TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.0397

제정일 2023.12.06.

데이터 주권 강화를 위한 개인 간 신원확인시스템

Peer-to-peer Identification System for Data Sovereignty Enhancing

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 개인정보보호/ID관리, 블록체인 보안 프로젝트그룹(PG502)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위
표준(과제) 제안	박근덕	서울외국어대학원대학교	교수	PG502 특별위원
표준 초안 에디터	박근덕	서울외국어대학원대학교	교수	PG502 특별위원
	염흥열	순천향대학교	교수	PG502 특별위원
사무국 담당	박수정	TTA	수석	-

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다. 준용표준인 경우 해당 표준화기구 또는 단체의 웹사이트에서 이를 확인해야 합니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2023. 12. 06.

서 문

1 표준의 목적

이 표준의 목적은 데이터 주권(data sovereignty) 강화를 위한 개인(Peer) 간 신원확인시스템을 정의함에 있다. 중앙화된 신원 관리에서 개인 간 신원확인은 서비스 제공자가 운영하는 개인정보처리시스템을 통하여 구현되기 때문에 개인정보 처리에 대한 보안 위협이 존재한다. 또한 탈중앙화 신원 관리에서 발행자(Issuer)와 이용자(Holder)를 분리한 서비스 모델은 신원확인 보증 수준이 높은 증명서(예: 모바일 운전면허증, 백신접종증명서 등)를 다루기에 적합하다. 하지만 일상적인 생활에서 널리 사용되고 있는 증명서(예: 명함, 수업출석증명서, 행사참석증명서, 식음료거래증명서, 여행지방문증명서 등)는 신원확인 보증 수준이 낮으므로 발행자와 이용자를 각각 분리하지 않고 이용자가 직접 자신의 개인정보 등을 입력한 증명서를 발행 및 제출하여 개인 간 상호 신원을 확인할 수 있는 서비스 모델이 필요하다. 이러한 서비스 모델은 본 표준에서 정의한 근거리 무선통신을 이용한 개인 간 신원확인시스템을 통하여 구현될 수 있다.

2 주요 내용 요약

이 표준은 무선통신 모듈(예: Bluetooth, Wi-Fi Direct), 신원 증명서 관리 모듈, 개인정보 관리 모듈, 암호키 관리 모듈, 오프체인(off-chain), 온체인(on-chain) 등으로 구성되는 근거리 무선통신을 이용한 개인 간 신원확인시스템을 기술한다. 또한 해당 시스템에 대한 보안 위협을 식별하고 그에 대응하는 보안 요구사항을 기술한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

해당 사항 없음

3.2 인용 표준과 본 표준의 비교표

해당 사항 없음

Preface

1 Purpose

The standard is to define a peer-to-peer identification system for data sovereignty enhancing. In centralized identity management, since identification between individuals is implemented through the personal information processing system operated by the service provider, there are security threats to personal information processing. In decentralized identity management, a service model that separates the issuer and the holder is suitable for handling certificates with a high assurance level (e.g., mobile driver's license, vaccination certificate, etc.). But certificates that are widely used in everyday life (e.g., business cards, class attendance certificates, event attendance certificates, food and beverage transaction certificates, travel certificates, etc.) have a low assurance level. A service model that can issue certificates with a low assurance level and with PII(Personally Identifiable Information) by holders and verify mutual identities between peers by presenting the certificates to relying parties is needed. Holders can put their PII into the certificates. The service model can be implemented through a peer-to-peer identification system using short-range wireless communication defined in this standard.

2 Summary

The standard should specify a peer-to-peer identification system using short-range wireless communication including wireless communication module (e.g., Bluetooth, Wi-Fi Direct), certificate management module, PII management module, cryptographic key management module, off-chain, on-chain. It also identifies security threats to the system and specify security requirements against the identified security threats.

3 Relationship to Reference Standards

None

목 차

데이터 주권 강화를 위한 개인 간 신원확인시스템 (Peer-to-peer Identification System for Data Sovereignty Enhancing)

1 적용 범위

본 표준은 개인의 데이터 주권(data sovereignty) 강화를 위하여 근거리 무선통신을 이용한 개인 간 신원확인시스템을 정의한다. 또한 제안 시스템에 대한 보안 위협 식별 및 그에 대응하는 보안 요구사항을 기술하고 부록에 활용 사례를 제시한다.

2 인용 표준

해당 사항 없음

3 용어 정의

3.1 개인정보(personal information)

성명, 주민등록번호, 영상 등을 통하여 알아볼 수 있는 살아있는 개인에 대한 정보.
해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 결합하여 쉽게 알아볼 수 있는 정보와 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 가명정보를 포함.

3.2 데이터 주권(data sovereignty)

국가나 개인이 자기 데이터의 소유 범위와 사용 방법에 대하여 결정할 수 있는 권한.

3.3 블루투스(Bluetooth)

IEEE 802.15.1 에서 표준화된 무선 통신 기기 간에 가까운 거리에서 낮은 전력으로 무선 통신을 하기 위한 표준.

[출처(3.1~3.3)] TTA 정보통신용어사전

3.4 신뢰 당사자(RP, relying party)

일부 요청하는 행위 과정에서 요청/주장하는 실체에 의한 신원 표현 또는 주장에 의존하는 실체(An entity that relies on an identity representation or claim by a requesting/asserting entity within some request context).

[출처] ITU-T X.1252 (04/21)

3.5 신원정보(identity information)

하나의 실체를 다른 실체와 구별하는 속성 값의 집합(set of values of attributes that differentiate one entity from others).

3.6 신원확인 보증 등급

신원확인을 위한 증거에 의거해 실체의 신원확인 과정에 대한 신뢰 등급.

3.7 오프체인(off-chain)

블록체인 외에서 이루어진 프로세스 혹은 블록체인 외부에 저장된 데이터 등을 수식할 때 사용.

3.8 온체인(on-chain)

블록체인 내에서 이루어진 프로세스 혹은 블록체인 내의 데이터 등을 수식할 때 사용.

3.9 와이파이 다이렉트(Wi-Fi Direct)

무선 액세스 포인트(AP)를 통하지 않고 와이파이 기기 간 직접 통신하는 방식.

3.10 큐알코드(QR code, quick response code)

흑백 격자 무늬 패턴으로 정보를 나타내는 매트릭스 형식의 2차원 바코드의 한 가지.

