

감염병 예방을 위한 분산 ID 기반 디지털
증명서 시스템 보안 요구사항

Security Requirements for a Decentralized
Identity based Digital Certificate System to
Prevent Infectious Diseases

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
	엄흥열	순천향대학교	명예교수	PG502 특별위원
사무국 담당	오흥룡	TTA	수석	-

본 문서에 대한 저작권은 TTA에 있으며, TTA와 사전 협의 없이 이 문서의 전체 또는 일부를 상업적 목적으로 복제 또는 배포해서는 안 됩니다.

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 : 2024. 12. 06.

서 문

1 표준의 목적

이 표준의 목적은 감염병 예방을 위한 디지털 증명서 시스템을 제안하고, 해당 시스템의 잠재적인 보안 위협 및 보안 요구사항을 식별 및 기술함에 있다. COVID-19 팬데믹으로 인하여 많은 국가에서 COVID-19 디지털 증명서 시스템을 도입하여 활용하였지만, QR코드를 이용한 증명서 제출로 인한 증명서 복제 및 도용, 개인정보 유·노출 등의 문제가 있었고 이기종 시스템 간의 상호운용성 부족으로 인하여 증명서 사용의 어려움이 있었다. 또한 COVID-19 감염자가 위·변조된 증명서를 이용하여 방역을 회피함으로써 감염병을 전파하기도 하였다. 본 표준은 분산ID 기반의 증명서 검증 정보를 블록체인에 저장하여 발급자가 다른 다수의 증명서의 상호운용성을 제공할 수 있는 감염병 예방을 위한 디지털 증명서 시스템을 기술한다. 본 표준 시스템의 신뢰 앵커는 증명서 위·변조 문제를 해결하고 증명서 발행자와 제출자의 신원을 보증하여 보안성을 향상시킨다. 또한 본 표준에서의 시스템은 이용자 단말기의 근거리 무선통신을 이용하여 한 번에 다수의 증명서를 제출할 수 있고, 다수의 증명서(예: 백신접종증명서, 감염병회복증명서, 감염병검사증명서, 신분증 등)를 일괄적으로 검증할 수 있어 이용자의 편의성을 제고한다.

2 주요 내용 요약

이 표준은 이용자(Holder), 수탁자(Custodian), 발행자(Issuer), 서비스 제공자(Relying party), 오프체인(Off-chain), 유니버설 온체인(Universal On-chain) 등으로 구성되는 디지털 증명서 시스템을 기술한다. 또한 해당 시스템에 대한 보안 위협을 식별하고 해당 보안 위협을 완화시킬 수 있는 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 propose a digital certificate system for prevention of infectious diseases, and to identify and specify potential security threats and security requirements for the system. Due to the COVID-19 pandemic, many countries introduced and utilized the COVID-19 digital certificate system, but there were problems such as duplication and theft of certificates and leakage or exposure of personal information due to submission of certificates using QR codes. Additionally, there were difficulties in using certificates due to lack of interoperability between heterogeneous systems. People infected with COVID-19 used forged certificates to evade quarantine, thereby spreading the disease as well. The proposed system is a digital certificate system for prevention of infectious diseases that can provide interoperability of heterogeneous certificates by storing decentralized identity based certificate verification information on the blockchain. The trust anchor of the proposed system solves the problem of certificate forgery and improves security by guaranteeing the identity of the certificate issuer and presenter. In addition, the proposed system can allow to submit multiple certificates at once using the short-range wireless communication of the user terminal, and can allow to verify multiple certificates (e.g., vaccination certificate, infectious disease recovery certificate, infectious disease test certificate, ID card, etc.) at once, which improves user convenience.

2 Summary

The standard should specify a digital certificate system consisting of holder, custodian, issuer, service provider(relying party), off-chain, and universal 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

1	적용 범위	1
2	인용 표준	1
3	용어 정의	1
4	약어	3
5	감염병 예방을 위한 분산ID 기반 디지털 증명서 시스템	3
6	보안 위협 및 보안 요구사항	7
6.1	보안 위협	7
6.2	보안 요구사항	8
부록 I	활용 사례	11
부록 II-1	지식재산권 확약서 정보	14
II-2	시험인증 관련 사항	15
II-3	본 표준의 연계(family) 표준	16
II-4	참고 문헌	17
II-5	영문표준 해설서	18
II-6	표준의 이력	19

감염병 예방을 위한 분산ID 기반 디지털 증명서 시스템 보안 요구사항 (Security Requirements for a Decentralized Identity based Digital Certificate System to Prevent Infectious Diseases)

1 적용 범위

본 표준은 감염병 예방을 위하여 분산ID 기반 디지털 증명서 시스템을 정의한다. 또한 본 시스템에 대한 보안 위협 식별 및 그에 대응하는 보안 요구사항을 기술하고 부록에 활용 사례를 제공한다.

2 인용 표준

해당 사항 없음

3 용어 정의

3.1 개인정보(personal information)

“개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.

가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보”라 한다).

[출처] 개인정보 보호법

3.2 디지털 배지(digital badge)

다양한 학습 환경에서 얻을 수 있는 성취도, 기술, 품질 또는 관심의 검증된 지표

3.3 분산 ID(decentralized identity)

중앙 등록 메커니즘 없이 신뢰된 분산 프레임워크 하에서 활용되는 신원정보 체계.

