Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.1, Feb. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.1.49

감염병 예방을 위한 분산ID 기반 디지털 증명서 시스템*

박 성 채,[1†] 이 주 현,[2] 박 근 덕,[3] 염 흥 열[4‡]
[1,2,4]순천향대학교 (대학원생, 학생, 교수), [3]서울외국어대학원대학교 (교수)

Decentralized Identity Based Digital Certificate System for Prevention of Infectious Diseases*

Sung-chae Park,[1†] Ju hyun Lee,[2] Keundug Park,[3] Heung Youl Youm[4‡]
[1,2,4]Soonchunhyang University (Graduate student, Undergraduate student, Professor),
[3]Seoul University of Foreign Studies (Professor)

요 약

최근 COVID-19 팬데믹으로 인하여 많은 국가에서 감염병 예방 디지털 증명서를 위한 시스템을 도입하여 활용하고 있지만, 이에 대한 국제표준이 없어 국가 간 호환성 있는 증명서 사용의 어려움이 있다. 이에 본 논문에서는 기존 QR 코드 방식의 증명서 제출과 무선 근거리 통신 방식의 증명서 제출 방식을 비교하고 보다 개선된 무선 근거리 통신 방식의 디지털 증명서 시스템을 제안한다. 제안 시스템은 분산ID 기반의 증명서 검증 정보를 블록체인에 저장하여 국가별로 상이한 증명서의 상호 운용 체계를 구축하는 감염병 예방 디지털 증명서 시스템이다. 블록체인 기반의 신뢰앵커는 증명서 위·변조 문제를 해결하고 증명서 발행자와 제출자의 신원을 보증하여 보안성을 향상 시킬 것이다. 아울러 제안 시스템은 한 번의 증명서 제출로 다수 증명서(백신 접종증명서, 회복증명서, 검사 증명서, 신분증 등)를 일괄 검증토록 하여 이용자 편의성을 제고할 수 있을 것으로 기대한다.

ABSTRACT

The COVID-19 pandemic has led many countries around the world to introduce and employ a digital certificate system to prevent infectious diseases, however, there are difficulties in using the compatible digital certificate between countries in that the international standards of the system have not been developed. Accordingly, we propose an improved system, comparing two methods of presenting a certificate, existing QR code-based and a short-range wireless communication-based certificates. The proposed system is a digital certificate system against the spread of infectious disease by storing verification information of the certificate using decentralized identity-based technology on the blockchain. Blockchain-based trust anchor improves security by solving the problem of forgery and alteration of certificates and guaranteeing the identity of certificate issuers and presenters. This system is also expected to enhance usability providing concurrent verification of a number of certificates(vaccination certificates, recovery certificates, test results, identity certificates, etc.) in a single certificate presentation.

Keywords: Decentralized Identity, Blockchain, Wireless communication, Digital Certificate, Vaccination passport

Received(11. 24. 2021), Modified(01. 17. 2022), Accepted(01. 17. 2022)
* 이 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(과제번호: 2021-0-00112, 차세대 보안 표준전문연구실)
† 주저자, zoesc.park@sch.ac.kr
‡ 교신저자, hyyoum@sch.ac.kr (Corresponding author)

I. 서 론

1.1 연구 배경 및 목적

최근 경제성장에 따라 국가 간 교역과 인간의 이동성 증가, 질병 벡터의 지리적 분포 변화 등으로 인해 국지적으로 발생된 감염병은 빠른 시간 내에 전세계로 확산되어 글로벌 보건 안보와 경제에 위협을 가하고 있다[1]. 또한 이 감염병은 의학 및 과학 기술의 눈부신 발전과 위생 환경의 개선, 질병 관리를 위한 법 체제 강화 등에도 불구하고 기존의 의료 방안으로 다스릴 수 없는 변이를 거듭하며 국제 사회와 전 인류를 위태롭게 한다. 중증급성호흡기증후군(Severe Acute Respiratory Syndrome, SARS), 중동호흡기증후군(Middle East Respiratory Syndrome, MERS) 이후 나타난 코로나바이러스 감염증-19(Corona Virus Disease-2019, COVID-19)은 2019년 12월 말 중국의 우한 지역에서 발생된 것으로 보고되었으며, 전 세계적으로 매우 빠르게 확산되었다[2]. 이에 따라 세계의 각 국가들은 의료적 대응과 사회적 통제 및 백신접종증명서, 중합효소 연쇄반응(Polymerase Chain Reaction, PCR) 검사 결과지를 발급하여 활용하는 등 COVID-19 확산 방지를 위해 다양한 조치를 취하고 있다. 특히 감염병 예방을 위한 증명서에 있어 현재 많은 국가들은 COIVD-19으로 인한 이동의 자유 제한을 최소화하고 경제 활동을 재개하기 위해 Table 1.과 같이 COIVD-19 백신접종 증명서, PCR 검사 결과지, COIVD-19 회복증명서와 같은 다양한 증명서를 도입 및 활용하고 있다[3]. 이와 관련하여 세계보건기구(World Health Organization, WHO)는 COVID-19 증명서 디지털문서 (Digital Documentation of COVID-19 Certificates: Vaccination Status, DDCC:VS)를 개발하였으며 국가 간 표준화를 추진 중이다. DDCC:VS는 COVID-19 백신 접종 상태를 확인할 수 있는 전자서명된 문서로, 의료정보 기술표준을 목적으로 하는 사실적 표준화 기구(Health Level Seven, HL7)에서 개발한 차세대 의료정보 표준 프레임워크(Fast Healthcare Interoperability Resources, FHIR) 문서이다. 이 문서는 DDCC:VS의 핵심 정보가 포함된 데이터 요소를 포함한다[4].

백신접종증명서를 비롯한 감염병 예방 증명서 시스템을 구축하고 국가 간 경계를 넘어 활용하기 위해서는 우선 고려해야 할 요구사항들이 있다. 먼저 증명서의 발급, 보관 및 휴대성, 이용자의 증명서 이용과 파기를 고려한 편의성이 제고되어야 하며, 디지털 약자를 배려하기 위하여 기존의 종이 증명서도 사용 가능해야 한다. 또한 최근 COVID-19과 관련된 각종 증명서 제출이 국내외적으로 증가함에 따라 위·변조된 백신접종증명서나 COVID-19 음성 확인서 등이 다크 웹, 소셜 미디어 사이트와 같은 온라인과 오프라인을 통해 유통 되면서 감염병 예방증명서 발행의 목적과 의미가 훼손되고 있다[5]. 이에 대한 대책으로 증명서 자체의 위변조 방지와 증명서 진위성 검증을 위한 증명서 발행자(issuer) 및 이용자(holder)의 신원 확인은 필수적으로 요구되는 중요 사항이다.