[출처(3.6~3.10)] TTA 정보통신용어사전

4 약어

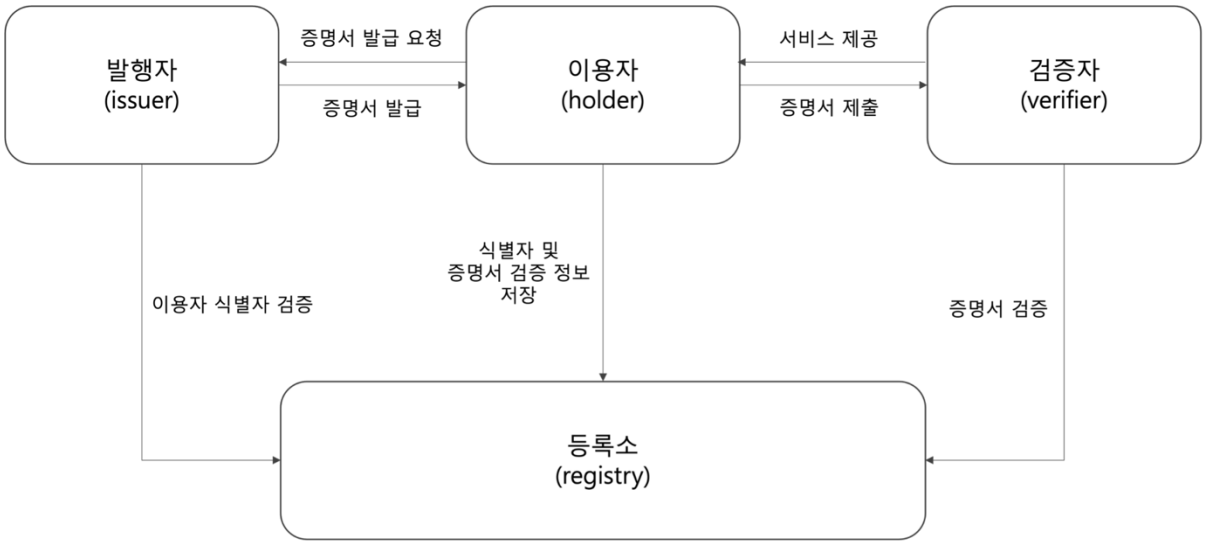
DLT	Distributed Ledger Technology
ID	Identity
QR	Quick Response

5 근거리 무선통신을 이용한 개인 간 신원확인시스템

5.1 기존의 분산 신원 관리 서비스 모델의 문제점

기존의 분산 신원 관리 서비스 모델은 발급자(issuer), 이용자(holder), 검증자(verifier), 등록소(registry) 등으로 구성된다. 발행자는 이용자의 요청에 의해 증명서를 발급한다.

이때 증명서의 유형에 따라 이용자는 발행자에게 개인정보를 제공한다. 이용자는 검증자에게 제출한 증명서를 검증할 수 있는 정보를 등록소에 저장하고, 발행자로부터 발급받은 증명서를 자신의 단말기에 저장 및 관리한다. 검증자는 등록소에 저장된 정보를 이용하여 이용자로부터 제출받은 증명서를 검증하고, 검증에 성공할 경우에 이용자에게 서비스를 제공한다. 등록소는 이용자의 식별자, 이용자 증명서를 검증할 수 있는 정보 등을 저장 및 관리하기 위하여 DLT 시스템을 이용할 수 있다.



(그림 5-1) 기존의 분산 신원 관리 서비스 모델 구성도

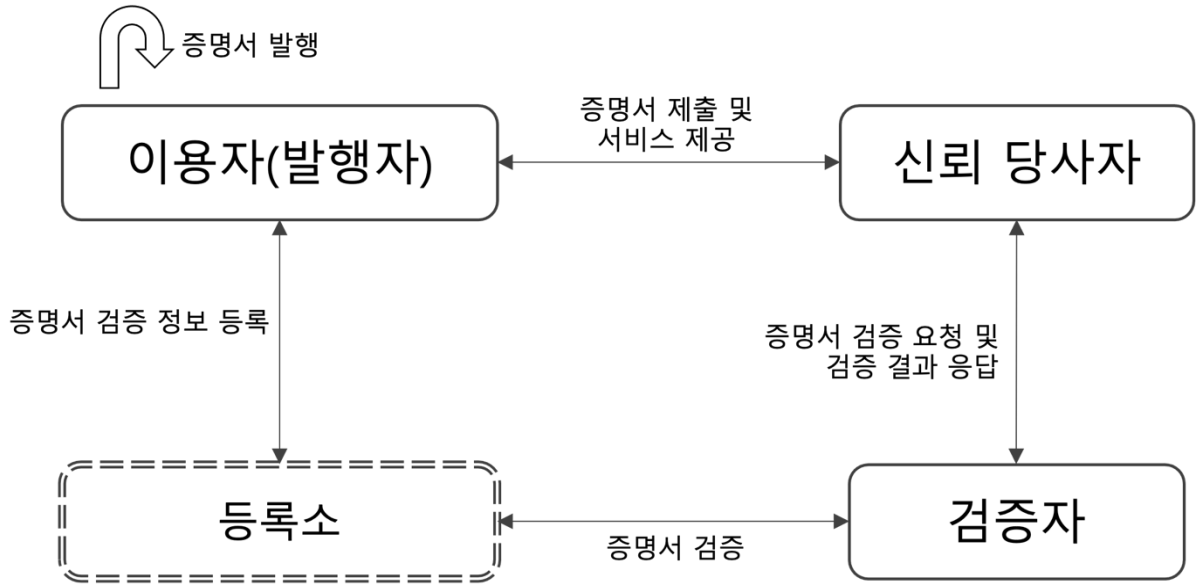
(그림 5-1)에서 기존의 분산 신원 관리 서비스 모델은 이용자 보호 측면에서 다음과 같은 몇 가지 문제점이 존재한다.

- 과도한 개인정보 제공: 이용자는 신원확인 보증 등급이 높은 증명서(예: 모바일 운전면허증, 백신접종증명서 등)를 발급받기 위하여 발행자에게 자신의 개인정보를 제공하여야 한다. 그러나 신원확인 보증 등급이 낮은 증명서(예: 디지털 명함 등)를 발급받기 위하여 발행자에게 자신의 개인정보를 제공하는 것은 과도한 개인정보 처리 행위이다.
- 과도한 개인정보 보관: 발행자가 신원확인 보증 등급이 낮은 증명서를 발행하기 위하여 수집한 이용자의 개인정보를 보관하는 것은 과도한 개인정보 처리 행위이다.
- 손쉬운 증명서 도용: 이용자가 큐알코드(QR code)를 활용하여 증명서를 검증자에게 제출하는 경우에 증명서 복제가 용이하고 이용자는 자신의 신원을 타인에게 제공하거나 자신의 신원을 도용 당할 수 있다.
- 개인정보 유출: 이용자가 큐알코드(QR code)를 활용하여 증명서를 검증자에게 제출하는 경우에 통상적인 큐알코드 스캐너(scanner)를 통하여 이용자의 개인정

보가 유출되는 것이 용이하고, 유출된 개인정보를 악용한 신원 도용 등 2차 피해가 발생할 수 있다.

5.2 셀프-발행 모델

셀프-발행 모델은 이용자가 직접 자신의 개인정보 등을 입력하여 신원확인 보증 등급이 낮은 증명서(예: 디지털 명함 등)를 발행할 수 있는 탈중앙화 신원 관리 모델이다. 셀프-발행 모델은 이용자(발행자), 신뢰 당사자, 검증자, 등록소 등으로 구성된다. 신뢰 당사자와 검증자는 동일한 실체가 될 수 있다.



(그림 5-2) 셀프-발행 모델 구성도

(그림 5-2)에서 셀프-발행 모델의 주요 구성 요소의 역할은 다음과 같다.

