보는 ①로 표시된 "이용자식별자, 단말기식별자" 정보와 ⑤로 표시된 "암호키사본, 공개키"가 있고, ON-CHAIN(10) 상에 등록하는 정보는 해당 OFF-CHAIN(140)에서 등록하는 정보(④)로 구성되며 공개키, 이용자식별자, 및 단말기식별자 정보 등이 있다.

[0043] 이러한 구성을 통하여 각 단말기는 OFF-CHAIN(140)에서 전자서명을 검증(②)하거나 타 도메인의 단말기와 정보를 교환하고자 할 때는 ON-CHAIN(10)에서 전자서명을 검증한다(③).

[0044] 이를 위하여 본 발명의 무선 통신을 이용한 개인간 비대면 신원 확인 시스템은 본 발명과 관련된 어플리케이션을 구동하여 증명서를 교환하고 검증을 수행하는 사용자앱부와 이를 제어하는 제어부 그리고 무선통신모듈을 포함하도록 단말기로 구성할 수 있다.

[0045] 도 2의 본 발명의 무선 통신을 이용한 개인간 비대면 신원 확인 시스템의 주요 구성도를 참고하면, 단말기(110)는 타블렛, 스마트폰, 스마트 패드, 스마트 워치, PDA, 또는 전용단말기로 구성될 수 있으며, 통상의 스마트폰과 같이 무선통신과 인터넷 통신을 수행할 수 있도록 동작하게 할 수 있다.

[0046] 또한, 본 발명은 모두 동일한 구성의 단말기를 사용할 수 있으므로 설명의 편의를 위하여 대표적으로 제1 단말기(110)의 구성을 설명하기로 한다.

[0047] 사용자 앱부(115)는 앱스토어 등을 통하여 관련 앱을 다운받아 저장하거나 또는 이동통신망을 통해 플랫폼으로 동작하는 웹서버(미도시)에 접속하여 어플리케이션을 다운받아 설치되도록 구성된다.

[0048] 본 발명에서의 어플리케이션(이하, 앱(app)이라 함)은 온오프체인에 관련 정보를 등록하고, 증명서를 생성하여 전자서명하고, 수신한 증명서를 검증할 수 있도록 GUI로 구성된다.

[0049] 바람직하게는 앱(App)의 설치과정에서 웹에서 동작하는 상기 서버의 인증과정을 거쳐 어플리케이션을 설치하도록 할 수 있다.

[0050] 즉, 본 발명은 추천 플랫폼으로 동작하는 웹서버(미도시)에 접속해서 앱을 다운받아 설치할 수도 있으나, IOS 계열이건 안드로이드 계열이건 관계없이 각 OS에 맞는 앱을 앱 스토어에 올려서 배포하는 방식을 사용할 수도 있다.

[0051] 이러한 앱(App)의 다운 및 설치과정 그리고 인증단계 등은 일반적인 것이므로 그 상세한 설명은 생략한다.

[0052] 무선통신모듈(111)은 40m이내에서 근거리 무선통신을 통하여 데이터를 송수신하도록 구성한다.

[0053] 본 발명은 비대면으로 증명서를 송수신하고 검증하는 것이므로, 블루투스나 와이파이다이렉트 무선통신 방식을 사용하는 것이 바람직하다.

[0054] 본 발명의 앱(App)은 상술한 바와 같이 해당 단말기 내 증명서, 개인키 그리고 암호키원본을 보관하고, 온오프체인에 등록된 타단말기의 공개키로 수신한 증명서를 검증하며, 해당 단말기의 이용자 식별자 및 개인키로 서명된 증명서를 상기 무선통신모듈을 통하여 타단말기로 전송하도록 하는 동작을 효율적으로 수행하기 위하여 암호키 관리모듈(115c)과 개인정보 관리모듈(115b) 그리고 신원증명서 관리모듈(115a)로 동작하도록 구성된다(도 3 참고).

[0055] 암호키 관리모듈(115c)은 암호키를 관리하며, 개인정보 관리모듈(115b)은 암호키관리모듈(115c)로부터 제공받은 암호키로 개인정보를 암호화 및 복호화하고, 신원증명서 관리모듈(115a)은 실질적인 제1 또는 제2 증명서 생성 시 개인정보관리모듈(115b)로부터 개인정보를 제공받음과 동시에 암호키관리모듈(115c)로부터 개인키를 제공받아 전자서명된 증명서를 생성하고, 무선통신모듈(111)을 통하여 전자 서명된 제1 또는 제2 증명서를 수신 또는 발신하도록 동작한다.

[0056] 저장부(116)는 본 발명의 앱(app) 운영에 필요한 여러 정보 즉 단말기 소지자의 개인 정보와 개인키/공개키, 암호키원본, 이용자 식별자, 단말기 식별자, 생성한 증명서 등을 저장한다.

[0057] 따라서 앱(app)이 실행되면, 개인정보관리모듈(115b)과 암호키관리모듈(115c)은 저장부(116)에서 각각 필요한 정보를 판독하여 사용한다.

[0058] 또한, 저장부(116)에는 앱(app)에서 사용할 수 있는 통합 증명서로 수업 출석 증명서, 행사 참석 증명서, 모임 참석 증명서, 여행지 방문 증명서, 식음료 거래 증명서 또는 디지털 명함 등의 통합 증명서 발급 아이콘을 설정해 두면, 상황에 따라 필요한 아이콘을 손쉽게 사용하게 할 수 있다.

[0059] 단말기제어부(114)는 본 발명과 관련된 사용자 앱부(115)의 어플리케이션을 구동하여 단말기표시부(120)에 표시함과 동시에 무선통신모듈(110)을 통하여 전자서명한 증명서를 전송하도록 하고, 타단말기에서 전자서명된 증명서를 수신하여 표시하도록 동작한다.

[0060] 또한, 단말기제어부(114)는 어플리케이션을 수행할 수 있는 아이콘을 표시부(112)에 표시하고, 해당 아이콘이 클릭될 경우 사용자 앱부(115)에 저장되어 있는 어플리케이션을 자동으로 구동하여 타단말기와 통신할 수 있도록 자동 제어할 수 있다.

[0061] 다시 도 2를 참고하면, 3대의 단말기로 OFF-CHAIN(140)에서 증명서를 송수신하는 것으로 예시되어 있으나, 본 발명은 3대 이상의 단말기가 온오프체인 상에서 동시에 증명서를 송수신하는 것이 가능하다.

[0062] 또한, 3대 이상의 단말기가 동시에 통신하더라도 2대의 단말기간에 주고받는 내용과 동일하므로, 이하에서는 제1 단말기와 제2 단말기간의 통신에 대하여 설명하기로 한다.

[0063] 또한, 본 발명은 단말기에서 자체 생성한 증명서는 제1 증명서로 타단말기에서 생성한 증명서는 제2 증명서로 설명하고, 제1 증명서와 제2 증명서를 결합한 완성된 증명서를 통합 증명서로 설명한다.

[0064] 즉, 제1 단말기(110)의 신원증명서 관리모듈(115a)이 해당 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제1 증명서를 생성하여 무선통신모듈(111)을 통하여 제2단말기(120)로 전송하고 제2단말기(120)로부터 해당 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제2 증명서를 수신하여 온오프체인에 등록된 제2단말기(120)의 공개키로 수신한 제2 증명서를 검증하도록 동작한다.

[0065] 또한, 제2 단말기(120)도 해당 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제2 증명서를 생성하여 무선통신모듈(111)을 통하여 제1단말기(110)로 전송하고 제1 단말기(110)로부터 해당 단말기 이용자의 이용자 식별자 및 개인키로 서명된 제1 증명서를 수신하여 온오프체인에 등록된 제1단말기(120)의 공개키로 수신한 제1 증명서를 검증하도록 동작한다.

[0066] 상술한 바와 같이 제1 및 제2 단말기에서 서로 송수신한 증명서가 검증되면, 각 단말기의 신원증명서 관리 모듈(115a)은 자체 생성한 제1 증명서와 타단말기에서 수신한 제2 증명서를 결합하여 통합 증명서를 생성한다.

[0067] 즉, 각 단말기의 제어부는 타단말기에서 전송된 증명서가 검증되면, 해당 단말기에서 생성한 이용자 식별자 및 개인키로 서명된 증명서와 타단말기에서 수신한 검증된 증명서를 결합하여 각 단말기에서 공동 서명한 통합 증명서를 단말기표시부에 표시하거나 저장부에 저장하도록 제어하는 것이다.