이 논문에서 제안하는 감염병 예방 디지털 증명서 시스템은 분산ID(Decentralized Identity, DID) 기술을 기반으로 하는 신원관리 시스템과 증명서 발급 시스템을 연계하고, 모바일 앱을 통해 다양한 증명서를 관리 및 이용 가능하게 함으로써 이용자 편의성을 강화할 수 있다. 현재 여러 기관과 국가에서 발급하는 대부분의 감염병 예방 증명서는 쓰이는 용어부터 적용되는 규격 등이 상이하여 글로벌화가 어렵기 때문에 이에 대응하기 위한 표준화된 기술과 지침이 필요하다.

본 논문에서는 분산원장기술(Distributed Ledger Technology, DLT) 기반의 분산ID 기술을 활용한 감염병 예방 증명서 시스템을 서술한다. 2장에서는 관련 기술 및 기존 모델을 비교하고 이에 대한 국제 표준화 현황을 살펴본다. 3장에서는 분산원장기술 기반의 분산ID 기술을 이용한 감염병 예방 증명서 시스템을 설명하고 4장에서는 본 논문이 제안하는 시스템의 보안 위협 및 요구사항에 대하여 설명하고자 한다.

II. 관련 기술 및 기존 모델

2장에서는 감염병 예방 디지털 증명서의 관련 기술에 대하여 웹 기반 기술표준화 기구인 W3C(World Wide Web Consortium)의 분산ID 모델과 WHO에서 발표한 공개키 구조(Public Key Infrastructure, PKI) 기반의 COVID-19 증명서 디지털문서(Digital Document of COVID-19 Certificates:Vaccination Status, DDCC:VS) 및 유럽연합의 디지털 코로나 증명서

Table 1. Examples of digital certificate by the countries[3]

Country	Vaccination Passport Name	Details		
		Vaccination	PCR-Test Result	Proof of Recovery
USA	NewYork State Excelsior Pass	○	○	-
EU	Digital COVID Certificate	○	○	○
Israel	Green Pass	○	○	○
Switzerland	Common Pass	○	○	○
China	Certificate of health examination for international traveller	○	○	○
Japan	Vaccination Passport	○	-	-
South Korea	COVID-19 Vaccination Certificate	○	-	-

(EU Digital COVID Certificate, DCC), 한국의 코로나19 전자예방접종증명인 쿠브 (COvid OVercome, COOV)에 대해 설명한다.

2.1 분산원장기술 기반의 분산ID

분산ID는 중앙 등록 메커니즘 없이 신뢰 분산 프레임워크 하에서 활용되는 신원정보 체계로 디지털 환경에서 분산원장을 기반으로 정보주체가 스스로 신원에 대한 증명 관리와 신원정보 제출 범위 및 제출 대상을 통제하여 개인정보에 대한 자기주권을 보장할 수 있는 탈중앙화된 디지털 신원증명 체계를 의미한다[6][7]. 분산ID는 W3C나 DIF(Decentralized Identity Foundation) 등에서 표준화 하고 IBM, Microsoft 같은 기업에서 상용화 서비스를 추진하면서 매우 빠르게 발전하고 있다[8]. W3C의 제안 권고안(Proposed Recommendation)은 분산ID를 탈중앙화 된 새로운 유형의 고유 식별자(identifier)로 정의하고 이를 이용한 개인정보 제공에 대한 개인정보 주체의 통제권과 여러 기관 또는 시스템과의 상호 운용성을 제시한다[9].

Fig.1.은 W3C의 검증 가능한 데이터 모델(verifiable credential data model)로 분산ID 이용자는 검증자 또는 서비스 제공자(verifier)가 제공하는 서비스를 이용하기 위해 발행자에게 자신의 신원 정보(verifiable credentials, VC) 발행을 요청하고 발행자로부터 필요한 신원정보를 제공 받아 서비스 제공자인 검증자에게 제공한다. 이때 발행자는 소유자의 신원정보 발행과 관련된 사항들을 검증 가능한 데이터 저장소(verifiable data registry)

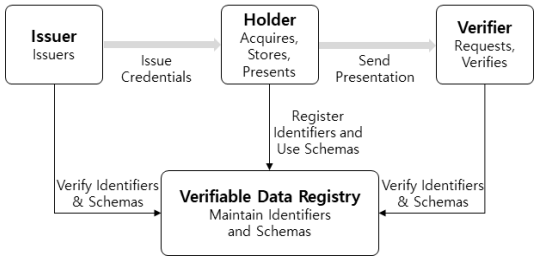

Fig. 1. Basic DID model of W3C[10]

에 저장한다.

W3C의 분산ID 관련 표준은 전 세계 60개 이상의 기관이 참여하는 COVID-19 인증 이니셔티브(COVID-19 Credential Initiative, CCI)에서 COVID-19 위기를 해결하기 위한 디지털 인증서의 기반 기술로 채택하였고, 대한민국 질병관리청과 국내 민간 기업이 공동 개발한 COVID-19 전자예방접종증명 어플리케이션인 쿠브도 W3C의 표준을 활용한 대표적 사례이다[11][12].

2.2 기존의 감염병 예방증명서

2.2.1 COVID-19 증명서 디지털문서 (DDCC:VS)

WHO는 COVID-19 이전에도 황열병, 소아마비 등의 국가 간 감염병 확산을 방지하기 위해 옐로우 카드(Yellow Card)로 알려진 국제공인예방접종증명서(International Certificate of Vaccination and Prophylaxis, ICVP)를 발행하여 여행자들이 특정 국가에 입국할 때 필수 서류로

제출토록 하였다[13]. 이와 유사하게 WHO에서는 COVID-19의 확산을 억제하기 위해 COVID-19 백신 접종 상태를 확인하고 검증할 수 있는 증명서인 DDCC:VS를 발표하였다. Fig.2.는 DDCC:VS가 지원하는 다양한 형태의 문서로 QR 코드가 인쇄된 종이 증명서와 PDF 문서, 스마트폰 증명서를 보여준다[14].