- 이용자(발행자): 이용자 자신의 개인정보 등을 입력한 증명서를 스스로 발행하여 신뢰 당사자에게 제출하고, 제출한 증명서 검증 결과에 따라 서비스를 제공받는다. 또한 자신이 발행한 증명서를 검증할 수 있는 정보(예: 이용자의 식별자, 이용자의 공개키, 증명서 유효 기간 등)를 등록소에 등록한다.
- 신뢰 당사자: 이용자로부터 제출받은 증명서를 검증자에게 전송하여 해당 증명서의 진위성, 유효성 등에 대한 검증을 요청한다. 검증자로부터 전송받은 증명서 검증 결과에 따라 이용자에게 서비스를 제공할 수 있다.
- 검증자: 등록소에 등록되어 있는 증명서 검증 정보를 활용하여 이용자가 제출한 증명서의 진위성, 유효성 등을 검증하고 그 결과를 신뢰 당사자에게 전송한다.
- 등록소: 이용자(발행자)가 등록한 증명서 검증 정보(예: 이용자의 식별자, 이용자의 공개키, 증명서 유효 기간 등)를 관리한다. 이용자가 제출한 증명서의 검증을

위하여 검증자에게 해당 증명서의 진위성, 유효성 등에 관한 검증 정보를 제공한다. 등록소는 DLT 시스템 또는 non-DLT 시스템으로 구현될 수 있다.

5.3 제안 시스템

근거리 무선통신을 이용한 개인 간 신원확인시스템은 무선통신 모듈, 신원 증명서 관리 모듈, 개인정보 관리 모듈, 암호키 관리 모듈, 오프체인(off-chain), 온체인(on-chain) 등으로 구성된다.

제안 시스템은 다음과 사항을 통하여 이용자의 데이터 주권을 강화한다.

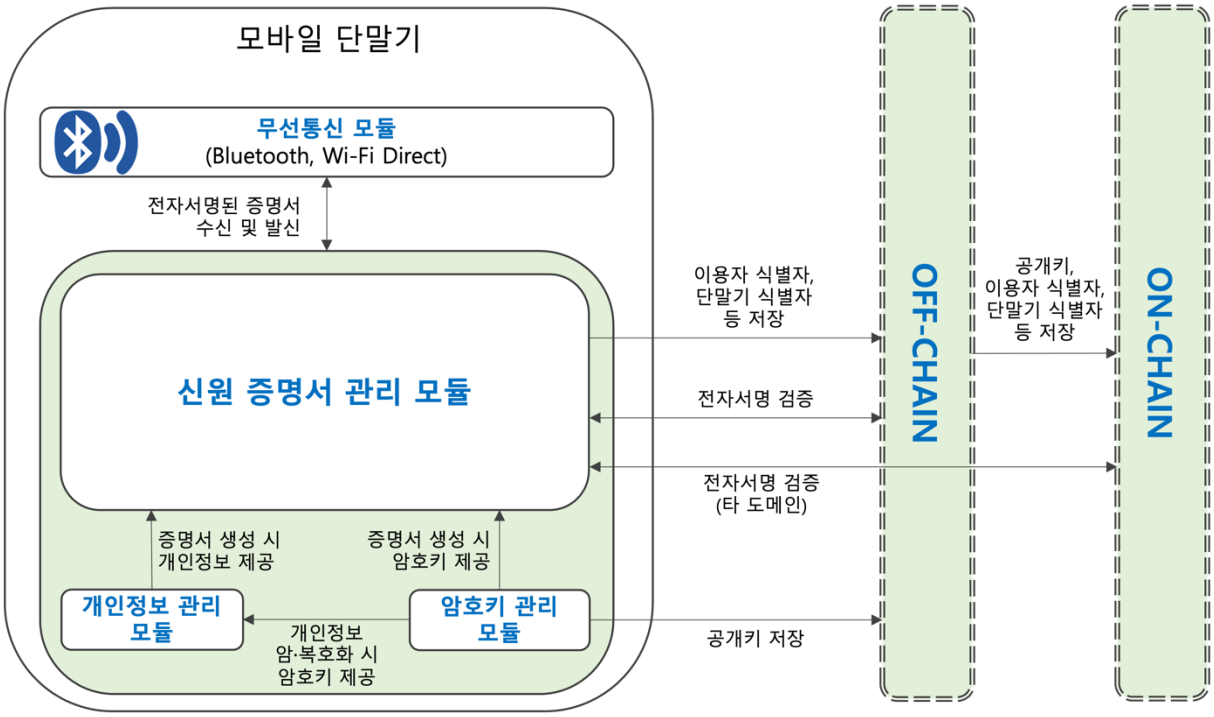
- 제안 시스템에서는 발행자(issuer)와 이용자(holder)가 동일한 실체이기 때문에 이용자의 증명서 발급 시 필요한 개인정보를 별도의 발행자에게 제공하지 않는다.
- 이용자의 개인정보는 이용자 자신이 소유한 모바일 단말기에서만 처리되기 때문에 이용자는 개인정보에 대한 완전한 통제권을 가진다.
- 이용자의 개인정보는 오프체인, 온체인에서 처리되지 않는다.

(그림 5-3)에서 제안 시스템의 주요 구성 요소의 역할은 다음과 같다.

- 무선통신 모듈: 모바일 단말기를 소유한 개인 간 신원확인을 위하여 쌍방의 신원 증명서를 근거리(예: 반경 40미터 이내)에서 무선으로 송수신 한다. 모바일 단말기 간 직접 연결이 가능한 블루투스(Bluetooth)나 와이파이 다이렉트(Wi-Fi Direct) 등을 이용한다. 블루투스 통신은 모바일 단말기 간의 거리 측정과 저용량 데이터 전송 등에 활용될 수 있고, 와이파이 다이렉트 통신은 모바일 단말기 간의 대용량 데이터 전송 등에 활용될 수 있다.
- 신원 증명서 관리 모듈: 모바일 단말기를 소유한 개인(이용자) 간 신원확인을 위하여 자신의 신원 증명서를 생성, 저장 및 관리한다. 또한 타인의 모바일 단말기로부터 수신한 신원 증명서를 저장 및 관리한다. 신원 증명서는 이용자 자신의 개인키로 전자서명한 증명서(개인정보 포함) 이다. 무선통신 모듈을 통하여 신원 증명서를 수신 및 발신한다. 이용자 식별자, 단말기 식별자 등을 오프체인(off-chain)에 제공한다. 오프체인 및 온체인에 저장되어 있는 정보(예: 이용자 식별자, 이용자의 공개키, 단말기 식별자 등)를 활용하여 타인의 신원 증명서의 진위성 및 유효성 등을 검증한다.
- 개인정보 관리 모듈: 모바일 단말기의 소유자가 정보주체로서 직접 자신의 개인정보를 저장 및 관리한다. 개인정보는 암호키 관리 모듈에 보관되어 있는 암호키로 암호화 및 복호화 된다. 신원 증명서 생성 시 신원 증명서 관리 모듈에게 개인정보를 제공한다.
- 암호키 관리 모듈: 모바일 단말기 소유자의 신원 증명서 생성에 필요한 전자서명

을 하기 위한 공개키/개인키 쌍을 생성 및 관리한다. 또한 모바일 단말기 소유자의 개인정보를 암호화 및 복호화 하기 위한 암호키를 생성 및 관리한다. 신원 증명서 생성 시 신원 증명서 관리 모듈에게 개인키를 제공한다. 개인정보 암호화 및 복호화 시 개인정보 관리 모듈에게 암호키를 제공한다. 공개키를 오프체인(off-chain)에게 제공한다.