3.4 블루투스(Bluetooth)

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

[출처(3.3~3.4)] TTA 정보통신용어사전

3.5 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(3.5)] ITU-T X.1252 (04/21)

3.6 신뢰 앵커(trust anchor)

신뢰 당사자가 신뢰하고 인증 경로에서 인증서를 검증하는데 이용되는 실체(Entity that is trusted by a relying party and used for validating certificates in certification paths).

[출처(3.6)] ISO/IEC 27099:2022, 용어정의를 따름

3.7 신원 지갑(identity wallet)

사용자가 자신의 개인키들을 저장함으로써 주로 식별자와 크리덴셜 정보들을 보관하는 애플리케이션 혹은 앱(응용 소프트웨어).

3.8 오라클 문제(oracle problem)

블록체인 환경에서 블록체인 밖의 데이터(off-chain data)를 블록체인 안 데이터(on-chain data)에 포함하여 기록할 때 발생하는 문제를 말한다.

3.9 오프체인(off-chain)

블록체인 환경 외부에서 이루어진 프로세스 혹은 블록체인 외부에 저장된 데이터 등을 지칭할 때 사용.

3.10 온체인(on-chain)

블록체인 환경 내부에서 이루어진 프로세스 혹은 생성된 데이터 등을 지칭할 때 사용.

3.11 와이파이 다이렉트(Wi-Fi Direct)

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

3.12 전자서명(electronic signature)

서명자의 신원과 서명 사실을 확인하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자 형태의 정보. 전자서명은 네트워크를 통해 전달되는 디지털 메시지 또는 문서에 대한 진위성(authenticity), 무결성(integrity), 부인 방지(non-repudiation) 특성을 제공.

3.13 쿼알코드(QR code)

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

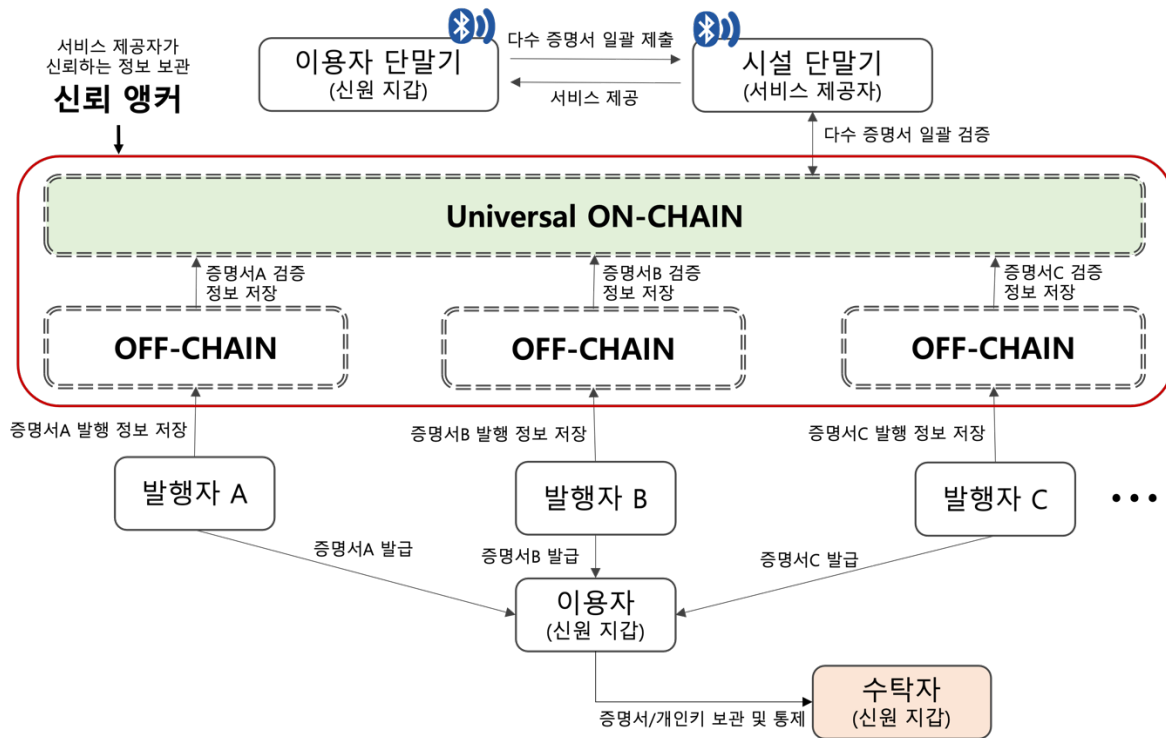
[출처(3.7~3.13)] TTA 정보통신용어사전

4 약어

API	Application Programming Interface
ID	Identity
QR	Quick Response
URL	Uniform Resource Locator

5 감염병 예방을 위한 분산ID 기반 디지털 증명서 시스템

감염병 예방을 위한 분산ID 기반 디지털 증명서 시스템은 발행자(Issuer), 이용자(Holder), 수탁자(Custodian), 서비스 제공자(Relying party), 오프체인(Off-chain), 유니버설 온체인(Universal on-chain) 등으로 구성된다. 그리고 이용자 및 수탁자는 신원 지갑을 보유하고, 오프체인 및 유니버설 온체인은 신뢰 앵커(Trust anchor)가 될 수 있다. 본 시스템을 활용하는 이용자 및 서비스 제공자의 모바일 단말기는 블루투스 및 와이파이 다이렉트 연결이 원활하도록 근거리로 위치한다.