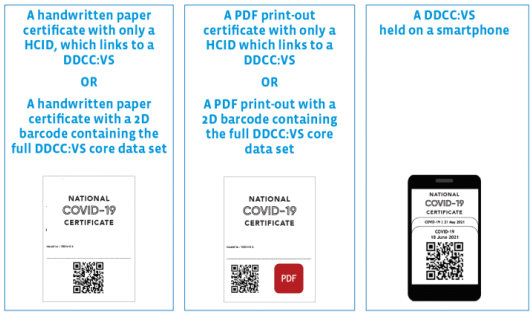

Fig. 2. Example of Digital Document of COVID-19 Certificates:Vaccination Status(extracted from WHO document[14])

WHO에서 발표한 COVID-19 증명서 디지털 문서에 대한 기술 사양 및 구현 지침 의하면 DDCC:VS가 지원하는 다양한 형태의 증명서에는 백신 접종 상태 등 개인의 민감 정보가 포함된다. DDCC:VS는 PKI 기반 전자 서명을 통해 증명서가 제공하는 정보들이 공인된 기관으로부터 검증되었음을 보증한다. 이는 다수의 사람들이 증명서를 제출할 때 그들이 제출한 증명서의 진위 여부와 증명서 발행자에 대한 신뢰성을 검증 가능하게 하며, 이를 기반으로 국가 간 상호 운용 가능한 신뢰 프레임워크 운용을 위해서는 DDCC:VS의 발급과 검증을 위한 각 국가 별 PKI 시스템 구축이 필요하다.

2.2.2 EU 디지털 코로나 증명서 (DCC)

유럽연합(European Union, EU)은 디지털 코로나 증명서인 DCC를 개발하여 유럽연합 회원국과 스위스, 노르웨이 등 비유럽연합 국가에 이를 활용할 수 있게 하였다. 또한 DCC의 글로벌 상호 운용성 확보를 위해 WHO, 국제민간항공기구(International Civil Aviation Organization, ICAO) 등과 협력하고 있다[15]. DCC는 백신접종 이력 뿐만 아니라 PCR 검사 결과, COVID-19 회

Fig. 3. Example of EU paper and digital COVID-19 certificate(extracted from EU documents[16][17])

복증명에 대한 정보를 포함한다. Fig.3.는 DCC가 지원하는 증명서의 예시로 QR 코드가 기록된 종이 증명서와 디지털 증명서의 예시를 보여준다[16][17].

EU의 DCC는 전반적으로 탈중앙화 방식으로 구현되며 일부 중앙 집중 방식을 포함한다. DCC가 지원하는 증명서에 포함된 정보의 무결성 및 진위 보호를 위해 PKI 기반 기술이 필요하며, DCC를 채택해 사용하는 국가는 국가 서명 인증기관(Certificate Signing Certificate Authorities, CSCA) 목록과 유효한 문서 서명용 인증서(Document Signer Certificate, DSC) 목록을 제공하고 해당 목록을 항상 최신 상태로 유지해야 한다[18].

2.2.3 한국 코로나19 전자예방접종증명, 쿠브 (COOV)

한국의 코로나19 예방 접종 인증 시스템인 쿠브는 증명서 증명서 위·변조 문제와 이용자들의 개인정보가 중앙 서버에 남겨져 발생하는 프라이버시 문제를 해결하기 위해 W3C의 분산ID 기술을 이용한다. 그리고 앞서 기술한 WHO의 DDCC:VS, EU의 DCC와 같이 QR 코드 기반의 디지털 증명서 제출 방식을 통해 사용자 자신의 예방 접종 여부를 증명하고 타인이 제시한 QR 코드 스캔을 통해 상대방의 백신 접종 상태도 검증 가능하도록 하였다. 쿠브는 모바일 앱을 통해 디지털 증명서를 발급 받고 제출하는 시스템으로, 여기에 본인 인증용 증명서와 여권정

Fig. 4. Example of user interfaces in COOV application (extracted from Coov Mobile Vaccination Certificate document[12])

보를 연동해 다양한 인증 시스템으로 확장 및 활용 가능하게 한다[19]. Fig.4는 쿠브의 사용자 화면 예시이다.

앞서 기술한 증명서를 비롯해 기존의 감염병 예방 디지털 증명서는 정적(Static) 혹은 동적(Dynamic) 방식의 QR 코드를 사용한다. QR 코드는 이용자가 단일 증명서를 제출할 때 쉽고 편리하게 사용할 수 있는 이점이 있지만, 증명서의 도용, 복제 등으로 인한 보안 위협과 QR 코드 검증을 위해 반드시 통신망이 연결되어야 하는 제약점이 존재한다. 따라서 이 논문은 3.3장의 기존 증명서 시스템과 제안 시스템과의 비교 분석을 통해 기존의 감염병 예방 디지털 증명서의 QR 코드가 가지는 보안 위협 문제를 살펴보고, 이를 효과적으로 대응할 수 있는 방안으로서 블루투스 등 무선통신 기술 기반의 감염병 예방 디지털 증명서를 제안하고자 한다. 또한 제안 시스템은 이용자 편의성을 높이기 위해 다수의 증명서를 이용자 선택에 따라 일괄 검증 가능토록 한다는 점에서 기존의 감염병 예방 디지털 증명서와 차별화를 두었다.

2.3 국제 표준화 현황

현재는 COVID-19 관련 감염병 예방증명서 시스템 구현을 위해 공개된 국제 표준이 없기 때문에, 여러 국가와 기업 등은 앞서 기술한 W3C의 분산ID 관련 표준이나 WHO의 기술 지침을 기반으로 증명 시스템을 개발하여 사용 중이다. 국내 질병청과 한 민간 기업에서 개발한 COVID-19 예방접종증명서인 쿠브는 W3C의 표준을 기반으로 한 대표적 사례에 해당한다. EU의 DCC는 WHO의 최신 지침을 준수하고 있으며, 약 60개국이 DCC 체계를 이미 활용하거나 도입을 준비 중이다. 특히 국제항공운송협회(International Air Transport Association, IATA)는 IATA 트래블패스(Travel Pass)와 완벽하게 연동되는 EU의 DCC를 글로벌 표준으로 지원한다고 발표했다[20].

2021년 8월에는 국제 표준화 기구인 ITU-T(International Telecommunication Union Telecommunication)와 WHO가 COVID-19 디지털 백신증명서의 국제 표준화를 논의하기 위한 워크숍을 실시했다. WHO와 회의 참가국들은 관련 증명서가 국가 간 상호 연동이 가능하고 국제 사회에 적합한 백신 여권으로 활용되기 위해서는 분산ID 기반의 분산신원증명 기술이 필요하다는 것에 동의했다. 2021년 10월 ITU-T TSAG에서 기존 표준화 활동을 조정하기 위한 JCA-DCC를 신설하기로 합의했고, 향후 세부적인 표준화 활동은 SG17을 포함하는 관련 ITU-T 연구반에서 추진될 것으로 예상한다[21][22].