- 오프체인(off-chain): 동일한 도메인에 속한 개인 간 신원확인을 위하여 상대방의 신원 증명서 검증(예: 진위성, 유효성 등)이 필요한 이용자가 접근할 수 있는 저장소로서 이용자 식별자, 모바일 단말기 식별자, 이용자의 공개키 등을 저장 및 관리하고, 이용자의 개인정보는 저장하지 않는다. 이용자의 공개키, 이용자 식별자, 단말기 식별자 등을 온체인(on-chain)에게 제공한다.
- 온체인(on-chain): 개인 간 신원확인이 필요한 이용자가 서로 다른 도메인에 속하는 경우에 상대방의 신원 증명서 검증(예: 진위성, 유효성 등)이 필요한 이용자가 접근할 수 있는 저장소로서 이용자 식별자, 모바일 단말기 식별자, 이용자의 공개키 등을 저장 및 관리하고, 이용자의 개인정보는 저장하지 않는다.

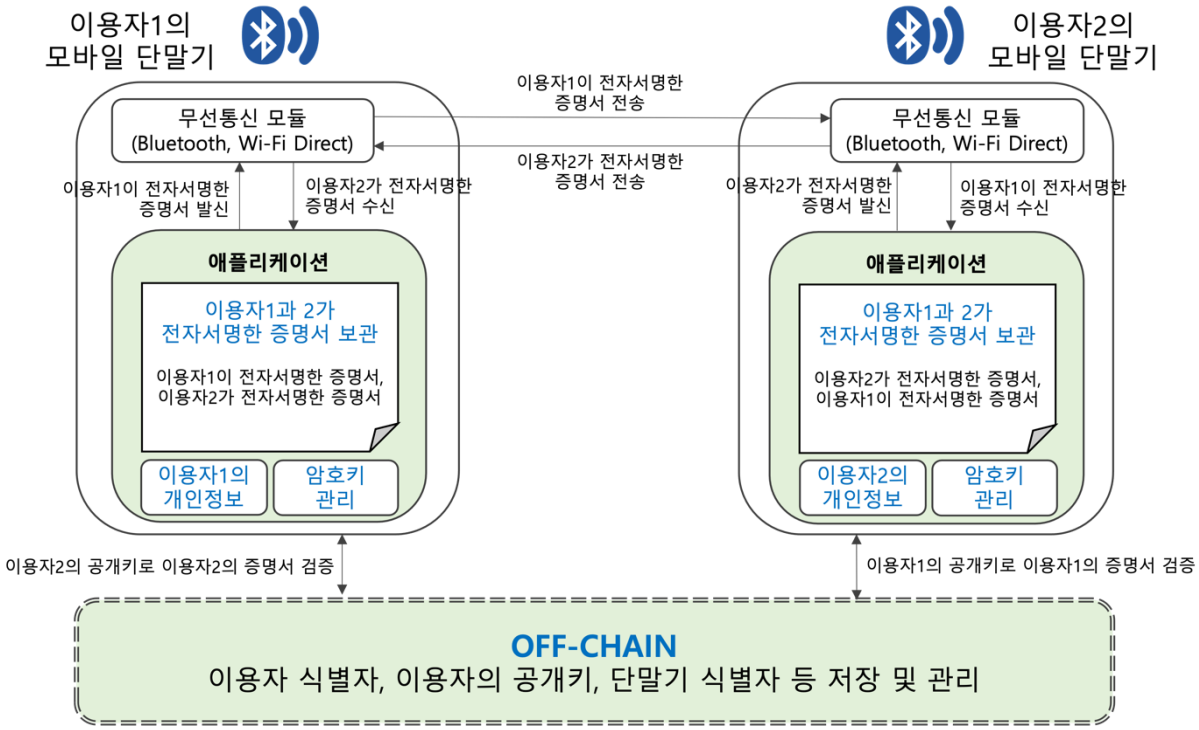


(그림 5-3) 근거리 무선통신을 이용한 개인 간 신원확인시스템 아키텍처

단일 도메인(예: 단일 사업자)에서 제안 시스템을 적용하는 경우에 이용자의 신원 증명서를 검증할 수 있는 정보를 저장 및 관리하는 저장소로서 오프체인을 활용하더라도 이용자 간의 신원확인을 수행할 수 있고, 온체인을 활용하는 것보다 비용도 절감할 수 있다. 또한 복수 도메인(예: 복수 사업자)에서 제안 시스템을 적용하는 경우에 각 도메인별 이용자의 신원 증명서를 검증할 수 있는 정보를 저장 및 관리하는 저장소의 상호운용성을 제공하기 위하여 온체인을 활용한다.

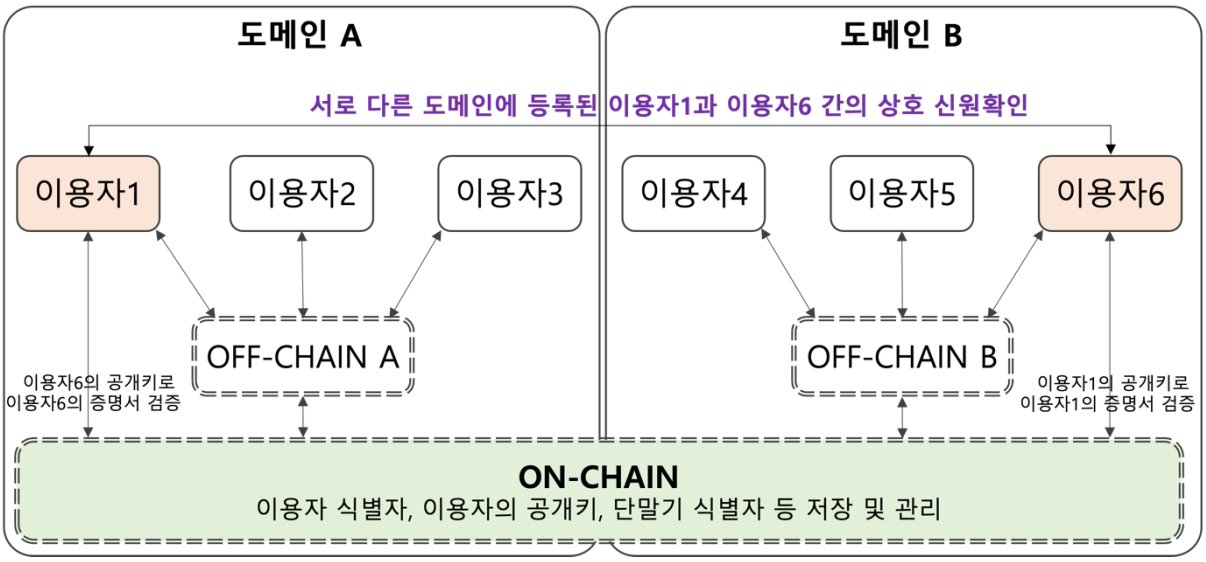
기존의 중앙화 신원 관리에서는 사업자가 이용자의 개인정보 및 신원정보를 보유하고 있어 이용자 간의 신원확인은 사업자가 수행하고 그 결과를 이용자에게 알려준다. 그러나 제안 시스템의 오프체인은 이용자의 신원 증명서를 검증할 수 있는 정보를 저장 및 관리하는 일종의 저장소 역할만 할 뿐이고 이용자 간의 신원확인은 당사자간에 직접 이루어지므로 탈중앙화 신원 관리의 주요한 구성 요소가 된다.