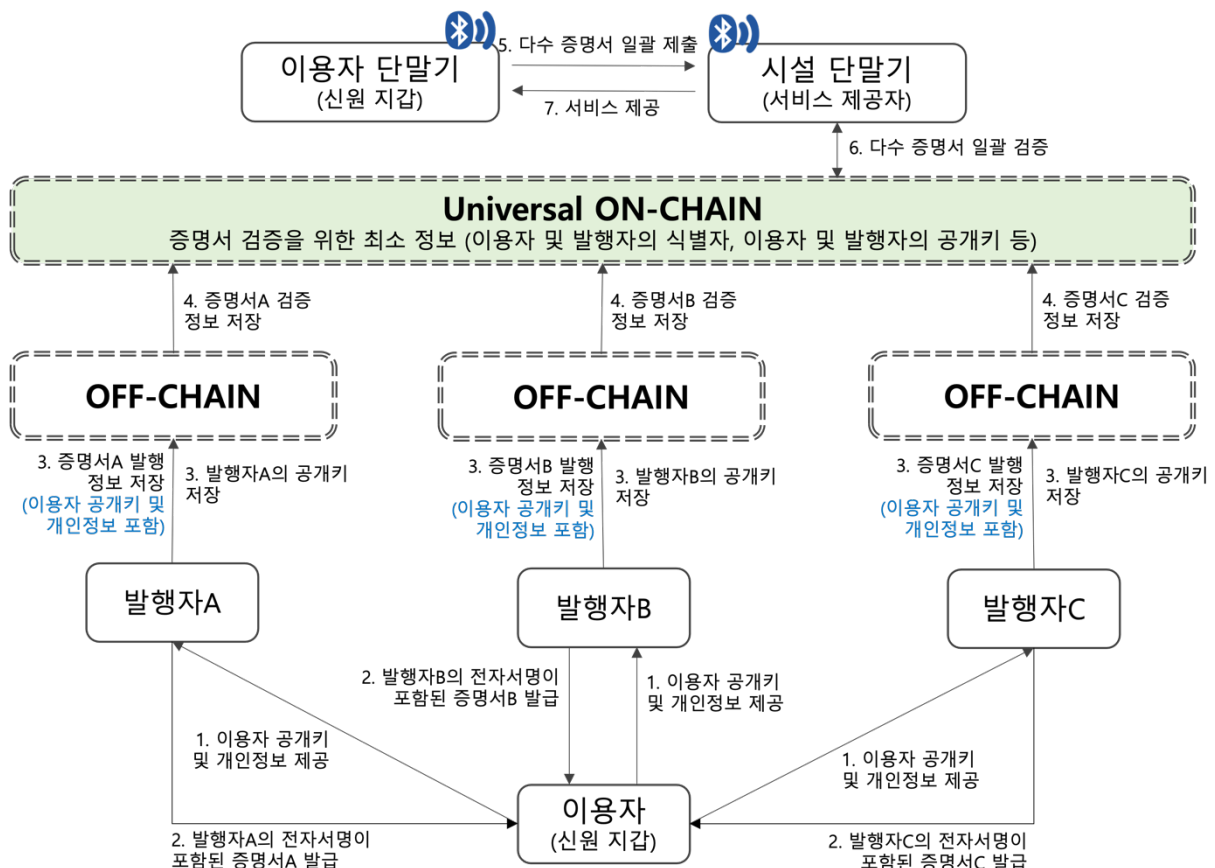
(그림 5-1) 감염병 예방을 위한 분산ID 기반 디지털 증명서 시스템 구성도

(그림 5-1)에서 본 표준의 시스템을 구성하는 주요 요소(Components)의 역할은 다음과 같다.

- 발행자: 이용자의 요청에 따라 발행자의 전자서명이 포함된 증명서를 해당 이용자에게 발급하고, 해당 증명서의 발행 정보(예: 발행자의 개인키 및 공개키, 이용자의 개인정보 및 공개키 등)를 오프체인에 저장한다.
- 이용자: 발행자에게 자신의 개인정보 및 공개키를 제공하여 증명서 발급을 요청하고, 발행자로부터 발급받은 증명서를 신원 지갑에 저장 및 관리한다. 신원 지갑(유형 예시: 공용 신원 지갑, 기기종 신원 지갑, 페더레이션 신원 지갑 등)은 통상적으로 이용자의 단말기(예: 스마트폰 등)에 설치 및 운용되고 고유한 개인키/공개키 쌍을 보유한다. 이용자의 단말기 또는 신원 지갑의 취약점으로 인한 개인키 및 증명서의 탈취 등을 방지하기 위하여 수탁자에게 이용자의 개인키 및 증명서 등을 위탁하여 관리할 수 있다. 서비스 제공자에게 자신의 전자서명이 포함된 증명서를 근거리 무선 통신(블루투스 및 와이파이 다이렉트)을 통하여 제출하고 해당 증명서의 진위성 및 유효성 검증 결과에 따라 서비스를 제공받는다. 또한 해당 근거리 무선 통신을 통하여 다수의 증명서가 일괄적으로 서비스 제공자에게 제출될 수 있다.
- 수탁자: 이용자의 요청에 따라 이용자의 개인키 및 증명서 등을 안전하게 수탁 및 관리한다.
- 서비스 제공자: 이용자가 제출한 증명서의 진위성 및 유효성을 검증하고 그 결과

에 따라 해당 이용자에게 서비스를 제공한다. 해당 증명서를 검증하기 위한 정보(예: 발행자의 식별자 및 공개키, 이용자의 식별자 및 공개키 등)는 유니버설 온체인으로부터 제공받는다. 검증이 완료된 이용자의 증명서 또는 증명서에 포함된 개인정보는 파기한다.