III. 분산ID 기반의 감염병 예방 디지털 증명서 시스템 제안

3.1 제안 시스템 구성

본 논문은 이용자의 편의성을 향상시키고 보안성을 높이기 위한 분산ID 기반의 감염병 예방증명시스템을 제안한다. 이는 감염병에 대한 검증이 필요한 경우에 사용된다. 이 논문에서 제안하는 시스템은 증명서를 단 한 번 제출함으로써 여권(신분증), 항공 탑승권, 백신접종증명서 및 다양한 감염병 검사 증명서 등 모든 증명서를 동시에 검증 가능하며 기존의 QR 코드 방식의 증명서가 가지는 보안 문제점에 대한 대안이 될 수 있다. 본 장에서는 제안시스템의 주요 구성요소와 필요한 구성기술들을 언급하고자 한다.

Fig.5.은 본 논문이 제안하는 분산원장기술 기반의 탈중앙화(decentralization) 디지털 감염병 예방 증명서 시스템의 전체적인 구성을 나타내며, 주요 구성요소는 다음과 같다.

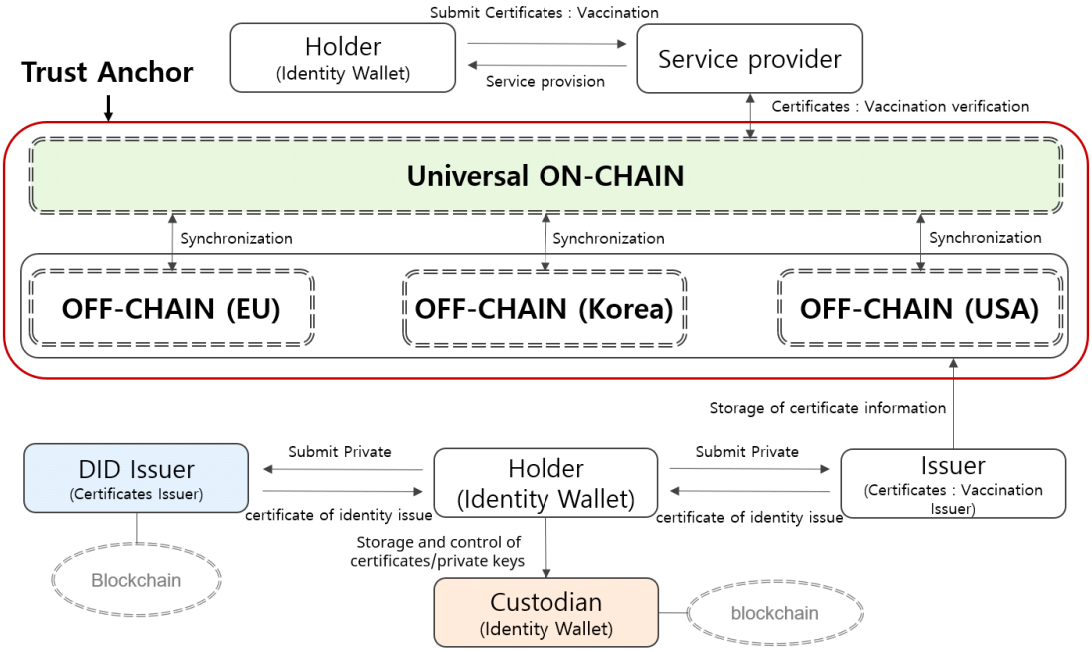

Fig. 5. The architecture of the proposed system

- 이용자(holder) : 개인인 정보주체로 각종 증명서들의 소유자
- 신원지갑(identity wallet) : 각종 증명서를 보관하는 저장소로 스마트폰 어플리케이션과 같은 모바일 기기의 전자지갑(앱)
- 서비스 제공자(service provider) : 공항, 마트, 경기장 등 다수의 대중이 이용하는 시설에서 이용자가 제출한 신원증명서(분산ID)를 검증하여 이용자의 신원을 확인한 후 서비스를 제공하는 기관 또는 사업자
- 신뢰 앵커(trust anchor) : 디지털 서명을 확인하고 인증 경로를 확인할 수 있는 구조〔23〕
- 유니버셜 온-체인(universal ON-CHAIN) : 제안 시스템에서 국가 간 도메인에 대하여 신원증명이 필요할 경우 사용되는 신뢰 저장소
- 오프-체인(OFF-CHAIN) : 이용자의 개인정보를 포함하고 있는 증명서 정보를 저장하는 신뢰 저장소
- 분산ID 발행자(DID issuer) : 분산원장기술을 기반으로 이용자에게 신분증, 여권과 같은 이용자의 분산ID를 발급하는 기관
- 발행자(issuer) : 백신접종증명서, PCR 검사 결과지, 감염병 회복 증명서 등 감염병 관련 건강 정보를 발급하는 기관
- 수탁 보관자(custodian): 스마트폰에 저장된 이용자의 개인키(private key)와 감염병 관련 증명서의 분실을 고려하여 이용자의 분산ID 및 여러 증명서들을 안전하게 보관할 수 있는 분산원장기술 기반의 제3의 기관 또는 저장소〔24〕

정보주체인 이용자는 서비스 제공자로부터 감염병 관련 증명서를 발급 받기 위해 분산ID 발행자를 통해 자기 신원을 증명하는 분산ID 형태의 신원증명서를 발급 받아 이를 서비스 제공자에게 제출하고, 서비스 제공자는 이용자가 제출한 신원증명서를 검증해 이용자가 요청한 증명서를 발급한다. 따라서 이용자의 신원지갑에는 이용자의 신분증에 해당하는 분산ID와 감염병 관련 증명서가 함께 저장된다. 이때 이러한 중요한 정보들을 수탁 보관자에게 보관함으로써 단말기기의 분실, 교체 또는 이용자의 분산ID 및 개인키의 유출 등에 대한 보안 문제를 해결할 수 있다.