(그림 5-4)에서 동일한 도메인 내 이용자1과 이용자2는 서로의 신원확인을 하기 위하여 모바일 단말기의 근거리(예: 반경 40미터 이내) 무선통신 모듈을 통하여 이용자1 및 이용자2가 각각 상대방이 전자서명한 증명서를 송수신하고, 오프체인(off-chain)에 저장되어 있는 이용자1 및 이용자2의 정보(예: 이용자 식별자, 이용자의 공개키, 단말기 식별자 등)를 활용하여 상대방의 신원 증명서를 검증한다.



(그림 5-4) 동일한 도메인 내 제안 시스템 운용 구성도

(그림 5-5)에서 도메인 A에 등록된 이용자1과 도메인 B에 등록된 이용자6은 서로의 신원확인을 하기 위하여 온체인(on-chain)에 저장되어 있는 이용자1 및 이용자6의 정보(예: 이용자 식별자, 이용자의 공개키, 단말기 식별자 등)를 활용하여 상대방의 신원 증명서를 검증한다.



(그림 5-5) 도메인 간 제안 시스템의 상호 운용 구성도

6 보안 위협 및 보안 요구사항

6.1 보안 위협

근거리 무선통신을 이용한 개인 간 신원확인시스템에서 발생할 수 있는 보안 위협(ST, security threat)을 다음과 같이 식별한다. 다만, IT 시스템에서 발생할 수 있는 일반적인 보안 위협은 제외한다.

- (ST-1) 신원정보 위조: 이용자는 제안 시스템을 통하여 증명서 생성 시 자신의 개인정보(예: 성명, 휴대폰 전화번호, 이메일 주소 등)를 사실과 다르게 등록할 수 있다. 허위 또는 위조된 개인정보를 포함한 증명서는 타인의 신원을 도용할 수 있다.
- (ST-2) 개인정보 유출: 모바일 단말기 도난 및 분실, 모바일 단말기 해킹 등을 통하여 모바일 단말기에 저장하고 있는 본인 및 타인의 증명서에 포함된 개인정보가 유출될 수 있다. 또한 모바일 단말기 간 근거리 무선통신(블루투스 및 와이파이 다이렉트)을 통하여 증명서 교환 시 본인 및 타인의 증명서에 포함된 개인정보가 유출될 수 있다.
- (ST-3) 암호키 분실: 모바일 단말기 도난 및 분실, 모바일 단말기 장애 등을 통하여 모바일 단말기에 보관하고 있는 암호키(개인정보 암호키) 및 개인키(증명서 전자서명 키) 등이 분실될 수 있다.
- (ST-4) 근거리 무선통신 장애: 모바일 단말기에 설치되어 있는 근거리 무선통신 모듈(블루투스 및 와이파이 다이렉트)의 취약점으로 인하여 모바일 단말기 간의 신원 증명서 송수신 장애가 발생할 수 있다.
- (ST-5) 정당한 수신자로 가장: 모바일 단말기에 설치되어 있는 근거리 무선통신

모듈(블루투스 및 와이파이 다이렉트)의 송수신 반경 내에 위치한 악의적인 수신자가 타인의 증명서를 무단으로 수집할 수 있다.

6.2 보안 요구사항

근거리 무선통신을 이용한 개인 간 신원확인시스템에서 발생할 수 있는 보안 위협에 대응할 수 있는 보안 요구사항(SR, security requirement)은 다음과 같다.

- (SR-1) 본인 확인: 이용자가 증명서를 생성하기 위하여 개인정보(예: 성명, 휴대폰 전화번호, 이메일 주소 등)를 입력하는 경우에 최소한의 본인 확인을 수행한다. 통신사 본인 확인 서비스를 통하여 이용자가 입력한 성명, 휴대폰 전화번호 등의 진위 여부를 확인할 수 있다. 또한 이메일 본인 확인 서비스를 통하여 이용자가 입력한 이메일 주소의 진위 여부를 확인할 수 있다.
- (SR-2) 데이터 암호화: 모바일 단말기에 본인 및 타인의 증명서를 저장 시 증명서에 포함된 개인정보를 안전한 암호알고리즘으로 암호화한다. 또한 모바일 단말기 간에 근거리 무선통신(블루투스 및 와이파이 다이렉트)을 이용하여 증명서를 송수신하는 경우에 증명서에 포함된 개인정보를 안전한 암호알고리즘으로 암호화한다. 개인정보 저장 및 전송 시 이용하는 암호키는 안전하게 관리한다.
- (SR-3) 접근 통제: 모바일 단말기에 설치되어 있는 타 애플리케이션에서 본인 및 타인의 증명서에 포함된 개인정보에 무단으로 접근하지 못하도록 통제한다. 모바일 단말기 제조사에서 제공하는 애플리케이션 간 접근 통제 기능을 활용할 수 있다.
- (SR-4) 데이터 백업: 모바일 단말기 제조사에서 제공하는 백업 및 복구 기능을 이용하여 중요한 데이터(예: 증명서, 개인정보, 암호키 등)를 안전하게 백업 및 복구한다.
- (SR-5) 패치 관리: 모바일 단말기 제조사 또는 근거리 무선통신 모듈(블루투스 및 와이파이 다이렉트) 제조사에서 주기적으로 제공하는 보안 패치, 업데이트 등을 설치한다.
- (SR-6) 무선통신 반경 최소화: 모바일 단말기에 설치되어 있는 근거리 무선통신 모듈(블루투스 및 와이파이 다이렉트)의 송수신 반경을 최소화하여 타인의 증명서 수신을 제한한다.

<표 6-1> 보안 위협과 보안 요구사항 간의 관계

구분	SR-1 본인 확인	SR-2 데이터 암호화	SR-3 접근 통제	SR-4 데이터 백업	SR-5 패치 관리	SR-6 무선통신 반경 최소화
ST-1 신원정보 위조	O					
ST-2 개인정보 유출		O	O			

구분	SR-1 본인 확인	SR-2 데이터 암호화	SR-3 접근 통제	SR-4 데이터 백업	SR-5 패치 관리	SR-6 무선통신 반경 최소화
ST-3 암호키 분실				O		
ST-4 근거리 무선통신 장애					O	
ST-5 정당한 수신자로 가장						O

(※ ST=보안 위협, SR=보안 요구사항)

SR-1(본인 확인)은 ST-1(신원정보 위조)를 방지할 수 있다. SR-2(데이터 암호화) 및 SR-3(접근 통제)는 ST-2(개인정보 유출)을 방지할 수 있다. SR-4(데이터 백업)은 ST-3(암호키 분실)을 방지할 수 있고, SR-5(패치 관리)는 ST-4(근거리 무선통신 장애)를 방지할 수 있다. SR-6(무선통신 반경 최소화)는 ST-5(정당한 수신자로 가장)을 방지할 수 있다.