- 오프체인: 이용자에게 발급한 증명서에 대한 발행 정보(예: 발행자의 개인키 및 공개키, 이용자의 개인정보 및 공개키 등)를 저장 및 관리한다. 발행자가 이용자에게 발급한 증명서의 진위성 및 유효성을 검증하기 위한 정보(예: 이용자의 식별자 및 공개키, 발행자의 식별자 및 공개키 등)를 유니버설 온체인에게 제공한다.
- 유니버설 온체인: 이용자가 서비스 제공자에게 제출한 증명서의 진위성 및 유효성을 검증하기 위한 최소한의 정보(예: 발행자의 식별자 및 공개키, 이용자의 식별자 및 공개키 등)를 저장 및 관리하고, 이용자의 개인정보는 저장하지 않는다.
- 신뢰 앵커: 서비스 제공자가 신뢰할 수 있는 정보(예: 이용자가 제출한 증명서의 진위성 및 유효성을 검증할 수 있는 데이터 등)를 제공하는 오프체인 및 유니버설 온체인으로 구성된다. 오라클 문제를 해결하기 위하여 오프체인에서 유니버설 온체인으로 전송되는 데이터의 기밀성 및 무결성을 보장하여야 한다.



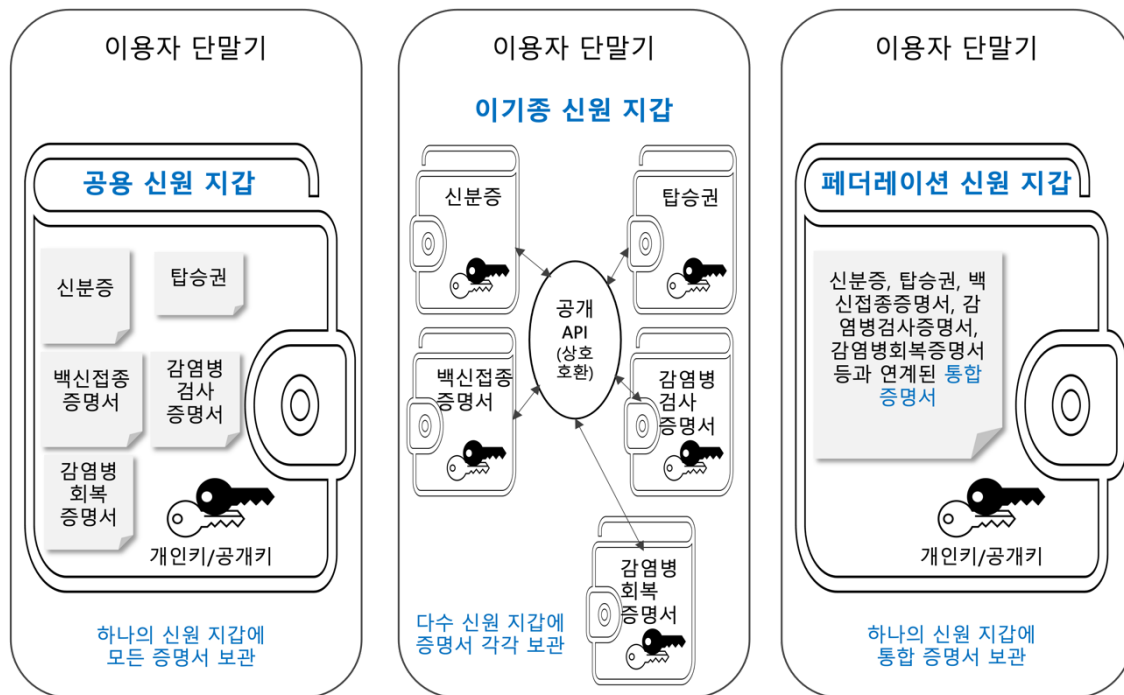
(그림 5-2) 본 표준의 시스템을 활용한 서비스 시나리오 구성도

(그림 5-2)에서 본 표준의 시스템을 활용한 서비스 시나리오를 다음과 같이 설명한다.

- 1단계: 이용자는 각각의 발행자A, 발행자B 및 발행자C에게 자신의 공개키 및 개인정보를 제공하고 증명서A, 증명서B 및 증명서C 발급을 요청한다.
- 2단계: 발행자A, 발행자B 및 발행자C는 이용자의 신원을 확인하고 자신의 전자서명이 포함된 증명서A, 증명서B 및 증명서C를 이용자에게 발급한다. 이용자는 각각의 발행자로부터 발급받은 증명서A, 증명서B 및 증명서C를 신원 지갑에 저장 및 관리한다.
- 3단계: 발행자A, 발행자B 및 발행자C는 자신의 공개키 및 증명서A, 증명서B, 증명서C의 발행 정보(이용자의 공개키 및 개인정보 포함)를 해당 발행자가 보유한 오프체인에 저장 및 관리한다.
- 4단계: 오프체인은 증명서A, 증명서B 및 증명서C를 검증할 수 있는 정보(예: 이용자 및 발행자A, 발행자B, 발행자C의 식별자, 이용자 및 발행자A, 발행자B, 발행자C의 공개키 등)를 유니버설 온체인에 저장한다.
- 5단계: 이용자는 모바일 단말기 내 신원 지갑에 저장되어 있는 증명서A, 증명서B, 증명서C 등 다수의 증명서를 근거리 무선 통신(블루투스 및 와이파이 다이렉트)을 이용하여 서비스 제공자의 시설 단말기(예: 공항 등)에 일괄 전송한다.
- 6단계: 서비스 제공자는 유니버설 온체인을 통하여 증명서A, 증명서B 및 증명서C의 진위성 및 유효성을 일괄 검증한다.
- 7단계: 서비스 제공자는 증명서A, 증명서B 및 증명서C의 진위성 및 유효성 검증 결과에 따라 이용자에게 서비스를 제공한다.