이 논문이 제안하는 시스템은 감염병의 확산 방지를 위한 신뢰 가능 수단으로 제시된다. 이를 위해 이용자가 서비스 제공자에게 신원증명서를 제출하면,

이용자의 식별 여부, 제출한 신원증명서의 진위성, 신원증명서의 발행자 검증 등이 동시에 이루어져야 할 것이다. 여러 가지 요소를 검증하기 위해서는 신뢰앵커 구축이 필요하며, 제안 시스템은 유니버셜 온-체인과 오프-체인 기반의 신뢰 앵커를 구축한다. 다수의 국가와 서비스 제공자들은 유니버셜 온-체인을 사용해 증명서를 검토하게 되는데, 유니버셜 온-체인에는 증명서 검증을 위한 최소 정보 (이용자 및 발행자의 식별자, 이용자 및 발행자의 공개키 등)만 저장되어 있고, 개인정보는 포함되어 있지 않다. 오프-체인에는 개인정보가 포함될 수 있으며 정부기관 또는 권한을 위임받은 기관이 관리할 수 있다. 또한 유니버셜 온-체인과의 동기화를 통해 온-체인에 저장되어야 할 내용을 동기화한다. 즉, 신뢰 앵커는 서비스 제공자가 증명서를 검증할 때 디지털 서명과 인증 경로를 확인할 수 있는 근거가 되며, 누구든지 이용할 수 있지만 보안성과 편의성을 고려하여 노드운영 및 관리 권한을 부여하는 공개형(public)과 허가형(permissioned) 분산원장 기술로 구성해 데이터의 위·변조 방지를 제공한다. 앞서 설명한 제안 시스템의 구현은 아래와 같은 기술 요소를 필요로 한다.

- JSON(JavaScript Object Notation) : 각종 디지털 증명서는 JSON을 사용하여 증명서 안에 구성된 이용자, 발행자, 날짜, 서명 등을 표현한다. 또한 데이터를 전송할 때 JSON형식을 사용하여 전송함으로써 각각의 엔티티를 표현한다.
- 검증 가능한 데이터 모델 : Fig.1.과 같은 검증 모델을 통해 자신의 신원을 검증받는다. ① 이용자가 발행자에게 자신의 신원 정보 및 증명서 정보를 전달한다. ② 발행자가 이용자가 준 정보를 전달 받으면 발행자의 서명용 개인키로 서명된 VC만들어 이용자에게 전달하고 검증 가능한 데이터 저장소에 저장한다. ③ 이용자는 발행자에게 전달받은 VC를 이용하여 이용자의 서명용 개인키로 서명한 검증 가능한 프레젠테이션(verifiable presentation, VP)을 생성하여 검증자에게 검증을 받는다. ④ 검증자는 VP를 이용자의 공개키를 이용하여 서명하고, 검증 가능한 데이터 저장소에 저장된 VC를 통해 검증한다.
- 신뢰확장을 위한 블록체인 : 증명서에 대한 서명을 검증할 때 블록체인에 저장되어 있는 공개키를 사용함으로써 공개키가 위·변조 되지 않고 신뢰할 수 있는 공개키임을 보장하며 해당 증명서 또한 신뢰할 수 있다. 즉, 블록체인으로 인한 신뢰체인이 형성됨에 따라 신뢰성이 확장된다.

3.2 제안 시스템 동작 원리

이 장에서는 감염병 예방 디지털 증명서 시스템의 동작원리를 단계별로 설명한다. Fig.6.은 Fig.5.를 감염병 예방 증명서 시스템에 적용한 모델이다. 감염병 예방 증명서 시스템 내의 여러 가지 증명서들을 분산원장에 등록하고, 검증받는 단계는 아래와 같다.

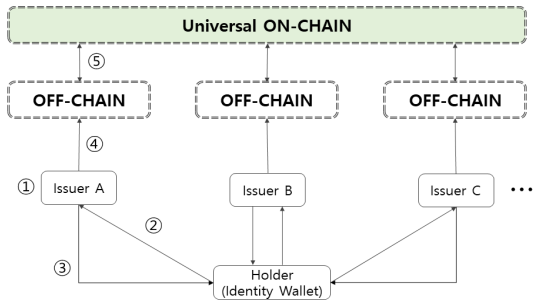

Fig. 6. The process for issuing various digital certificates

① 감염병 예방 증명서 시스템에는 여러 가지 증명서들이 존재하고 각 증명서 마다 다른 발행자가 존재한다.

② 이용자는 발급받고자 하는 증명서 발행자에게 이용자의 공개키 및 개인정보를 제공한다.

③ 발행자는 자신의 전자서명이 포함된 증명서를 이용자에게 발급한다.

④ 증명서는 이용자의 신원 지갑에 저장되고 오프-체인에 이용자의 공개키 및 개인정보를 포함한 증명서 발행 정보와 발행자의 공개키를 저장한다.

⑤ 유니버셜 온-체인에 오프-체인에서 변경된 내용을 반영하여 데이터를 동기화한다.

⑥ 이용자의 단말기와 서비스 제공자 단말기를 상호 감지하고 통신을 초기화한다. 여기서 서비스 제공자란 공항, 공연장, 백화점, 전시장 등 다수의 사람들이 모이거나 이용하는 장소를 의미한다.

⑦ 서비스 제공자 단말기가 이용자에게 증명서를 요청한다.

⑧ 이용자의 단말기에서 이용자의 전자서명이 포

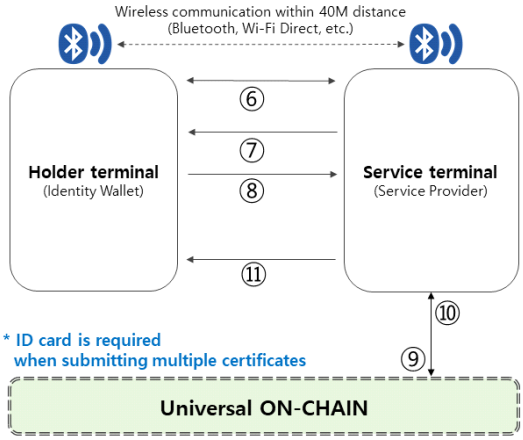

Fig. 7. The process for digital certificate presentation and verification

함된 증명서를 제출한다. (신분증, 탑승권, 백신접종 증명서, 감염병 검사 증명서, 감염병 회복 증명서 등이 포함될 수 있음)

⑨ 발행자의 식별자 및 공개키 등을 이용하여 다수 증명서를 일괄 검증한다. (증명서 자체 위변조 검증 및 증명서 발행자의 신원 검증 수행)

⑩ 이용자의 식별자 및 공개키 등을 이용하여 다수 증명서를 일괄 검증한다. (증명서 제출자의 신원과 증명서에 기록된 개인정보가 일치하는지를 검증 한다.)