[0068] 구체적으로 제1 단말기(110)는 수신한 제2 증명서가 검증되면 자체 생성한 제1 증명서와 상기 검증된 제2 증명서를 결합하여 공동서명한 통합 증명서를 생성하여 저장부(116)에 저장하거나 단말기표시부(112)에 표시하고, 제2 단말기(120)도 수신한 제1 증명서가 검증되면 제2 증명서와 검증된 제1 증명서를 결합하여 공동서명한 통합 증명서를 생성하여 저장하거나 표기할 수 있다.

[0069] 미설명부호 114는 본 발명의 앱실행에 필요한 정보들을 입력하는 키입력부를 의미한다.

[0070] 상술한 구성을 이용한 개인간 비대면 신원 확인 방법에 대하여 설명한다.

[0071] 도 4는 오프 체인을 이용한 증명서 검증 방법을 설명하기 위한 흐름도로서, 도시된 바와 같이, 본 발명의 신원확인 방법은 제1 단말기(Terminal_a;110)에서 사용자 앱부(115)의 어플리케이션이 구동되면(S110), 제1 단말기(110)의 이용자식별자, 공개키, 암호키사본, 단말기 식별자 등의 정보를 판독하여 OFF-CHAIN(140)에 등록한다(S111).

[0072] 또한, 제1 단말기(110)와 증명서를 송수신할 제2 단말기(Terminal_b;120)도 사용자 앱부(125)의 어플리케이션을 구동하여(S120), 제2 단말기(120)의 이용자식별자, 공개키, 암호키사본, 단말기 식별자 등의 정보를 판독하여 OFF-CHAIN(140)에 등록한다(S121).

[0073] 단계 S111과 단계 S121에서 OFF-CHAIN에 정보가 등록되면, 해당 도메인 내에서 증명서의 교환이 가능하게 된다(S130).

[0074] 단계 S130에서의 증명서 교환은 제1 단말기(110)에서 필요 정보를 입력하여 생성한 제1 증명서를 이용자식별자와 개인키를 이용하여 전자서명한 다음 제2 단말기(120)로 전송하고, 이와 동시에 제2 단말기(120)에서 필요 정보를 입력하여 생성한 제2 증명서를 이용자식별자와 개인키를 이용하여 전자서명한 다음 제1 단말기(110)로 전송하는 것이다.

[0075] 단계 S130에서 증명서의 교환이 이루어지면 각 단말기제어부는 OFF-CHAIN을 통하여 타단말기의 공개키로 수신한 증명서를 검증하게 된다.

[0076] 구체적으로 제1 단말기(110)는 수신한 제2 증명서를 OFF-CHAIN(140)에 등록된 제2 단말기(120)의 공개키를 이용

하여 검증하고(S112), 제2 단말기(120)는 수신한 제1 증명서를 OFF-CHAIN(140)에 등록된 제1 단말기(110)의 공개키를 이용하여 검증한다(S122).

[0077] 단계 S112와 단계 S122에서 수신한 타단말기의 증명서의 검증이 완료되면, 각각 제1 증명서와 제2 증명서를 결합하여 공동서명한 통합 증명서를 생성할 수 있는 것이다.

[0078] 도 5는 일례로 실제 운영자와 방문객 간에 주고 받는 증명서 발급 과정을 설명하기 위한 흐름도로서, 제1 단말기(Terminal_a;110)는 운영자가 소지한 단말기로서, 사용자 앱부(115)의 어플리케이션을 활성화하여(S210), 방문증명서 발급에 필요한 필수 정보를 입력한다(S211).

[0079] 운영자가 필수 입력해야 할 정보로는 방문장소, 방문일시 그리고 운영자명 등을 입력하고, 제1 단말기(110)가 전자서명한 운영자 확인증을 제2 단말기(120)로 전송한다(S212).

[0080] 이때 제2 단말기(Terminal_b;120)는 방문객이 소지한 단말기로서, 사용자 앱부(125)의 어플리케이션을 활성화하여(S220), 방문증명서 발급에 필요한 필수 정보를 입력한다(S221).

[0081] 방문객이 필수 입력해야 할 정보로는 위치정보(위도/경도), 방문객 성명 등을 입력하고, 제2 단말기(120)가 전자서명한 방문 확인증을 제1 단말기(110)로 전송한다(S222).

[0082] 단계 S221과 단계 S222에서 단말기간에 운영자 확인증과 방문확인증의 교환이 이루어지면 각 단말기제어부는 OFF-CHAIN을 통하여 타단말기의 공개키로 수신한 확인증을 검증하게 된다.

[0083] 구체적으로 제1 단말기(110)는 수신한 방문확인증(제2 증명서)을 OFF-CHAIN(140)에 등록된 제2 단말기(120)의 공개키를 이용하여 검증하고(S213), 제2 단말기(120)는 수신한 운영자확인증(제1 증명서)을 OFF-CHAIN(140)에 등록된 제1 단말기(110)의 공개키를 이용하여 검증한다(S223).

[0084] 단계 S213과 단계 S223에서 수신한 타단말기의 확인증의 검증이 완료되면, 각각 운영자확인증과 방문확인증을 결합하여 공동서명한 방문증명서를 발급할 수 있는 것이다(S214, S224).

[0085] 이와 같이 본 발명의 일실시예에 의한 통합 증명서는 수업 출석 증명서, 행사 참석 증명서, 모임 참석 증명서, 여행지 방문 증명서, 식음료 거래 증명서 또는 디지털 명함 중 어느 하나일 수 있다.

[0086] 이하, 구체적인 실시예를 제시하여 여러 가지 증명서를 발행하는 과정에 대하여 도면을 참고하여 설명한다,

[0087] 도 6은 본 발명의 일실시예에 의한 수업출석 증명서를 발급하는 과정을 설명하기 위한 참고 도면으로, 통합 증명서가 수업 출석 증명서인 경우의 일례를 예시한 것이다.

[0088] 본 실시예에서는 제1 단말기(110)는 교수가 소지하는 단말기이고, 제2 단말기(120)는 수강생_1이 소지하는 단말기(Terminal_b)로 설명한다.

[0089] 수강생-_1은 제2 단말기(120)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 수업 출석 증명서 아이콘을 활성화하여, 수강생이 생성할 출석확인증과 교수가 생성할 교수확인증 중에서 출석확인증을 클릭하여 필수 정보들을 입력한다.

[0090] 이러한 수강생이 입력할 필수정보로 과목명, 학번, 그리고 수강생 성명 등을 입력하여 생성된 출석확인증에 전자서명한다. 전자서명은 상술한 바와 같이 저장부에 저장되어 있는 이용자식별자와 개인키를 이용한다.

[0091] 교수도 제1 단말기(110)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 수업 출석 증명서 아이콘을 활성화하여, 수강생이 생성할 출석확인증과 교수가 생성할 교수확인증 중에서 교수확인증을 클릭하여 필수 정보들을 입력한다.

[0092] 이러한 교수가 입력할 필수정보로 학교명, 과목명, 수업일시, 그리고 교수 성명 등을 입력하여 생성된 교수확인증에 동일한 방법으로 전자서명한다.

[0093] 각각의 확인증에 전자서명이 완료되면 각 단말기는 전자서명된 확인증을 서로 교환한다.

[0094] 구체적으로 제1 단말기(110)에서 전자서명된 교수확인증은 무선통신모듈(111)을 통하여 제2 단말기(120)로 전송하고, 제2 단말기(120)에서 전자서명된 출석확인증은 무선통신모듈(121)을 통하여 제1 단말기(110)로 전송한다.

[0095] 제1 단말기(110)는 전자서명이 첨부된 출석확인증을 수신하여 온오프 체인에 등록되어 있는 해당 수강생의 공개키로 검증하고, 검증이 완료되면 생성한 교수확인증에 상기 출석확인증을 결합하여 공동 서명된 수업 출석 증명서를 생성하는 것이다.

[0096] 또한, 제2 단말기(120)도 전자서명이 첨부된 교수확인증을 수신하여 온오프 체인에 등록되어 있는 해당 교수의 공개키로 검증하고, 검증이 완료되면 생성한 출석확인증에 상기 교수확인증을 결합하여 공동 서명된 수업 출석 증명서를 생성하는 것이다.

[0097] 상기 수업 출석 증명서에는 학교명, 과목명, 수업일시, 교수성명, 학번, 그리고 수강생성명 등이 기재될 수 있다.

[0098] 도 7은 본 발명의 다른 실시예에 의한 행사 참석 증명서를 발급하는 과정을 설명하기 위한 참고 도면으로, 통합 증명서가 행사 참석 증명서인 경우의 일례를 예시한 것이다.

[0099] 본 실시예에서는 제1 단말기(110)는 주최자가 소지하는 단말기이고, 제2 단말기(120)는 참석자_1이 소지하는 단말기(Terminal_b)로 설명한다.