이용자 단말기에 설치 및 운용되는 신원 지갑의 유형은 (그림 5-3)에서 보는 바와 같이 공용 신원 지갑, 이기종 신원 지갑, 페더레이션 신원 지갑 등으로 분류될 수 있다. 공용 신원 지갑은 하나의 신원 지갑에 모든 증명서를 저장 및 관리하는 것으로써 해당 증명서에 대한 전자서명을 위하여 유일한 개인키/공개키 쌍을 보유한다. 이기종 신원 지갑은 다수의 증명서를 각기 다른 신원 지갑에 저장 및 관리하는 것으로써 신원 지갑 간의 상호운용성은 공개 API를 통하여 구현될 수 있고, 각각의 증명서에 대한 전자서명을 위하여 각기 다른 개인키/공개키 쌍을 보유한다.

페더레이션(Federation) 신원 지갑은 하나의 신원 지갑에 다수의 증명서를 연계한 통합 증명서를 저장 및 관리하는 것으로써 해당 증명서에 대한 전자서명을 위하여 유일한 개인키/공개키 쌍을 보유한다. 통합 증명서는 각각의 증명서에서 공통으로 활용되는 이용자의 개인정보와 각각의 자격정보, 각각의 증명서 발행 이력(예: 백신접종증명서의 경우에 문진표 등 의사 상담 내역) 등으로 구성될 수 있다. 통합 증명서를 활용하여 디지털 배지(Digital badge)를 구현할 수 있다.



(그림 5-3) 신원 지갑의 유형

6 보안 위협 및 보안 요구사항

6.1 보안 위협

분산ID 기반 디지털 증명서 시스템에서 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 위·변조: 발행자로부터 진본 증명서를 발급받지 않고 허위 또는 거짓 정보를 입력하여 위조 증명서를 생성하거나, 진본 증명서의 일부 또는 전체 내용을 허위 또는 거짓 정보로 무단 변경하여 증명서를 변조할 수 있다. 허위 또는 위조된 개인정보 및 자격정보(예: 백신접종 유무, 감염병검사 유무, 감염병회복 유무 등)를 포함한 증명서는 타인의 신원을 도용할 수 있다.
- (ST-2) 개인정보 유출: 이용자의 모바일 단말기 도난 및 분실, 모바일 단말기 해킹 등을 통하여 해당 모바일 단말기 내 신원 지갑에 저장하고 있는 증명서에 포함된 개인정보가 유출될 수 있다. 또한 이용자와 서비스 제공자의 모바일 단말기 간 근거리 무선 통신(블루투스 및 와이파이 다이렉트)을 통하여 증명서를 제출 시 증명서에 포함된 개인정보가 유출될 수 있고, 다수의 증명서를 일괄 제출 시 서비스 제공자가 요구하지 않은 증명서를 제출하는 경우에 과도하게 개인정보가 유출될 수 있다. 서비스 제공자의 모바일 단말기에 저장된 대량의 증명서

에 포함된 개인정보가 유출될 수 있다. 이용자의 모바일 단말기 내 이기종 신원 지갑 간의 상호운용을 위하여 공개API를 이용하는 경우에 타 신원 지갑 내 저장된 증명서에 포함된 개인정보가 유출될 수 있다.

- (ST-3) 암호키·개인키 분실: 이용자의 모바일 단말기 도난 및 분실, 모바일 단말기 장애 등을 통하여 모바일 단말기에 보관하고 있는 암호키(개인정보 암호·복호화 용도) 및 개인키(증명서 전자서명 용도)가 분실될 수 있다.
- (ST-4) 근거리 무선 통신 장애: 이용자 및 서비스 제공자의 모바일 단말기에 설치되어 있는 근거리 무선 통신 모듈(블루투스 및 와이파이 다이렉트)의 취약점으로 인하여 모바일 단말기 간의 신원 증명서 송수신 장애가 발생할 수 있다.
- (ST-5) 서비스 제공자로 가장: 이용자의 모바일 단말기에 설치되어 있는 근거리 무선 통신 모듈(블루투스 및 와이파이 다이렉트)의 송수신 반경 내에 위치한 악의적인 수신자가 서비스 제공자로 가장하여 이용자의 증명서를 무단으로 수집할 수 있다.
- (ST-6) 증명서 검증 정보 위·변조: 이용자 증명서의 진위성 및 유효성을 검증하기 위한 정보(예: 이용자 및 발행자의 식별자, 이용자 및 발행자의 공개키 등)를 오프체인에서 유니버설 온체인으로 전송 시 데이터 위·변조가 발생할 수 있다. 허위 또는 위조된 해당 검증 정보를 악용하여 해당 증명서의 발행자 및 이용자의 신원을 무단으로 변경함으로써 허위 또는 위조 증명서를 악용할 수 있다.