⑪ 이용자에게 서비스를 제공한다.

이용자들은 위의 단계들을 통하여 감염병 예방 증명서를 한 번만 제출하면 동시에 여러 개의 증명서들을 일괄적으로 검증받을 수 있어 이를 편리하게 사용할 수 있다. 이때 여러 종류의 신원지갑에 이용자의 신분증, 탑승권, 백신접종증명서, 감염병 검사 증명서, 감염병 회복 증명서 등 여러 가지 증명서를 보관할 수 있다. 본 시스템에서 사용하는 신원 지갑은 아래와 같이 공용 신원 지갑, 이종 신원 지갑, 페더레이션(Federation) 신원 지갑 등이다.

Fig.8.은 공용 신원 지갑의 구성도이다. 공용 신원 지갑은 하나의 신원 지갑에 신분증, 탑승권, 백신접종증명서, 감염병 검사 증명서, 감염병 회복 증명서등 모든 증명서를 보관하며, 서로 다른 증명서를 한 곳에 저장하기 때문에 높은 호환성이 요구된다.

Fig. 9.은 이종 신원 지갑의 구성도이다. 이종 신원 지갑은 모바일 단말기의 다수 신원 지갑에 서로 다른 증명서를 각각 보관한다. 따라서 공개 API를 기반으로 한 이종의 신원지갑 간 상호 호환성을 유지해야 한다.

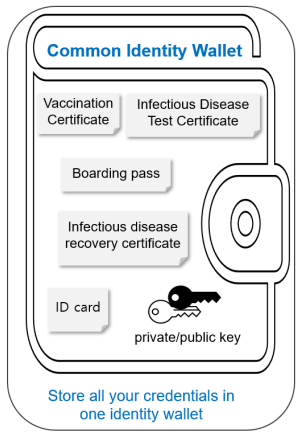

Fig. 8. Common identity wallet

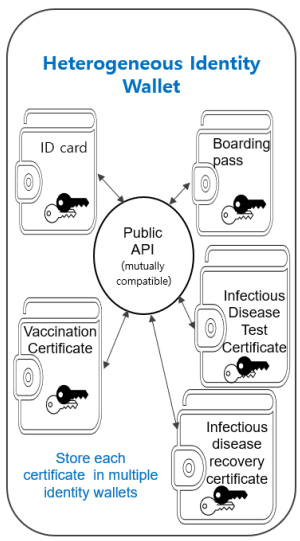

Fig. 9. Heterogeneous identity wallet

Fig.10.은 페더레이션(Federation) 신원 지갑의 구성도이다. 페더레이션 신원 지갑은 하나의 신원 지갑에 여러 증명서를 통합하여 보관하는 방식으로, 공용 신원 지갑과 유사한 방식이다. 공용 신원 지갑과의 차이점은 해당 신원 지갑을 수탁 보관자가 제공한다는 점이다. 이처럼 설계 환경을 고려하여 시스템에 맞는 신원 지갑을 선택하여 시스템을 구현할 수 있다.

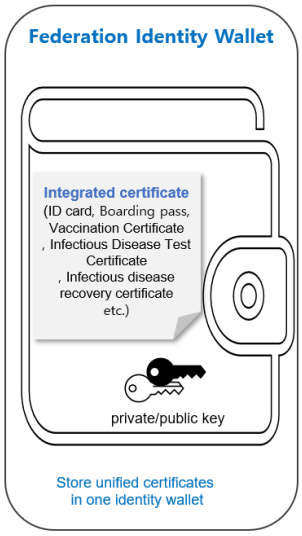

Fig. 10. Federation identity wallet

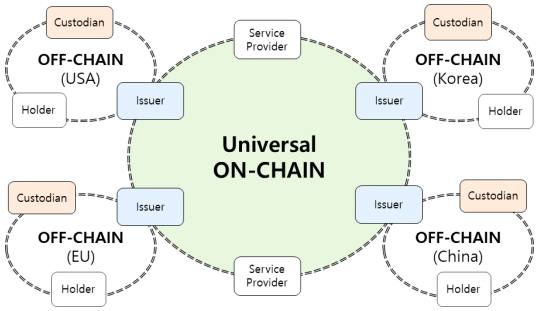

Fig. 11. Participants in the proposed digital certificate system in the universal on-chain and off-chain

Fig.11.은 해당 시스템을 글로벌 측면에서 바라본 구성도이다. 유니버셜 온-체인에는 전 세계 국가의 각종 증명서 발행자, 서비스 제공자 등이 참여하고, 오프-체인에는 국가별/지역별 이용자, 각종 증명서 발행자, 수탁 보관자 등이 참여한다. 이 시스템을 도입하면 유니버셜 온-체인으로 국가 간 네트워크가 형성되어 국가 간 이동시에 편리하고 안전하게 각종 증명서를 검증할 수 있다.

3.1 기존 증명서 시스템과 제안 시스템과의 비교분석

3.1.1 QR 코드 증명서와 비교

앞서 설명한 바와 같이 WHO의 DDCC:VS, EU의 DCC, 우리나라의 COOV 등 현재 사용되는 감염병 예방 증명서 시스템은 종이나 모바일 앱에 삽입된 QR 코드를 기반으로 증명서를 제출하고 이를 검증하도록 한다. QR 코드는 코드가 생성되면 저장된 데이터를 변경할 수 없는 정적 QR 코드와 데이터 변경이 가능한 동적 QR 코드 모두 사용될 수 있다. 증명서 제출 시 이용자는 QR 코드가 포함된 증명서를 QR 코드 리더기에 인식 시켜야하므로, QR 코드 종류에 관계없이 이를 반드시 외부에 노출해야만 한다. 그러나 외부로 드러난 QR 코드는 복제나 도용이 가능하고 위·변조될 수 있어 감염병 예방과 확산 방지를 위한 해당 시스템의 도입 목적에 부합하지 않는 방식으로 악용될 수 있다. 또한 기존의 증명서는 다수의 증명서 제출 시 증명서를 생성하고 각각을 스캔해야 하므로 이용자의 불편함을 초래한다. Table 2.는 기존의 QR 코드 기반의 증명서 시스템과 무선 통신 방식을 이용하는 제안 시스템을 비교하여 제안 시스템이 가지는 차별점을 설명한다.