[0100] 참석자-_1은 제2 단말기(120)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 행사 참석 증명서 아이콘을 활성화하여, 참석자가 생성할 참석확인증과 주최자가 생성할 주최자 확인증 중에서 참석확인증을 클릭하여 필수 정보들을 입력한다.

[0101] 이러한 참석자가 입력할 필수정보로 행사명, 참석자 직장명, 그리고 참석자 성명 등을 입력하여 생성된 참석확인증에 전자서명한다. 전자서명은 상술한 바와 같이 저장부에 저장되어 있는 이용자식별자와 개인키를 이용한다.

[0102] 주최자도 제1 단말기(110)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 행사 참석 증명서 아이콘을 활성화하여, 참석자가 생성할 작성할 참석확인증과 주최자가 생성할 주최자확인증 중에서 주최자확인증을 클릭하여 필수 정보들을 입력한다.

[0103] 이러한 주최자가 입력할 필수정보로 행사명, 행사기간 그리고 주최자 성명 등을 입력하여 생성된 주최자확인증에 동일한 방법으로 전자서명한다.

[0104] 각각의 확인증에 전자서명이 완료되면 각 단말기는 전자서명된 확인증을 서로 교환한다.

[0105] 구체적으로 제1 단말기(110)에서 전자서명된 주최자확인증은 무선통신모듈(111)을 통하여 제2 단말기(120)로 전송하고, 제2 단말기(120)에서 전자서명된 참석확인증은 무선통신모듈(121)을 통하여 제1 단말기(110)로 전송한다.

[0106] 제1 단말기(110)는 전자서명이 첨부된 참석확인증을 수신하여 온오프 체인에 등록되어 있는 해당 참석자의 공개키로 검증하고, 검증이 완료되면 생성한 주최자확인증에 상기 참석확인증을 결합하여 공동 서명된 행사 참석 증명서를 생성하는 것이다.

[0107] 또한, 제2 단말기(120)도 전자서명이 첨부된 주최자확인증을 수신하여 온오프 체인에 등록되어 있는 해당 주최자의 공개키로 검증하고, 검증이 완료되면 생성한 참석확인증에 상기 주최자확인증을 결합하여 공동 서명된 행사 참석 증명서를 생성하는 것이다.

[0108] 상기 행사 참석 증명서에는 행사명, 행사기간, 주최자명, 참석자 직장명, 그리고 참석자명 등이 기재될 수 있다.

[0109] 도 8은 본 발명의 또 다른 실시예에 의한 모임참석 증명서를 발급하는 과정을 설명하기 위한 참고 도면으로, 통합 증명서가 모임 참석 증명서인 경우의 일례를 예시한 것이다.

[0110] 본 실시예에서는 제1 단말기(110)는 주최자가 소지하는 단말기이고, 제2 단말기(120)는 회원_1이 소지하는 단말기(Terminal_b)로 설명한다.

[0111] 회원-_1은 제2 단말기(120)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 모임 참석 증명서 아이콘을 활성화하여, 회원이 생성할 참석확인증과 주최자가 생성할 주최자 확인증 중에서 참석확인증을 클릭하여 필수 정보들을 입력한다.

[0112] 이러한 참석자가 입력할 필수정보로 모임명, 회원명(닉네임) 등을 입력하여 생성된 참석확인증에 전자서명한다. 전자서명은 상술한 바와 같이 저장부에 저장되어 있는 이용자식별자와 개인키를 이용한다.

[0113] 주최자도 제1 단말기(110)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 모임 참석 증명서 아이콘을 활성화하여, 회원이 생성할 참석확인증과 주최자가 생성할 주최자확인증 중에서 주최자확인증을 클릭하여 필

수 정보들을 입력한다.

[0114] 이러한 주최자가 입력할 필수정보로 모임명, 모임일시 그리고 주최자 성명 등을 입력하여 생성된 주최자확인증에 동일한 방법으로 전자서명한다.

[0115] 각각의 확인증에 전자서명이 완료되면 각 단말기는 전자서명된 확인증을 서로 교환한다.

[0116] 구체적으로 제1 단말기(110)에서 전자서명된 주최자확인증은 무선통신모듈(111)을 통하여 제2 단말기(120)로 전송하고, 제2 단말기(120)에서 전자서명된 참석확인증은 무선통신모듈(121)을 통하여 제1 단말기(110)로 전송한다.

[0117] 제1 단말기(110)는 전자서명이 첨부된 참석확인증을 수신하여 온오프 체인에 등록되어 있는 해당 회원의 공개키로 검증하고, 검증이 완료되면 생성한 주최자확인증에 상기 참석확인증을 결합하여 공동 서명된 모임 참석 증명서를 생성하는 것이다.

[0118] 또한, 제2 단말기(120)도 전자서명이 첨부된 주최자확인증을 수신하여 온오프 체인에 등록되어 있는 해당 주최자의 공개키로 검증하고, 검증이 완료되면 생성한 참석확인증에 상기 주최자확인증을 결합하여 공동 서명된 모임 참석 증명서를 생성하는 것이다.

[0119] 상기 모임 참석 증명서에는 모임명, 모임일시, 주최자명, 회원명(닉네임) 등이 기재될 수 있다.

[0120] 도 9는 본 발명의 또 다른 실시예에 의한 여행지 방문 증명서를 발급하는 과정을 설명하기 위한 참고 도면으로, 통합 증명서가 여행지 방문 증명서인 경우의 일례를 예시한 것이다.

[0121] 본 실시예에서는 제1 단말기(110)는 운영자가 소지하는 단말기이고, 제2 단말기(120)는 방문객_1이 소지하는 단말기(Terminal_b)로 설명한다.

[0122] 방문객-_1은 제2 단말기(120)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 여행지 방문 증명서 아이콘을 활성화하여, 방문객이 생성할 방문확인증과 운영자가 생성할 운영자확인증 중에서 방문확인증을 클릭하여 필수 정보들을 입력한다.

[0123] 이러한 방문객이 입력할 필수정보로 위치정보(위도/경도), 방문객 성명 등을 입력하여 방문확인증을 생성하고 전자서명한다. 전자서명은 상술한 바와 같이 저장부에 저장되어 있는 이용자식별자와 개인키를 이용한다.

[0124] 위치정보(위도/경도)의 경우 통상적인 방문 장소로 하여도 되나 대리 방문이나 증명서의 허위발급을 방지하기 위하여 실제 단말기 소지자의 위도와 경도로 위치 확인을 하는 것이다.

[0125] 운영자도 제1 단말기(110)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 여행지 방문 증명서 아이콘을 활성화하여, 방문객이 생성할 방문확인증과 운영자가 생성할 운영자확인증 중에서 운영자확인증을 클릭하여 필수 정보들을 입력한다.

[0126] 이러한 운영자가 입력할 필수정보로 방문장소, 방문일시, 운영자 성명 등을 입력하여 생성된 운영자확인증에 동일한 방법으로 전자서명한다.

[0127] 각각의 확인증에 전자서명이 완료되면 각 단말기는 전자서명된 확인증을 서로 교환한다.

[0128] 구체적으로 제1 단말기(110)에서 전자서명된 운영자확인증은 무선통신모듈(111)을 통하여 제2 단말기(120)로 전송하고, 제2 단말기(120)에서 전자서명된 방문확인증은 무선통신모듈(121)을 통하여 제1 단말기(110)로 전송한다.

[0129] 제1 단말기(110)는 전자서명이 첨부된 방문확인증을 수신하여 온오프 체인에 등록되어 있는 해당 방문객의 공개키로 검증하고, 검증이 완료되면 생성한 운영자확인증에 상기 방문확인증을 결합하여 공동 서명된 여행지 방문 증명서를 생성하는 것이다.

[0130] 또한, 제2 단말기(120)도 전자서명이 첨부된 운영자확인증을 수신하여 온오프 체인에 등록되어 있는 해당 운영자의 공개키로 검증하고, 검증이 완료되면 생성한 방문확인증에 상기 운영자확인증을 결합하여 공동 서명된 여행지 방문 증명서를 생성하는 것이다.

[0131] 상기 여행지 방문 증명서에는 방문장소, 위치정보(위도/경도), 방문일시, 운영자명 그리고 방문객성명 등이 기재될 수 있다.

[0132] 도 10은 본 발명의 또 다른 실시예에 의한 거래 증명서를 발급하는 과정을 설명하기 위한 참고 도면으로, 통합

증명서가 식음료 거래 증명서인 경우의 일례를 예시한 것이다.