6.2 보안 요구사항

분산ID 기반 디지털 증명서 시스템에서 발생할 수 있는 보안 위협을 완화시킬 수 있는 보안 요구사항(SR, security requirement)은 다음과 같다.

- (SR-1) 발행자 신원 확인: 서비스 제공자는 이용자가 제출한 증명서의 진위성 및 유효성을 검증할 때 해당 증명서에 포함된 발행자의 전자서명을 검증하여 발행자의 신원 및 적격성을 확인한다.
- (SR-2) 데이터 암호화: 이용자의 모바일 단말기에 증명서를 저장 시 증명서에 포함된 개인정보를 안전한 암호 알고리즘으로 암호화한다. 또한 이용자 및 서비스 제공자의 모바일 단말기 간에 근거리 무선 통신(블루투스 및 와이파이 다이렉트)을 이용하여 증명서를 송수신하는 경우에 증명서에 포함된 개인정보를 안전한 암호 알고리즘으로 암호화한다. 개인정보 저장 및 전송 시 이용하는 암호키는 안전하게 관리한다. 이용자 증명서의 진위성 및 유효성을 검증하기 위한 정보(예: 이용자 및 발행자의 식별자, 이용자 및 발행자의 공개키 등)를 오프체인에서 유니버설 온체인으로 전송 시 데이터를 안전한 암호 알고리즘으로 암호화한다.
- (SR-3) 개인정보 파기: 서비스 제공자의 모바일 단말기에 수집된 이용자의 증명서는 진위성 및 유효성 검증이 완료된 후에 해당 증명서를 완전히 파기하거나

해당 증명서에 포함된 개인정보를 완전히 파기한다.

- (SR-4) 접근 통제: 이용자의 모바일 단말기에 설치되어 있는 타 애플리케이션에서 증명서에 포함된 개인정보에 무단으로 접근하지 못하도록 통제한다. 모바일 단말기 제조사에서 제공하는 애플리케이션 간 접근 통제 기능을 활용할 수 있다. 이용자의 모바일 단말기 내 이기종 신원 지갑 간의 상호운용을 위하여 공개API를 이용하는 경우에 타 신원 지갑 내 저장된 증명서에 무단으로 접근하지 못하도록 통제한다.
- (SR-5) 데이터 백업: 모바일 단말기 제조사에서 제공하는 백업 및 복구 기능을 이용하여 중요한 데이터(예: 증명서, 암호키, 개인키 등)를 안전하게 백업 및 복구한다.
- (SR-6) 패치 관리: 이용자 및 서비스 제공자의 모바일 단말기 제조사 또는 근거리 무선 통신 모듈(블루투스 및 와이파이 다이렉트) 제조사에서 주기적으로 제공하는 보안 패치, 업데이트 등을 설치한다.
- (SR-7) 모바일 단말기 간 상호 인증: 이용자 및 서비스 제공자의 모바일 단말기에 설치되어 있는 근거리 무선 통신 모듈(블루투스 및 와이파이 다이렉트)의 송수신 반경을 최소화하고, 해당 모바일 단말기 간의 상호 인증을 통하여 제3자에 의한 증명서 무단 수신을 제한한다.

<표 6-1> 보안 위협과 보안 요구사항 간의 대응 관계

구분	SR-1 발행자 신원 확인	SR-2 데이터 암호화	SR-3 개인정보 파기	SR-4 접근 통제	SR-5 데이터 백업	SR-6 패치 관리	SR-7 모바일 단말기 간 상호 인증
ST-1 신원정보 위·변조	○						
ST-2 개인정보 유출		○	○	○			
ST-3 암호키·개인키 분실					○		
ST-4 근거리 무선 통신 장애						○	
ST-5 서비스 제공자로 가장							○
ST-6 증명서 검증 정보 위·변조		○					

(※ ST=보안 위협, SR=보안 요구사항)

SR-1(발행자 신원 확인)은 ST-1(신원정보 위·변조)를 완화시킬 수 있다. SR-2(데이터 암호화)는 ST-6(증명서 검증 정보 위·변조)를 완화시킬 수 있다. SR-2(데이터 암호화),

SR-3(개인정보 파기) 및 SR-4(접근 통제)는 ST-2(개인정보 유출)을 완화시킬 수 있다. SR-5(데이터 백업)은 ST-3(암호키·개인키 분실)을 완화시킬 수 있고, SR-6(패치 관리)는 ST-4(근거리 무선 통신 장애)를 완화시킬 수 있다. SR-7(모바일 단말기 간 상호 인증)는 ST-5(서비스 제공자로 가장)을 완화시킬 수 있다.