첫 번째로는 사용하는 기술과 증명서 제출 방식의 차이가 있다. 제안 시스템은 블루투스 또는 와이파이 다이렉트를 사용한 근거리 통신 기술을 통해 증명서 제출 시 이를 기반으로 하고, 기존 시스템은 이미지 인식 기술을 활용해 카메라를 통한 초근접 QR 코드 스캔으로 증명서를 제출한다. 두 번째로는 제안 시스템에서의 인증서 복제가 기존 시스템 보다 어렵다. 세 번째로는 제안 시스템에서의 증명서 도용이 기존 시스템 보다 어렵다. 네 번째로는 제안 시스템에서의 증명서 변조가 기존 시스템 보다 어렵다. 다섯 번째는 인증서 제출 방법의 차이로, 제안 시스템은 신분증 및 다수 증명서의 일괄 자동 제출이 가능하지만 기존 시스템은 각각의 신분증 및 증명서를 각기 제출해야한다.

기존의 증명서 시스템이 가지는 제약점과 보안 위협 사항을 해결하기 위해 이 논문이 제시하는 증명서 시스템은 다음과 같은 장점이 있다.

- 편리한 증명서 제출 및 이용자 밀집도 분산 : QR 코드 방식은 증명서를 제출 할 때 카메라를 통하여 초근접 QR 코드 스캔을 한다. 이 때, 카메라 화질이 낮거나 인식이 잘 안 되는 경우가 많아 이용자 편의성이 감소된다. 반면에 무선 통신 방식을 이용하면 블루투스 통신 범위내로 이용자의 단말기가 가까이 접근 했을 때, 자동으로 이를 인식을 하여 모바일 앱에서 증명서 제출에

Table 2. Digital certificate presentation methods using wireless communication and QR code

	Wireless communication	QR code	
		Dynamic	Static
Technology & Methods of proof	Short-range approach via Bluetooth, Wi-Fi Direct	Image recognition (Very close-rage scanning QR code with camera)	
Difficulty level of certificate copy	High	Low	Very Low
Difficulty level of certificate theft	High	Low	Very Low
Difficulty level of certificate modification	High	Low	
Certificate verification	Automatic submission and verification of IDs and multiple certificates	Submit and verify the number of IDs and certificates	

대한 동의 버튼만 누르면 증명서를 제출할 수 있다. 또한 기존 QR 코드 방식의 증명서 제출은 QR 코드 인식기에 매우 가까이 (10cm ~ 30cm 내외) 다가가 증명서를 제출하여야 하여 사람들을 매우 좁은 공간에 밀집시키지만 상대적으로 블루투스나 와이파이 다이렉트 (5m ~ 10m)는 매우 좁은 공간에 사람을 밀집시키는 정도를 낮출 수 있다. 그리고 여러 사람의 증명서를 동시에 검증함으로써 기존의 증명서에 비해 비교적 빠른 시간에 처리가 가능하다.

- 증명서 복제·도용 방지 : QR 코드 방식은 정적 QR 코드와 동적 QR 코드 방식이 있다. 정적 QR 코드는 QR 코드가 한번 생성되면 코드 내의 데이터가 변하지 않기 때문에 QR 코드를 캡처하여 SNS 등으로 공유하면 언제 어디서나 증명서를 사용할 수 있다. 동적 QR 코드 방식인 경우에도 일정 시간(예.15초)내로 SNS를 통해 공유가 가능하기 때문에 증명서의 복제 및 도용이 쉽다. 하지만 제안시스템은 사용자 단말기에서 서비스 제공자 단말기로 무선 통신을 통한 증명서를 제출하기 때문에 복제·도용이 어렵다
- 증명서 변조의 어려움 : QR 코드 방식은 QR 코드가 노출되어 있기 때문에 디코딩을 통하여 QR 코드 내에 있는 데이터 값들을 손쉽게 변조할 수 있다. 해당 사항을 프로그램화 시켜서 실행시킨다면 변조된 QR 코드가 생성되기까지 단 몇초 밖에 걸리지 않아서 동적 QR 코드 방식으로도 대응할 수가 없다. 하지만 제안시스템은 증명서제출 시 무선통신을 이용하기 때문에 외부에 노출될 위험이 적어 변조가 어렵다.
- 인터넷 연결 제약을 최소화 : 정적 QR 코드의 보안 위협을 낮추기 위해 동적 QR 코드를 사용하는 경우, 이용자의 감염병 예방 디지털 증명서 시스템은 일정 시간 간격으로 증명서를 갱신하기 위해 이를 관리하는 각 국가의 보건당국이나 관련 데이터 저장 서버에 항상 연결되어 있어야 한다. 만일 인터넷 연결이 원활하지 않으면 QR 코드 갱신이 어렵고 이용자의 증명서 제출과 서비스 제공자의 증명서 검증을 정상적으로 수행할 수 없다. 이 논문은 해당 문제를 해결하기 위한 대안으로 감염병 예방 디지털 증명서 시스템에 블루투스나 와이파이 다이렉트 기술을 활용하도록 하였다.
- 증명서 일괄 제출 : QR 코드 방식은 신분증 및 제출이 요구되는 증명서의 개수만큼 여러 차례 QR 코드를 생성하고 스캔해야 한다. 그러나 무선 통신 방식을 도입하면 이용자의 신분장과 제출이 필요한 다수의 증명서를 선택하여 동시에 자동 제출할 수 있고, 증명서 상의 신원과 신분증 상의 신원을 일괄적으로 비교 검증할 수 있어 증명서 시스템의 가용성(availability)과 편의성을 향상시킬 수 있다.

여러 국가에서 QR 코드 방식의 감염병 예방 증명서를 사용하고 있지만, 위에 언급한 이유로 분산ID 기술을 이용한 무선 통신 방식의 예방 증명서 시스템이 도입 된다면 글로벌 서비스 측면에서도 더욱 편리하고 보안 수준이 높은 서비스 제공이 가능할 것이다.

3.1.2 PKI 기반 증명서와 비교

이 논문이 제안하는 분산ID 기반의 디지털 증명서는 근본적으로 PKI를 이용한 전자서명을 기반으로 한다. 그러나 중앙 집중형 시스템에 의존하지 않는다는 점에서 PKI 기반의 증명서와 차이가 있다. 특히 온-체인은 탈중앙화 방식의 블록체인 기반 저장소로, 증명서 검증을 위한 공개키를 블록체인에 저장해 데이터의 위·변조를 어렵게 함으로써 무결성(integrity)을 강화하고, 탈중앙화 방식으로 운영되는 시스템 특성 상 PKI 기반의 증명서에 비해 시스템 가용성, 확장성, 상호운용성 등을 높이는 장점이 있다. 이 장에서는 PKI 기반의 감염병 예방 디지털 증명서와 분산ID 기반의 감염병 예방 디지털 증명서를 생성하고 검증하는 간단한 실험을 통해 두 방식의 증명서 시스템에 대한 성능을 비교하였다.