[0133] 본 실시예에서는 식음료 거래를 증명하기 위한 방법을 설명하나, 거래 내용만 수정하면 여러 가지 거래를 할 수 있는 증명서로 사용할 수 있음을 물론이다.

[0134] 본 실시예에서는 제1 단말기(110)는 판매자가 소지하는 단말기이고, 제2 단말기(120)는 주문자_1이 소지하는 단말기(Terminal_b)로 설명한다.

[0135] 주문자-_1은 제2 단말기(120)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 식음료 거래 증명서 아이콘을 활성화하여, 주문자가 생성할 주문확인증과 판매자가 생성할 판매확인증 중에서 주문확인증을 클릭하여 필수 정보들을 입력한다.

[0136] 이러한 주문자가 입력할 필수정보로 업소명, 주문일시, 주문내역, 그리고 주문자 성명 등을 입력하여 생성된 주문확인증에 전자서명한다. 전자서명은 상술한 바와 같이 저장부에 저장되어 있는 이용자식별자와 개인키를 이용한다.

[0137] 판매자도 제1 단말기(110)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 식음료 거래 증명서 아이콘을 활성화하여, 주문자가 생성할 주문확인증과 판매자가 생성할 판매확인증 중에서 판매자가 생성할 판매확인증을 클릭하여 필수 정보들을 입력한다.

[0138] 이러한 판매자가 입력할 필수정보로 업소명, 판매자 성명, 판매일시, 그리고결제 금액 등을 입력하여 생성된 판매확인증에 동일한 방법으로 전자서명한다.

[0139] 각각의 확인증에 전자서명이 완료되면 각 단말기는 전자서명된 확인증을 서로 교환한다.

[0140] 구체적으로 제1 단말기(110)에서 전자서명된 판매확인증은 무선통신모듈(111)을 통하여 제2 단말기(120)로 전송하고, 제2 단말기(120)에서 전자서명된 주문확인증은 무선통신모듈(121)을 통하여 제1 단말기(110)로 전송한다.

[0141] 제1 단말기(110)는 전자서명이 첨부된 주문확인증을 수신하여 온오프 체인에 등록되어 있는 해당 주문자의 공개키로 검증하고, 검증이 완료되면 생성한 판매확인증에 상기 주문확인증을 결합하여 공동 서명된 식음료 거래 증명서를 생성하는 것이다.

[0142] 또한, 제2 단말기(120)도 전자서명이 첨부된 판매확인증을 수신하여 온오프 체인에 등록되어 있는 해당 판매자의 공개키로 검증하고, 검증이 완료되면 생성한 주문확인증에 상기 판매확인증을 결합하여 공동 서명된 식음료 거래 증명서를 생성하는 것이다.

[0143] 상기 식음료 거래 증명서에는 업소명, 판매자성명, 판매일시, 결제금액, 주문일시, 주문내역 그리고 주문자성명 등이 기재될 수 있다.

[0144] 도 11은 본 발명의 또 다른 실시예에 의한 디지털 명함을 주고받는 과정을 설명하기 위한 참고 도면으로, 통합 증명서가 디지털 명함인 경우의 일례를 예시한 것이다.

[0145] 본 실시예에서는 제1 단말기(110)와 제2 단말기(120)는 명함을 주고받을 상대방의 단말기로 설명한다.

[0146] 본인 단말기로 동작하는 제2 단말기(120)의 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 디지털 명함 아이콘을 활성화하여, 필수 정보들을 입력한다.

[0147] 이러한 디지털 명함 작성의 필수정보로 직장명/부서명, 성명, 직장 전화번호, 휴대폰 번호, 이메일 주소 그리고 직장 주소 등을 입력하여 생성된 제1 디지털 명함 확인증에 전자서명한다. 전자서명은 상술한 바와 같이 저장부에 저장되어 있는 이용자식별자와 개인키를 이용한다.

[0148] 디지털 명함을 주고받을 상대방 단말기로 동작하는 제1 단말기(110)도 앱(app)을 실행하여 발급할 통합 증명서에 설정되어 있는 디지털 명함 아이콘을 활성화하여, 필수 정보들을 입력한다.

[0149] 이러한 디지털 명함 작성의 필수정보로 직장명/부서명, 성명, 직장 전화번호, 휴대폰 번호, 이메일 주소 그리고 직장 주소 등을 입력하여 등을 입력하여 생성된 제2 디지털 명함 확인증에 동일한 방법으로 전자서명한다.

[0150] 각각의 디지털 명함에 전자서명이 완료되면 각 단말기는 전자서명된 디지털명함 확인증을 서로 교환한다.

[0151] 구체적으로 제1 단말기(110)에서 전자서명된 제1 디지털명함 확인증은 무선통신모듈(111)을 통하여 제2 단말기(120)로 전송하고, 제2 단말기(120)에서 전자서명된 제2 디지털명함 확인증은 무선통신모듈(121)을 통하여 제1 단말기(110)로 전송한다.

[0152] 제1 단말기(110)는 전자서명이 첨부된 제2 디지털명함 확인증을 수신하여 온오프 체인에 등록되어 있는 제2 단말기 소유자의 공개키로 검증하고, 검증이 완료된 제2 디지털명함 확인증에 주고받은 일시를 결합하여 디지털 명함으로 생성하는 것이다.

[0153] 또한, 제2 단말기(120)도 전자서명이 첨부된 제1 디지털명함 확인증을 수신하여 온오프 체인에 등록되어 있는 제1 단말기 소유자의 공개키로 검증하고, 검증이 완료되면 제1 디지털명함 확인증에 주고받은 일시를 결합하여 디지털 명함으로 생성하는 것이다.

[0154] 상술한 바와 같이 본 발명의 무선 통신을 이용한 개인간 비대면 신원 확인 시스템에 의하면, 전자서명된 증명서들을 서로 교환하고, 수신한 증명서를 해당 증명서 작성자의 공개키로 검증하고, 검증이 완료되면 통합 증명서를 생성함으로써, 무선 통신을 이용하기 때문에 개인간 비대면으로 증명서를 교환할 수 있어, 행사, 워크샵, 컨퍼런스, 전시회 또는 회의 주최자는 행사장에 위치한 다수의 참석자들의 행사 참석 여부를 동시에 빠르고 정확하게 확인할 수 있는 효과가 있다.

[0155] 이상에서 본 발명은 기재된 구체예에 대하여 상세히 설명되었지만 본 발명의 기술사상 범위 내에서 다양한 변형 및 수정이 가능함은 당업자에게 있어서 명백한 것이며, 이러한 변형 및 수정이 첨부된 특허 청구범위에 속함은 당연한 것이다.

부호의 설명

[0156] 10 : ON-CHAIN

100 : Domain A 110 : 제1 단말기(Terminal_a)

111 : 무선통신모듈 112 : 단말기표시부

114 : 단말기제어부 115 : 사용자 앱부

115a : 신원증명서 관리모듈 115b : 개인정보 관리모듈

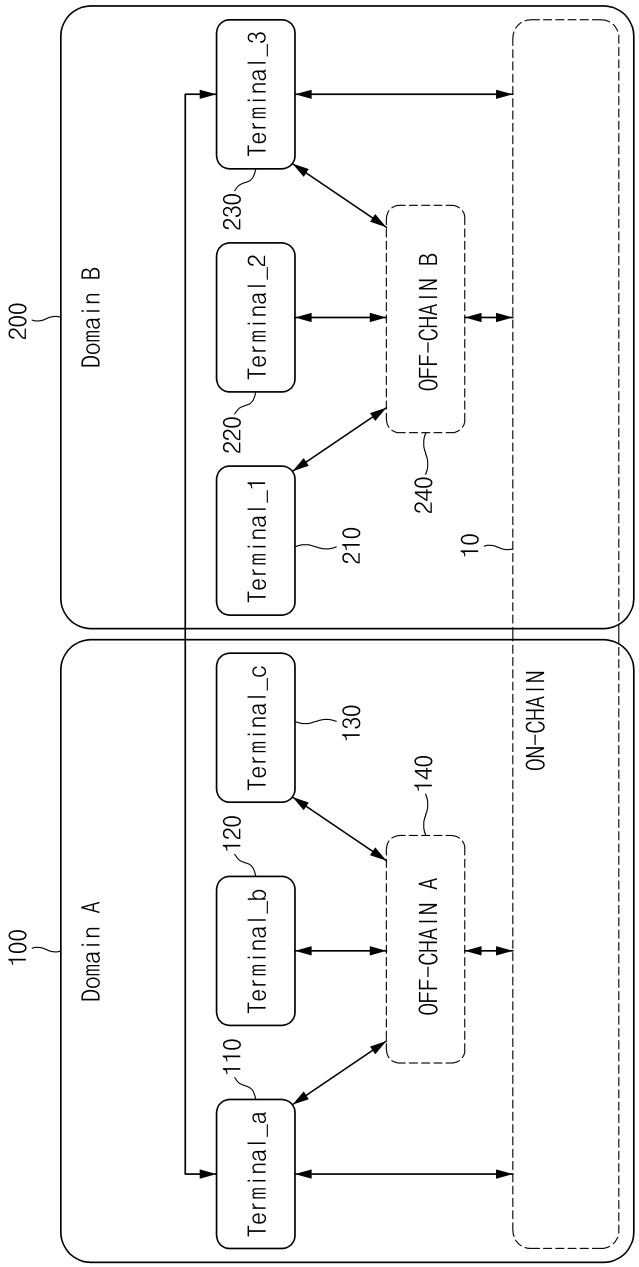
115c : 암호키 관리모듈 116 : 저장부

120 : 제1 단말기(Terminal_b) 130 : 제1 단말기(Terminal_c)