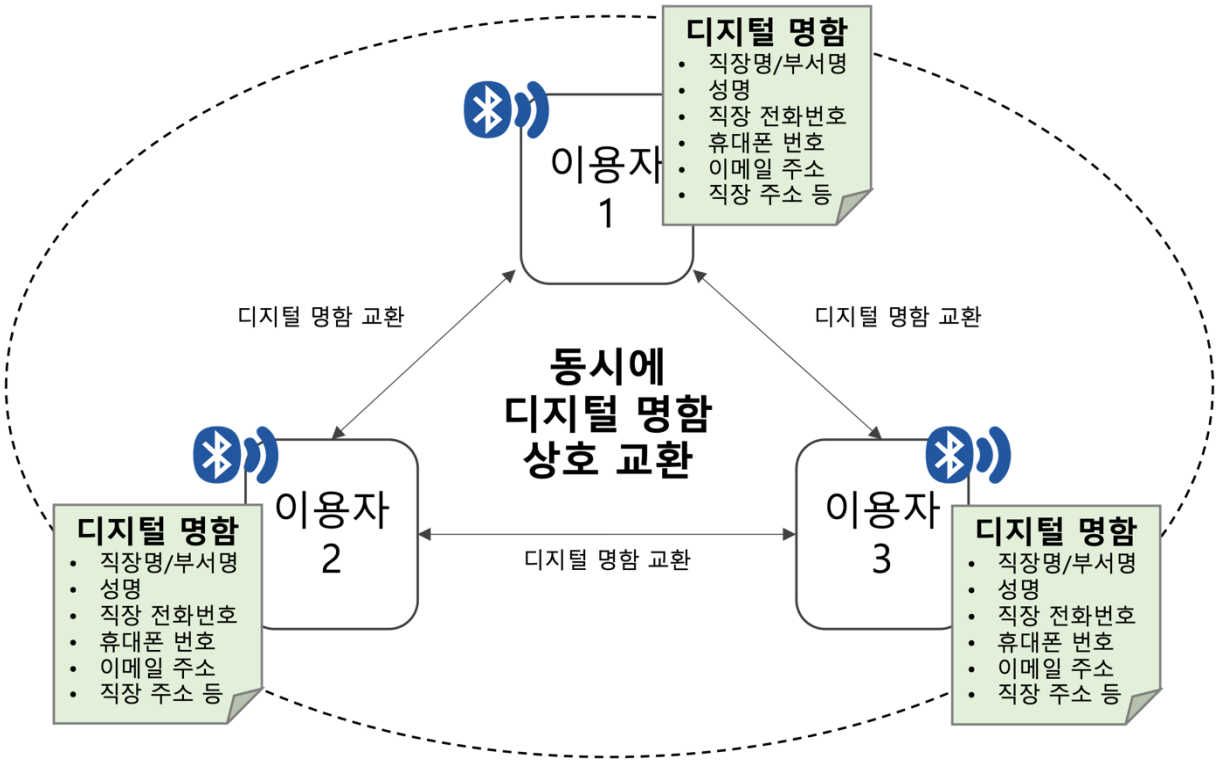
부 록 Ⅰ

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

활용 사례

Ⅰ.1 디지털 명함

(그림 Ⅰ.1-1)에서 다수의 이용자는 제안 시스템을 활용하여 디지털 명함을 상호 교환할 수 있다. 이용자는 자신의 모바일 단말기에서 직장명/부서명, 성명, 직장 전화번호, 휴대폰 번호, 이메일 주소, 직장 주소 등을 직접 입력한 디지털 명함을 생성 및 관리할 수 있다. 이용자는 타인의 모바일 단말기로부터 수신한 디지털 명함을 자신의 모바일 단말기에 저장 및 관리할 수 있다. 실물 명함을 제작 및 보관하는 비용을 절감할 수 있고, 실물 명함을 지참하고 있지 않더라도 즉석에서 디지털 명함을 생성하여 타인에게 제공할 수 있다.

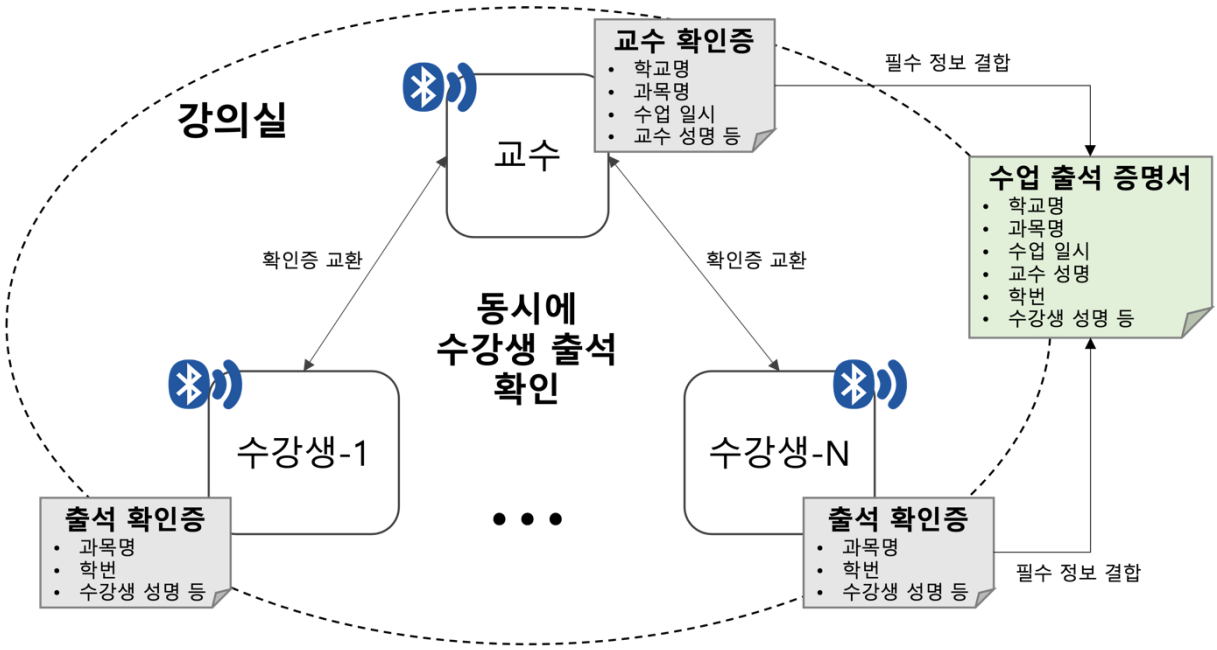


(그림 Ⅰ.1-1) 디지털 명함 운용 구성도

제안 시스템을 활용하는 이용자들의 모바일 단말기는 블루투스 및 와이파이 다이렉트 연결이 원활하도록 근거리(예: 반경 40미터 이내 등)에 위치하여야 한다.