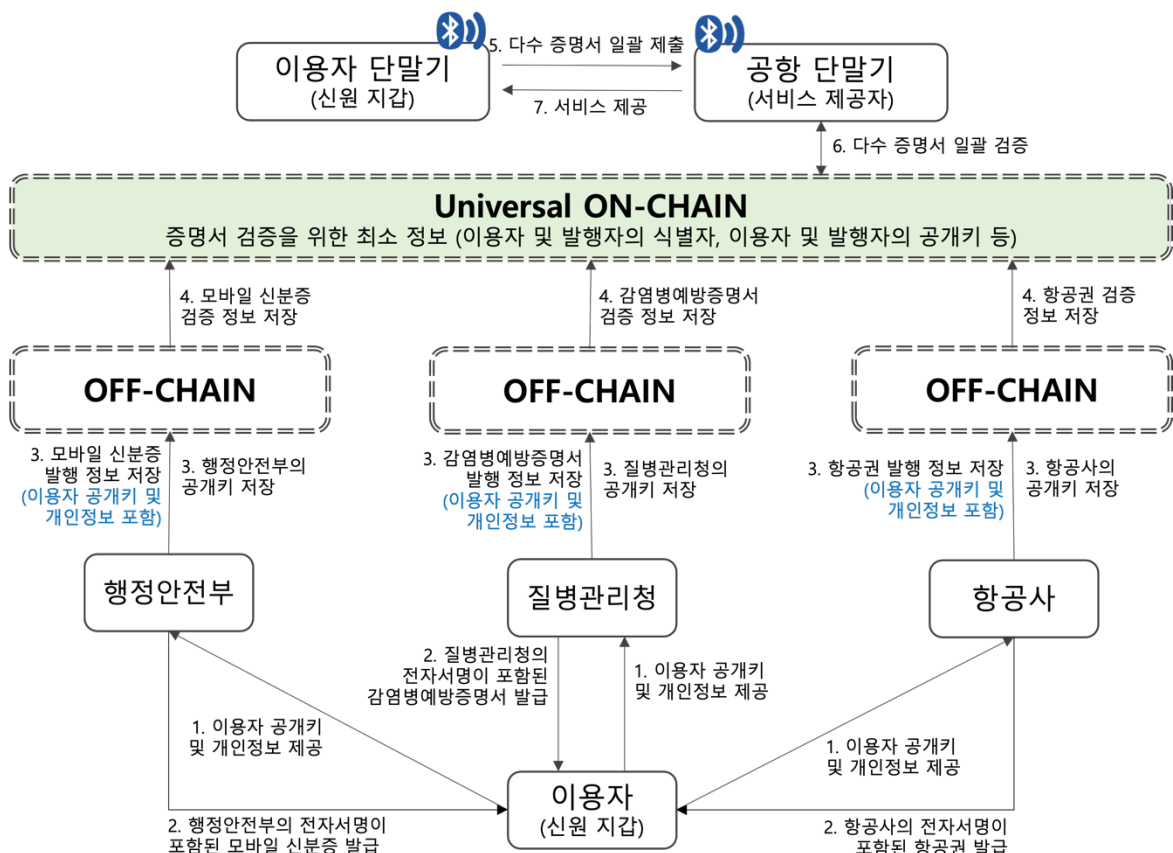
부 록 I

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

활용 사례

I.1 백신 여권

본 표준의 시스템을 활용하는 백신 여권의 경우에 (그림 I.1-1)에서 보는 바와 같이 이용자는 행정안전부, 질병관리청 및 항공사를 통하여 모바일 신분증(예: 모바일 운전면허증, 모바일 주민등록증, 모바일 여권 등), 감염병 예방 증명서(예: 백신접종증명서, 감염병검사증명서, 감염병회복증명서 등) 및 항공권을 발급받아 이용자의 모바일 단말기 내 신원지갑에 저장 및 관리한다. 이용자는 공항에 설치하여 운용하는 모바일 단말기를 통하여 모바일 신분증, 감염병 예방 증명서, 항공권을 2개 이상 복수로 선택하여 일괄적으로 제출하고 해당 증명서의 진위성 및 유효성 검증 결과에 따라 보안 구역을 통과하고 항공기에 탑승할 수 있다.

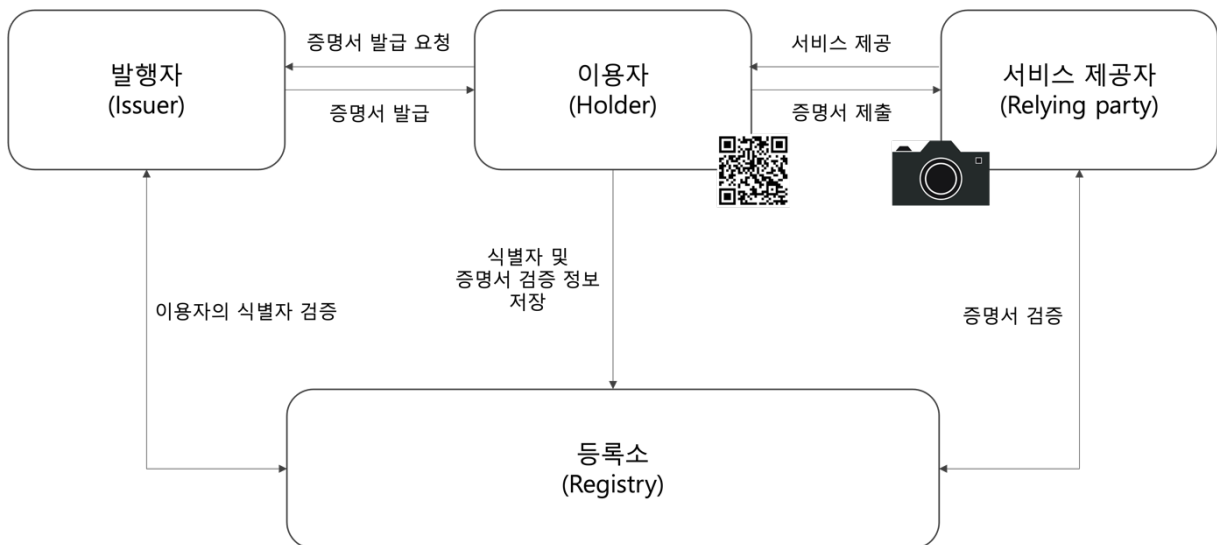


(그림 I.1-1) 백신 여권 운용 구성도

본 표준의 시스템을 활용하는 이용자 및 서비스 제공자의 모바일 단말기는 모바일 신분증, 감염병예방증명서, 항공권 등 다수의 증명서 송수신을 위하여 블루투스 및 와이파이 다이렉트 연결이 원활하도록 근거리에서 위치한다.