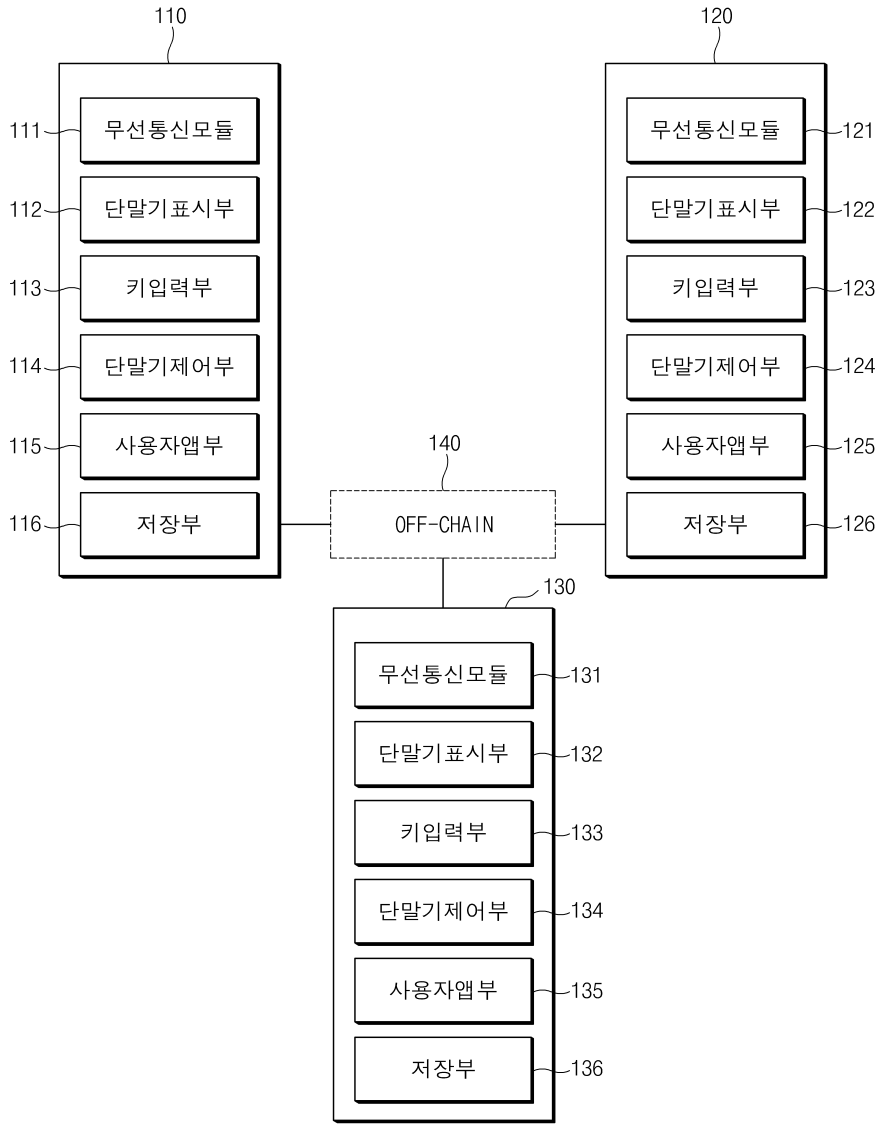
140 : OFF-CHAIN 200 : Domain B

도면

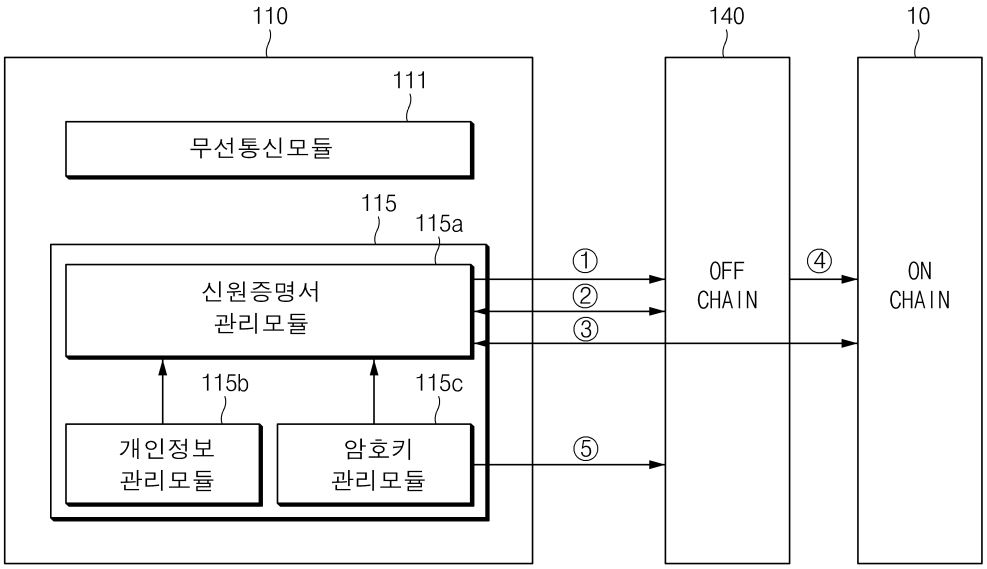
도면1


100
Domain A
Terminal_a
110
Terminal_b
120
Terminal_c
130
OFF-CHAIN A
140
200
Domain B
Terminal_1
210
Terminal_2
220
Terminal_3
230
OFF-CHAIN B
240
10
ON-CHAIN

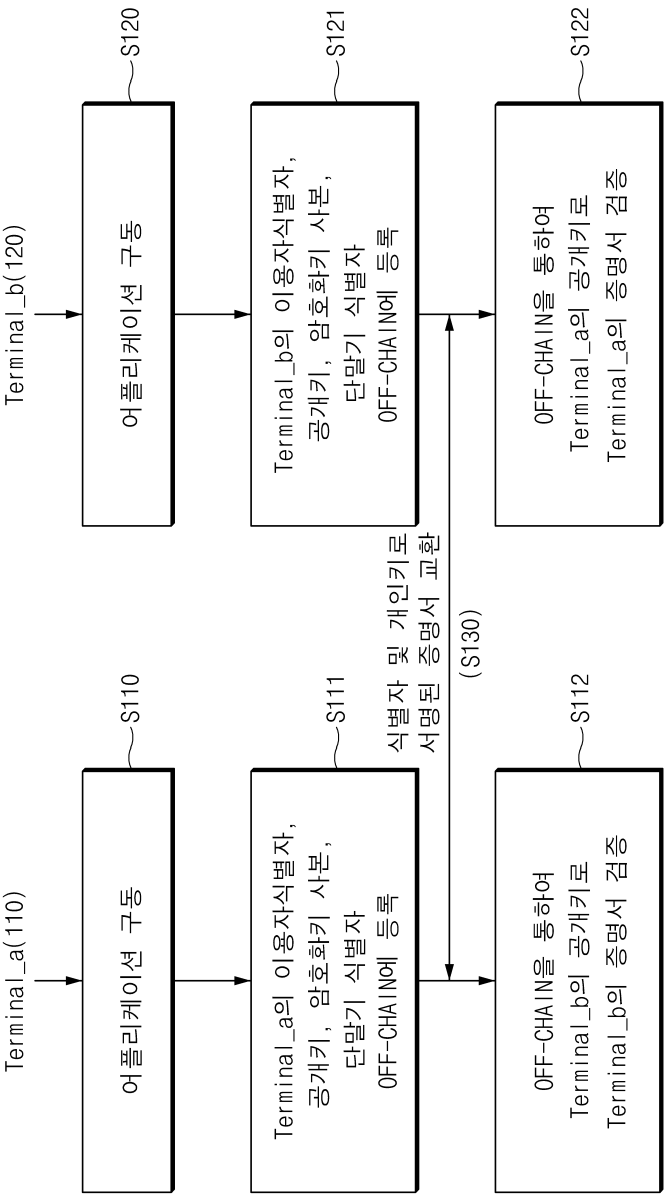
도면2


110
111
무선통신모듈
112
단말기표시부
113
키입력부
114
단말기제어부
115
사용자앱부
116
저장부
120
무선통신모듈
121
단말기표시부
122
키입력부
123
단말기제어부
124
사용자앱부
125
저장부
126
140
OFF-CHAIN
130
무선통신모듈
131
단말기표시부
132
키입력부
133
단말기제어부
134
사용자앱부
135
저장부
136