Ⅰ.2 수업 출석 증명서

(그림 I.2-1)에서 교수와 수강생은 제안 시스템을 활용하여 교수 확인증 및 출석 확인증을 상호 교환하여 결합함으로써 수업 출석 증명서를 발급할 수 있다. 교수는 자신의 모바일 단말기에서 학교명, 과목명, 수업 일시, 교수 성명 등을 직접 입력한 교수 확인증을 생성하여 수강생에게 전송할 수 있다. 수강생은 자신의 모바일 단말기에서 과목명, 학번, 수강생 성명 등을 직접 입력한 출석 확인증을 생성하여 교수에게 전송할 수 있다. 교수 및 수강생은 타인의 모바일 단말기로부터 수신한 교수 확인증 및 출석 확인증을 자신의 모바일 단말기에 저장 및 관리할 수 있다. 교수는 다수의 수강생에 대한 수업 출석 여부를 확인하는 시간을 절감할 수 있고, 강의실에 입장하지 않은 수강생은 수업 출석 증명서를 발급받을 수 없다.



(그림 I.2-1) 수업 출석 증명서 운용 구성도

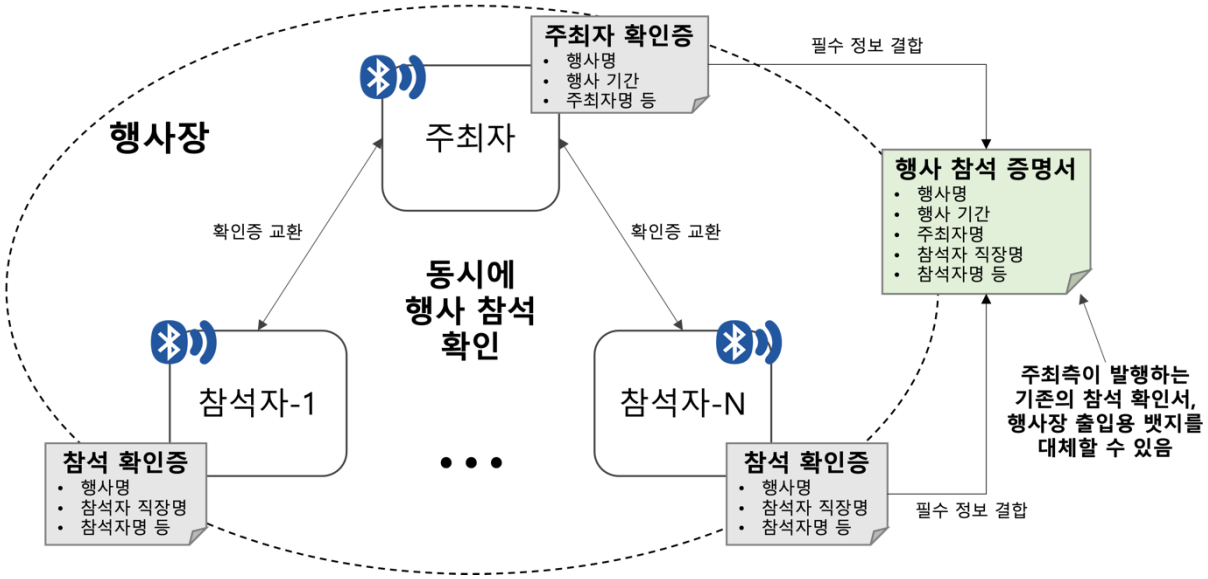
제안 시스템을 이용하는 교수와 수강생의 모바일 단말기는 블루투스 및 와이파이 다이렉트 연결이 원활하도록 근거리(예: 반경 40미터 이내 등)에 위치하여야 한다.

Ⅰ.3 행사 참석 증명서

(그림 I.3-1)에서 행사 주최자와 참석자는 제안 시스템을 활용하여 주최자 확인증 및 참석 확인증을 상호 교환하여 결합함으로써 행사 참석 증명서를 발급할 수 있다. 주최자는 자신의 모바일 단말기에서 행사명, 행사 기간, 주최자명 등을 직접 입력한 주최자 확인증을 생성하여 참석자에게 전송할 수 있다. 참석자는 자신의 모바일 단말기에서 행사명, 참석자 직장명, 참석자명 등을 직접 입력한 참석 확인증을 생성하여 주최자에게 전송할 수

있다. 주최자 및 참석자는 타인의 모바일 단말기로부터 수신한 주최자 확인증 및 참석 확인증을 자신의 모바일 단말기에 저장 및 관리할 수 있다. 주최자는 다수의 참석자에 대한 행사 참석 여부를 확인하는 시간을 절감할 수 있고, 행사장에 입장하지 않은 참석자는 행사 참석 증명서를 발급받을 수 없다.

제안 시스템을 활용한 행사 참석 증명서는 주최자가 발행하는 기존의 참석 확인서, 행사장 출입용 배지 등을 대체할 수 있다.

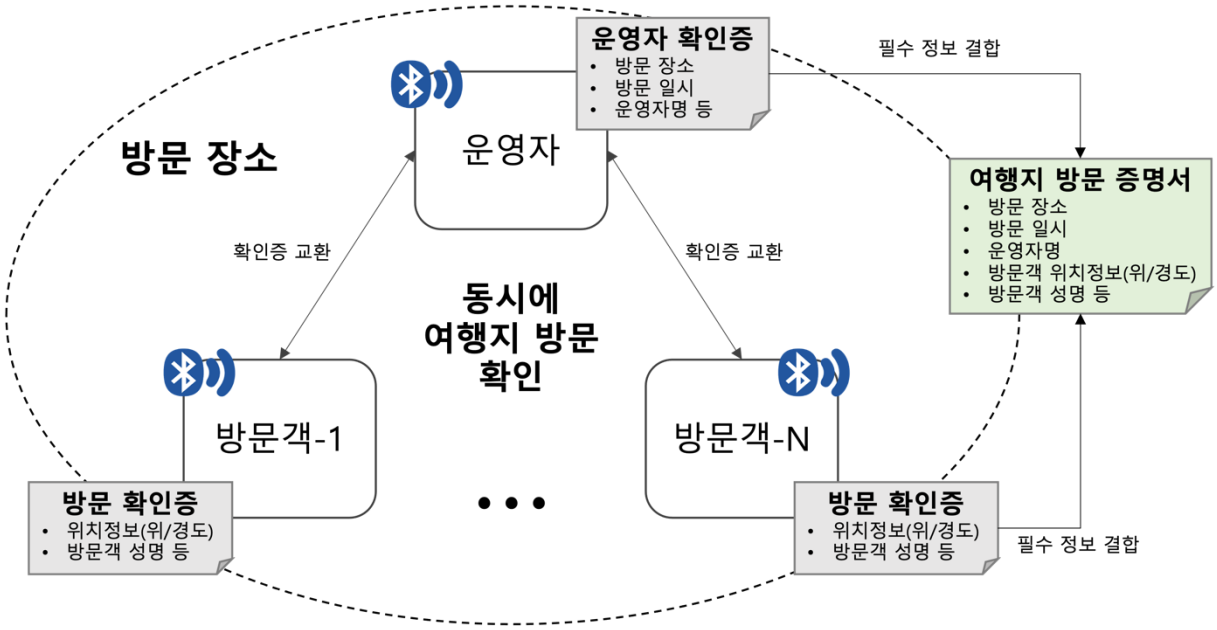


(그림 I.3-1) 행사 참석 증명서 운용 구성도

제안 시스템을 이용하는 행사 주최자와 참석자의 모바일 단말기는 블루투스 및 와이파이 다이렉트 연결이 원활하도록 근거리(예: 반경 40미터 이내 등)에 위치하여야 한다.