1.2 큐알코드를 이용한 증명서 시스템

기존의 큐알코드(QR code)를 이용한 증명서 시스템은 발급자(Issuer), 이용자(Holder), 서비스 제공자(Relying party), 등록소(Registry) 등으로 구성된다. 발행자는 이용자의 요청에 의해 증명서를 발급한다. 이때 이용자는 발행자에게 개인정보를 제공한다. 이용자는 발행자로부터 발급받은 증명서를 자신의 단말기에 저장 및 관리하고, 서비스 제공자에게 제출한 증명서의 진위성 및 유효성을 검증할 수 있는 정보를 등록소에 저장한다. 서비스 제공자는 등록소에 저장된 정보를 이용하여 이용자로부터 제출받은 증명서의 진위성 및 유효성을 검증하고, 해당 검증에 성공할 경우에 이용자에게 서비스를 제공한다. 등록소는 이용자의 식별자, 이용자 증명서의 진위성 및 유효성을 검증할 수 있는 정보 등을 저장 및 관리한다.



(그림 1.2-1) 큐알코드를 이용한 증명서 시스템 구성도

(그림 1.2-1)에서 기존의 큐알코드를 이용한 증명서 시스템은 이용자 보호 및 편의성 측면에서 다음과 같은 몇 가지 한계점이 존재한다.

- 증명서 도용: 이용자가 큐알코드를 이용하여 증명서를 서비스 제공자에게 제출하는 경우에 증명서 복제(예: 단말기 스크린 샷 등)가 용이하고 이용자는 자신의 신원을 타인에게 제공하거나 자신의 신원을 도용 당할 수 있다. 증명서 복제를 어렵게 하기 위하여 동적 큐알코드(예: 큐알코드 유효시간 15초 등)를 이용할

수 있으나 쿼알코드 유효 시간을 너무 짧게 설정하는 경우에 서비스 제공자가 해당 쿼알코드를 인식하는데 실패할 가능성이 높아져 증명서 제출이 지연될 수 있다.

- 다중 증명서(Multi-credential) 처리 불편: 이용자가 쿼알코드를 이용하여 다중 증명서를 서비스 제공자에게 제출하는 경우에 다수의 증명서별 쿼알코드를 각각 생성하여 제출하고 검증 받아야 하는 불편함이 있다.
- 개인정보 유출: 이용자가 쿼알코드를 이용하여 증명서를 서비스 제공자에게 제출하는 경우에 통상적인 쿼알코드 스캐너(Scanner)을 통하여 이용자의 개인정보를 손쉽게 수집할 수 있다. 쿼알코드를 이용하여 이용자의 증명서를 서비스 제공자에게 직접 제출하는 방식이 아닌 것으로써, 쿼알코드를 이용하여 증명서가 저장된 위치(예: URL 등) 정보를 서비스 제공자에게 제출하는 경우에 해당 증명서를 저장 및 관리하고 있는 정보시스템(예: 메시지 서버 등)을 통하여 대량의 개인정보가 유출될 수 있다.
- 증명서 상호운용성 부족: 이기종의 증명서 시스템 간에 이용자 증명서의 진위성 및 유효성을 검증하는데 어려움이 있다.

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: 블록체인 기반의 증명서를 위한 시스템
- 권리자의 성명: 서울외국어대학원대학교 산학협력단, 순천향대학교 산학협력단
- 등록 번호: 제10-2579669호
- 등록 연월일: 2023년 9월 13일
- 실시조건: 지적재산권을 합리적 조건하에 비차별적으로 실시하도록 하여
- 확약서 접수일: 2024년 7월 25일

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.

- [1] ITU-T X.srdidm, Security requirements for decentralized identity management systems using distributed ledger technology, March 2024.
- [2] W3C, Verifiable Credentials Data Model v2.0, March 2024.
- [3] NIST, “A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems”, January 2020.
- [4] ISO/IEC 27099:2022, Information technology — Public key infrastructure — Practices and policy framework, July 2022.
- [5] Wikipedia, “Digital badge”, https://en.wikipedia.org/wiki/Digital_badge#cite_note-1, July 2024.
- [6] 한국인터넷진흥원(KISA), “암호 키 관리 안내서(KISA-GD-2014-0013)”, 2014년 12월.
- [7] 한국인터넷진흥원(KISA), “암호 알고리즘 및 키 길이 이용 안내서(KISA-GD-2018-0034)”, 2018년.
- [8] 박성채, 이주현, 박근덕, 염흥열, “감염병 예방을 위한 디지털 증명서 시스템”, 정보보호학회논문지, 32(1), pp.49~65, 2022년 2월.

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	2024.12.06.	제정 TTAK.KO-12.0412	-	개인정보보호/ID관리, 블록체인 보안 프로젝트그룹 (PG502)