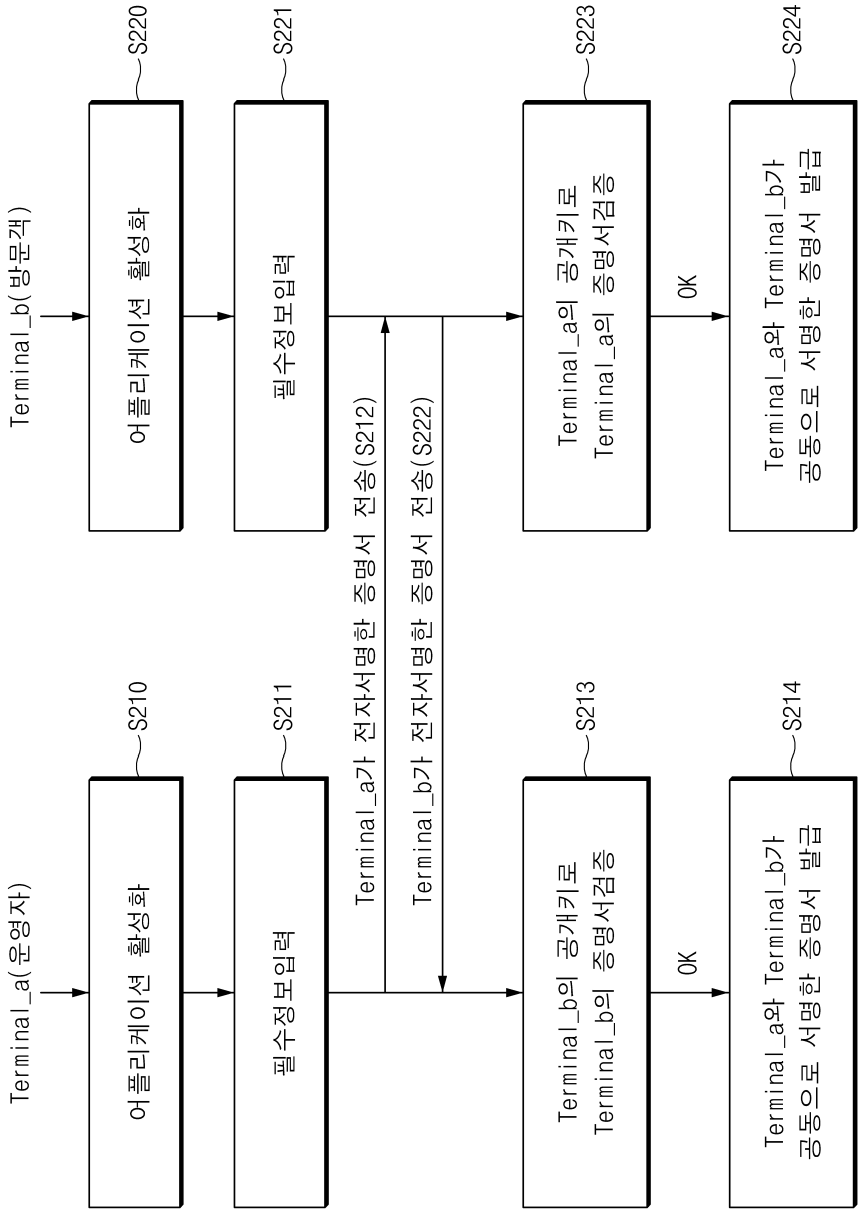
도면3


110
111
무선통신모듈
115
115a
신원증명서
관리모듈
115b
115c
개인정보
관리모듈
암호키
관리모듈
①
②
③
⑤
140
OFF
CHAIN
④
10
ON
CHAIN

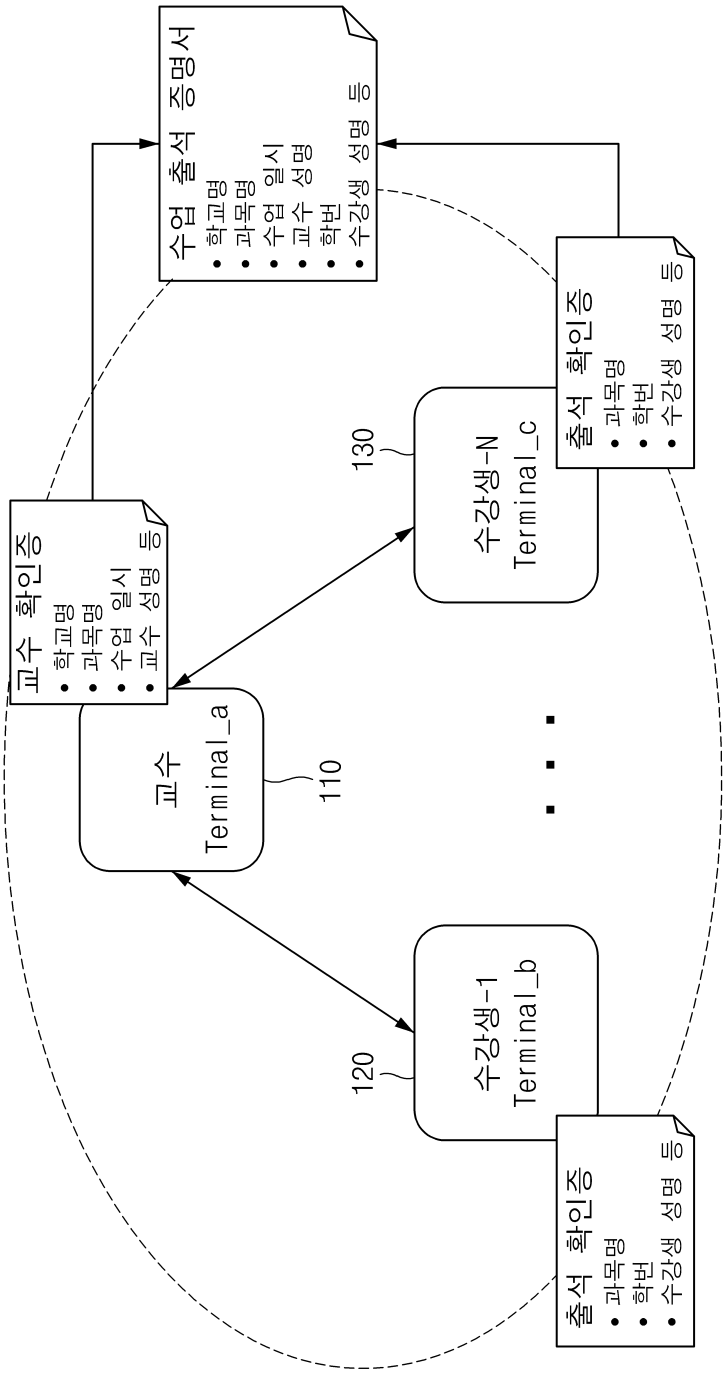
도면4


Terminal_a(110)
어플리케이션 구동
S110
Terminal_a의 이용자식별자,
공개키, 암호화키 사본,
단말기 식별자
OFF-CHAIN에 등록
S111
식별자 및 개인키로
서명된 증명서 교환
(S130)
OFF-CHAIN을 통하여
Terminal_b의 공개키로
Terminal_b의 증명서 검증
S112
Terminal_b(120)
어플리케이션 구동
S120
Terminal_b의 이용자식별자,
공개키, 암호화키 사본,
단말기 식별자
OFF-CHAIN에 등록
S121
OFF-CHAIN을 통하여
Terminal_a의 공개키로
Terminal_a의 증명서 검증
S122