I.4 여행지 방문 증명서

(그림 I.4-1)에서 여행지 사무소 운영자와 방문객은 제안 시스템을 활용하여 운영자 확인증 및 방문 확인증을 상호 교환하여 결합함으로써 여행지 방문 증명서를 발급할 수 있다. 운영자는 자신의 모바일 단말기에서 방문 장소, 방문 일시, 운영자명 등을 직접 입력한 운영자 확인증을 생성하여 방문객에게 전송할 수 있다. 방문객은 자신의 모바일 단말기에서 위치정보(위도/경도), 방문객 성명 등을 직접 입력한 방문 확인증을 생성하여 운영자에게 전송할 수 있다. 운영자 및 방문객은 타인의 모바일 단말기로부터 수신한 운영자 확인증 및 방문 확인증을 자신의 모바일 단말기에 저장 및 관리할 수 있다. 운영자는 다수의 방문객에 대한 여행지 방문 여부를 확인(예: 스탬프 날인 등)하는 시간을 절감할 수 있고, 여행지 사무소에 도착하지 않은 방문객은 여행지 방문 증명서를 발급받을 수 없다.



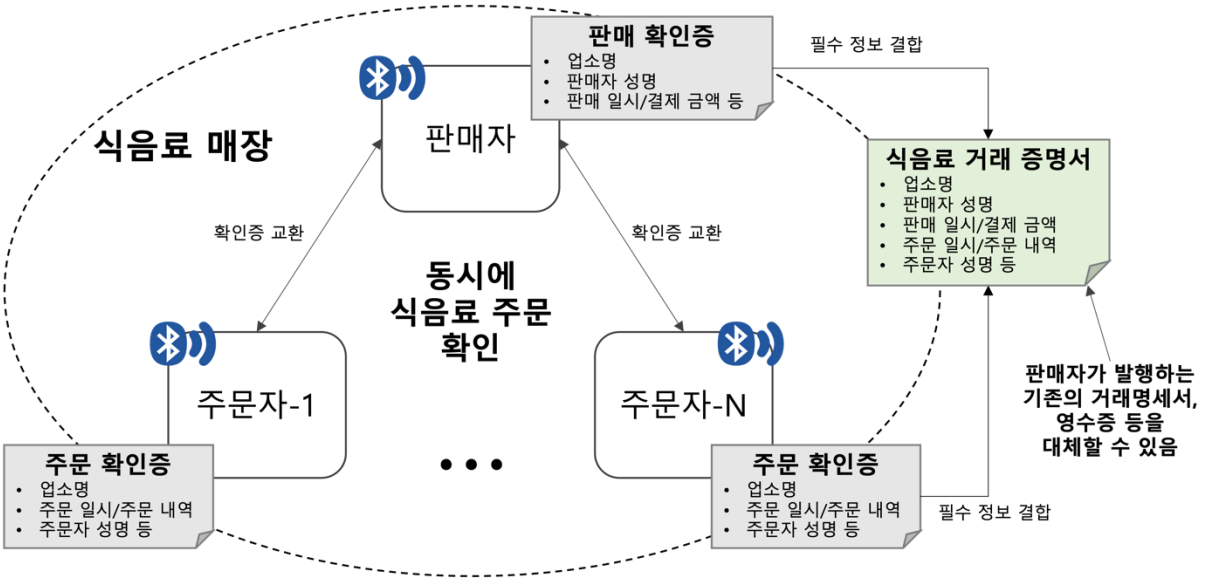
(그림 I.4-1) 여행지 방문 증명서 운용 구성도

제안 시스템을 이용하는 여행지 사무소 운영자와 방문객의 모바일 단말기는 블루투스 및 와이파이 다이렉트 연결이 원활하도록 근거리(예: 반경 40미터 이내 등)에 위치하여야 한다.

I.5 식음료 거래 증명서

(그림 I.5-1)에서 식음료 판매자와 주문자는 제안 시스템을 활용하여 판매 확인증 및 주문 확인증을 상호 교환하여 결합함으로써 식음료 거래 증명서를 발급할 수 있다. 판매자는 자신의 모바일 단말기에서 업소명, 판매자 성명, 판매 일시, 결제 금액 등을 직접 입력한 판매 확인증을 생성하여 주문자에게 전송할 수 있다. 주문자는 자신의 모바일 단말기에서 업소명, 주문 일시, 주문 내역, 주문자 성명 등을 직접 입력한 주문 확인증을 생성하여 판매자에게 전송할 수 있다. 판매자 및 주문자는 타인의 모바일 단말기로부터 수신한 판매 확인증 및 주문 확인증을 자신의 모바일 단말기에 저장 및 관리할 수 있다. 판매자는 다수의 주문자에 대한 주문 내역 확인 및 결제하는 시간을 절감할 수 있고, 식음료 매장에 도착하지 않은 주문자는 식음료 거래 증명서를 발급받을 수 없다.

제안 시스템을 활용한 식음료 거래 증명서는 판매자가 발행하는 기존의 거래명세서, 영수증 등을 대체할 수 있다.



(그림 I.5-1) 식음료 거래 증명서 운용 구성도

제안 시스템을 이용하는 식음료 판매자와 주문자의 모바일 단말기는 블루투스 및 와이파이 다이렉트 연결이 원활하도록 근거리(예: 반경 40미터 이내 등)에 위치하여야 한다.

부 록 II-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

아래에 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

II-1.1 지식재산권 확약서(1)

- 발명의 명칭: 무선 통신을 이용한 개인간 비대면 신원 확인 시스템
- 권리자의 성명: 서울외국어대학원대학교 산학협력단
- 등록 번호: 10-2530058
- 등록 연월일: 2023년 5월 2일
- 실시조건: 합리적 조건하에 비차별적으로 실시
- 확약서 접수일: 2023년 12월 7일

부 록 II-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

해당 사항 없음

부 록 II-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당 사항 없음

부 록 II-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

아래 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따른다.

ITU-T X.srdidm, Security requirements for decentralized identity management systems using distributed ledger technology, March 2023.
W3C, Peer DID Method Specification, June 2023.
W3C, Verifiable Credentials Data Model v1.1, March 2022.
NIST, “A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems”, January 2020.
여기호, 박근덕, 염흥열, “단거리 무선 통신을 이용한 개인 간 분산 신원증명 시스템 제안”, 정보보호학회논문지, 31(5), pp.923~936, 2021년 10월.

부 록 II-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 II-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2023.12.06.	제정 TTAK.KO-12.0397	-	개인정보보호/ID관리, 블록체인 보안 프로젝트그룹 (PG502)