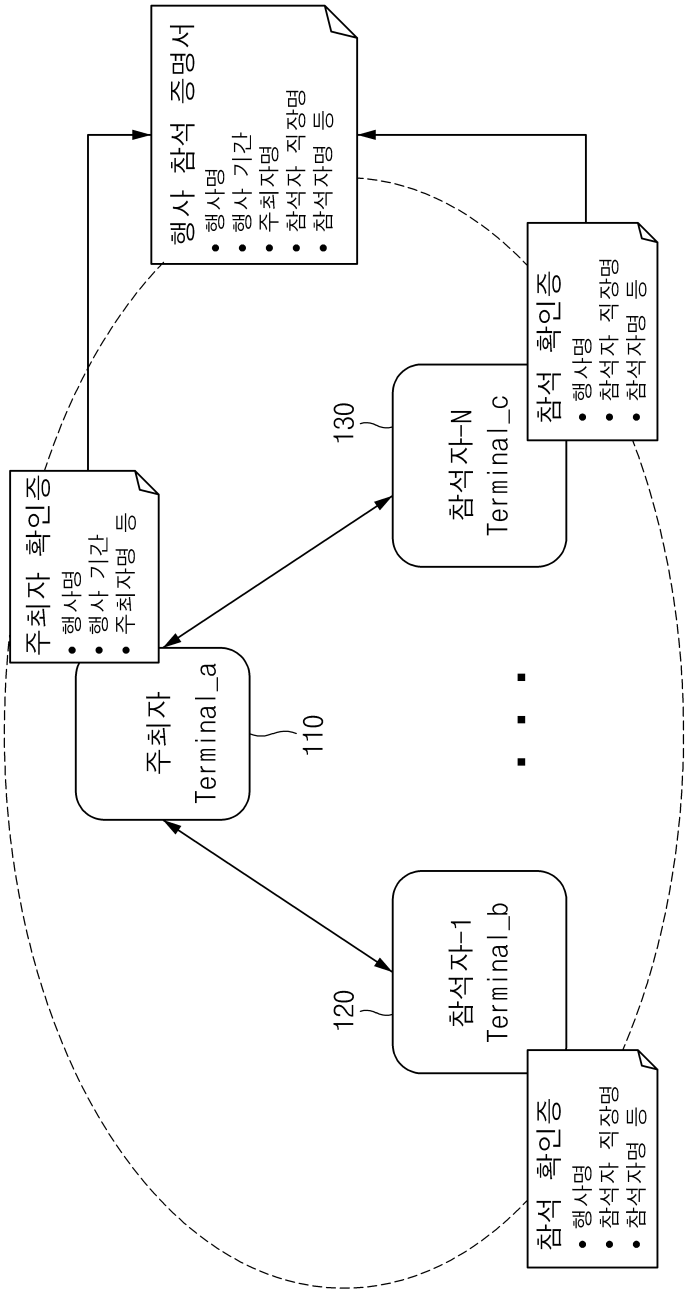
도면5


Terminal_a(운영자)
어플리케이션 활성화
S210
필수정보입력
S211
Terminal_a가 전자서명한 증명서 전송(S212)
Terminal_b가 전자서명한 증명서 전송(S222)
Terminal_b의 공개키로
Terminal_b의 증명서검증
S213
OK
Terminal_a와 Terminal_b가
공동으로 서명한 증명서 발급
S214
Terminal_b(방문객)
어플리케이션 활성화
S220
필수정보입력
S221
Terminal_a의 공개키로
Terminal_a의 증명서검증
S223
OK
Terminal_a와 Terminal_b가
공동으로 서명한 증명서 발급
S224

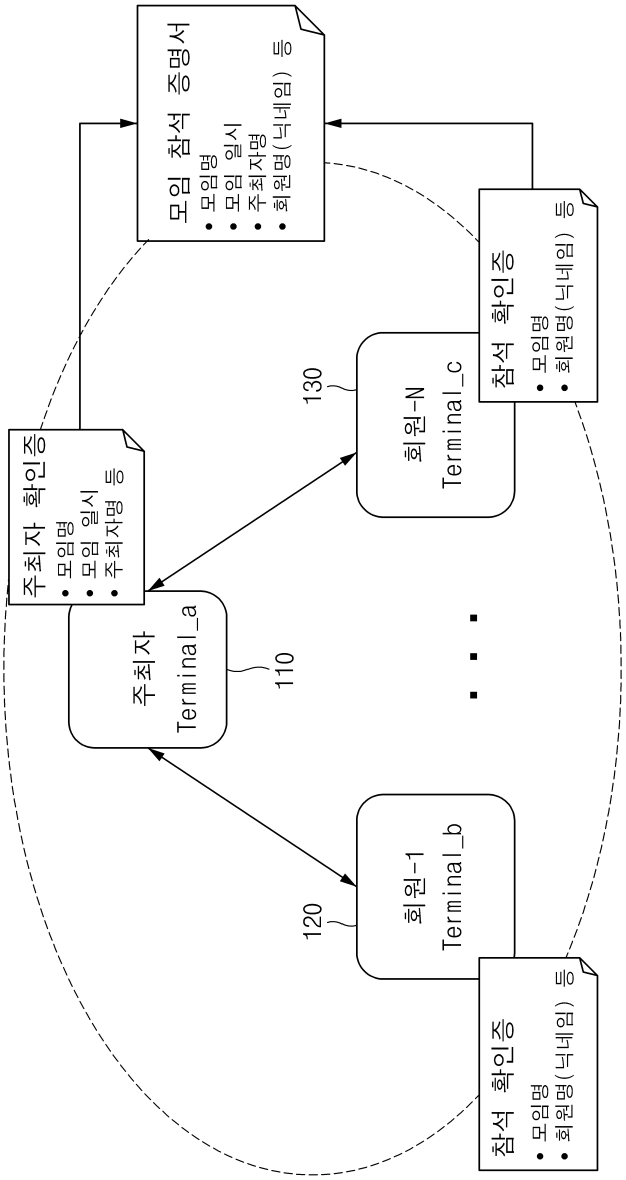
도면6


수업 출석 증명서
• 학교명
• 과목명
• 수업 일시
• 교수 성명
• 학번
• 수강생 성명 등
교수 확인증
• 학교명
• 과목명
• 수업 일시
• 교수 성명 등
교수
Terminal_a
110
수강생-1
Terminal_b
120
수강생-N
Terminal_c
130
출석 확인증
• 과목명
• 학번
• 수강생 성명 등
출석 확인증
• 과목명
• 학번
• 수강생 성명 등

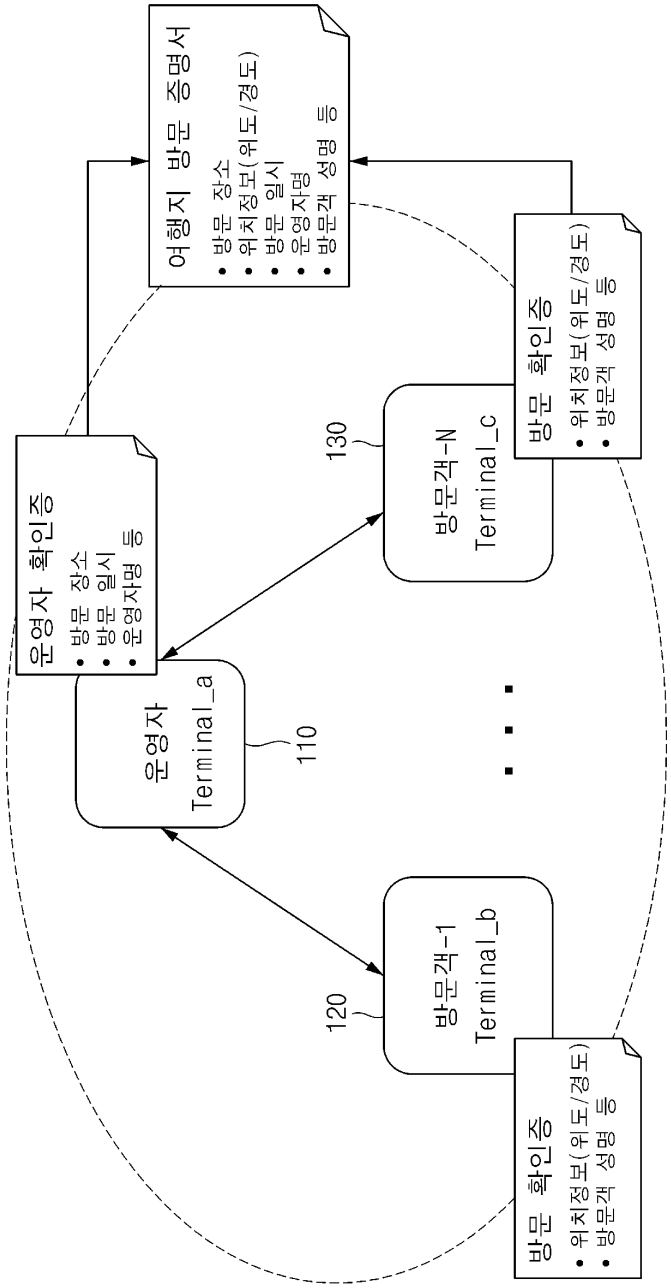
도면7


행사 참석 증명서
• 행사명
• 행사 기간
• 주최자명
• 참석자 직장명
• 참석자명 등
주최자 확인증
• 행사명
• 행사 기간
• 주최자명 등
주최자
Terminal_a
110
참석자-1
Terminal_b
120
참석자-N
Terminal_c
130
참석 확인증
• 행사명
• 참석자 직장명
• 참석자명 등
참석 확인증
• 행사명
• 참석자 직장명
• 참석자명 등

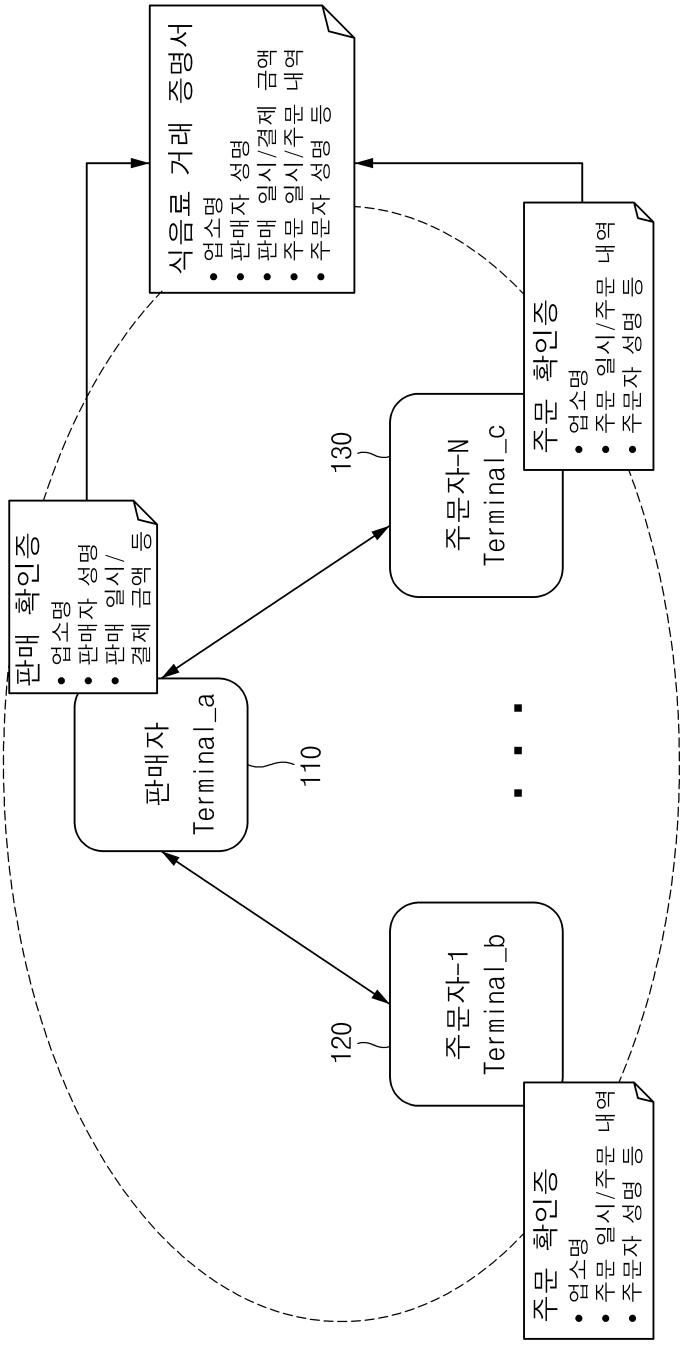
도면8


모임 참석 증명서
• 모임명
• 모임 일시
• 주최자명
• 회원명(닉네임) 등
주최자 확인증
• 모임명
• 모임 일시
• 주최자명 등
주최자
Terminal_a
110
회원-1
Terminal_b
120
회원-N
Terminal_c
130
참석 확인증
• 모임명
• 회원명(닉네임) 등
참석 확인증
• 모임명
• 회원명(닉네임) 등

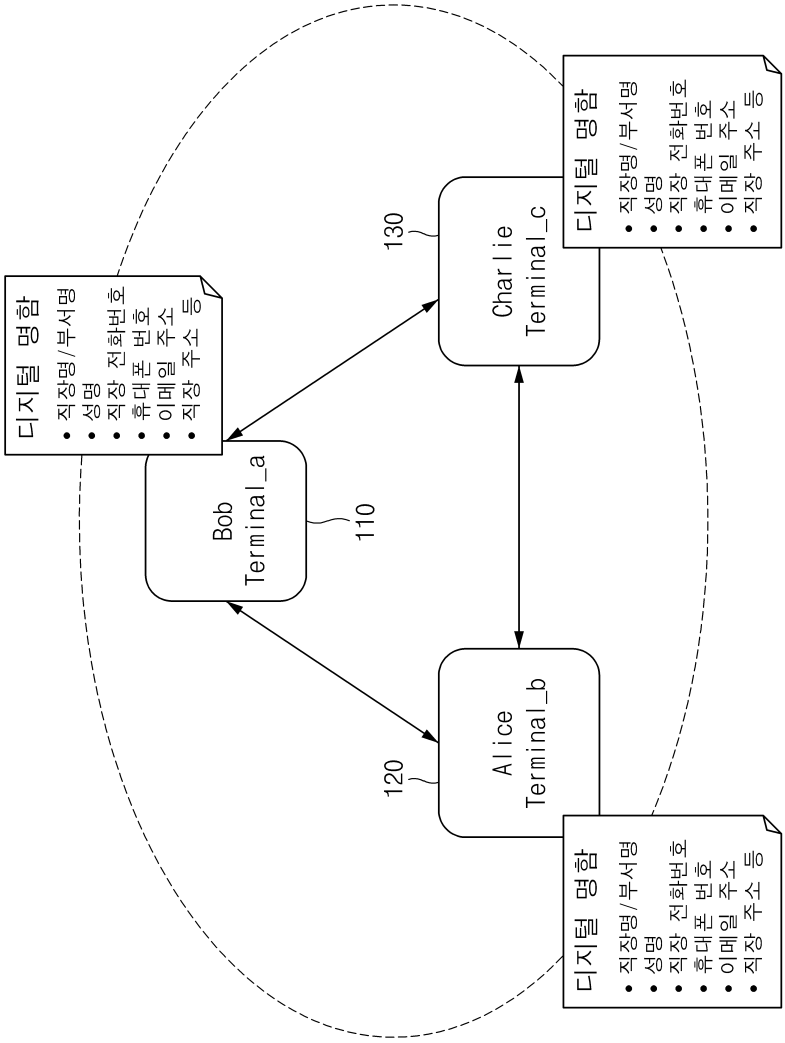
도면9


여행지 방문 증명서
• 방문 장소
• 위치정보(위도/경도)
• 방문 일시
• 운영자명
• 방문객 성명 등
운영자 확인증
• 방문 장소
• 방문 일시
• 운영자명 등
운영자
Terminal_a
110
방문객-1
Terminal_b
120
방문객-N
Terminal_c
130
방문 확인증
• 위치정보(위도/경도)
• 방문객 성명 등
방문 확인증
• 위치정보(위도/경도)
• 방문객 성명 등

도면10


식음료 거래 증명서
• 업소명
• 판매자 성명
• 판매 일시/결제 금액
• 주문 일시/주문 내역
• 주문자 성명 등
판매 확인증
• 업소명
• 판매자 성명
• 판매 일시/
결제 금액 등
판매자
Terminal_a
110
주문자-1
Terminal_b
120
주문자-N
Terminal_c
130
주문 확인증
• 업소명
• 주문 일시/주문 내역
• 주문자 성명 등
주문 확인증
• 업소명
• 주문 일시/주문 내역
• 주문자 성명 등

도면11


디지털 명함
• 직장명/부서명
• 성명
• 직장 전화번호
• 휴대폰 번호
• 이메일 주소
• 직장 주소 등
Bob
Terminal_a
110
130
Charlie
Terminal_c
120
Alice
Terminal_b
디지털 명함
• 직장명/부서명
• 성명
• 직장 전화번호
• 휴대폰 번호
• 이메일 주소
• 직장 주소 등
디지털 명함
• 직장명/부서명
• 성명
• 직장 전화번호
• 휴대폰 번호
• 이메일 주소
• 직장 주소 등