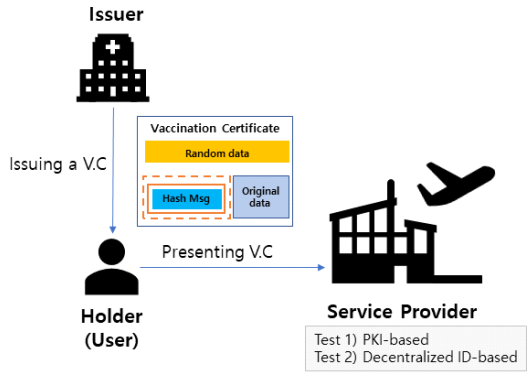

Fig. 12. The process of issuing and presenting certificates for the testing

해당 실험의 목적은 이용자가 Fig.12.와 같이 발행자로부터 감염병 예방 디지털 증명서를 발급 받고 이를 서비스 제공자에게 제출할 때, 각 각의 디지털 증명서를 검증하는데 걸리는 시간량을 측정함으로써 PKI 기반의 디지털 증명서와 분산ID 기반의 디지털 증명서가 가지는 정량적 차이점을 알아보기 위함이다. 실험은 Table 3.와 같이 동일한 서버 환경에서 진행하였다.

PKI와 분산ID 기반의 디지털 증명서를 생성하고 검증하는 전체 과정은 각 각 Fig.14., Fig.15.와 같으며, 실험을 위해 공통적으로 전제되어야 할 몇 가지 사항들이 있다.

Table 3. Test server specifications

Classification	Specifications
CPU	Intel(R) Xeon(R) CPU E5-2670 v3 @ 2.30GHz
Memory	1 GB
OS	ubuntu-18.04

- 감염병 예방 디지털 증명서 : 감염병과 관련된 임의의 간략한 정보를 기입한 파일(원본 파일)과 이에 대한 해시 메시지 및 감염병 예방 디지털 증명서 사이즈를 동일하게 맞추기 위한 랜덤 데이터로 구성하여 생성한다. Fig.13.은 실험에 사용된 감염병 예방 디지털 증명서의 내용과 구성을 보여준다.

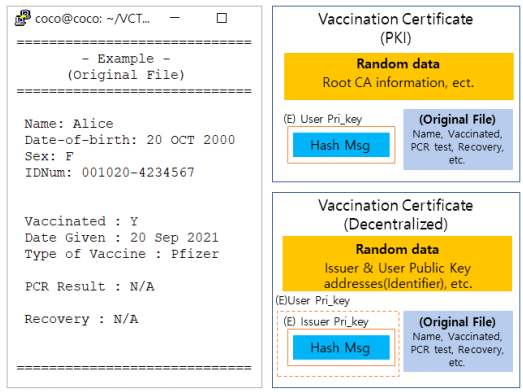

Fig. 13. Examples of digital certificates

- 공개키 저장소 : PKI와 분산ID 기반의 감염병 예방 디지털 증명서 시스템의 실제 사용에서 이용자, 발행자 및 상위 기관의 공개키는 외부의 별도 저장소에 저장된다. 실험에서는 각 디지털 증명서의 검증 시간 비교를 위해 동일 서버내의 별도 디렉토리를 공개키의 저장소로 가정한다.
- 원본 파일의 해시 알고리즘 : SHA-256 알고리즘을 사용한다.
- 이용자, 발행자 및 상위 인증기관(Root CA)의 공개키와 개인키 생성과 검증 알고리즘 : RSA-2048 알고리즘을 기반으로 한다.
- 감염병 예방 디지털 증명서는 이용자가 이미 발급 받은 것으로 가정하여 측정 시간에는 포함하지 않는다.

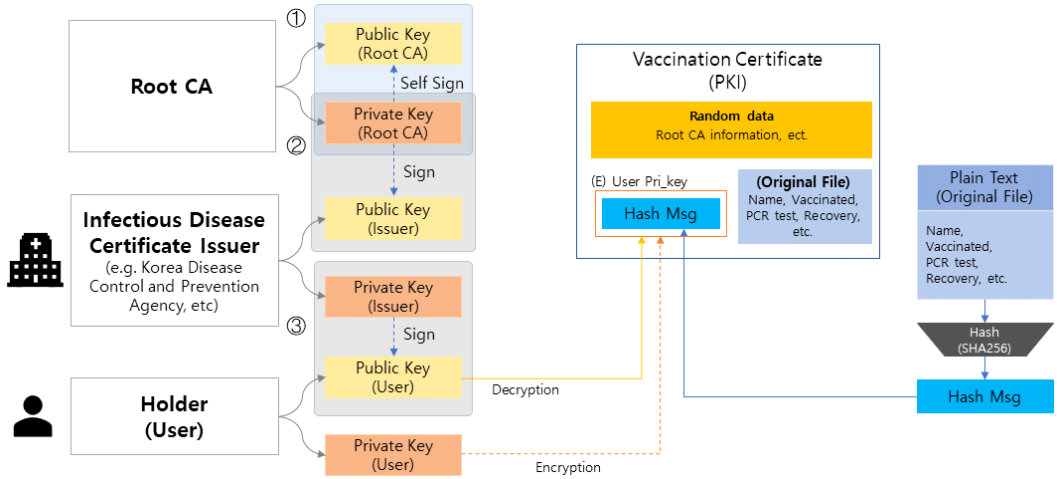

Fig. 14. Verification of digital certificate signature generated by digital certificate based on PKI

실험은 PKI 및 분산ID 기반의 감염병 예방 증명서를 서비스 제공자에게 제출한 뒤 이를 검증하는데 걸리는 시간을 각 10회씩 측정하여 이 값들에 대한 평균 시간을 구하는 방식으로 진행하였다. 검증 시간은 각 전자서명문의 복호화 시간과 원본 파일을 SHA-256으로 해시한 값을 감염병 예방 디지털 증명서에 저장된 해시값과의 동일 여부를 비교하고 비교값이 동일할 경우, 이 과정에 소요되는 시간을 포함하여 전체 시간이 출력되도록 하였다. 실험 결과는 Table 4. 와 같다. 분산ID 기반의 감염병 예방 디지털 증명서 검증에 비해 PKI 기반의 감염병 예방 디지털 증명서 검증에 약 2.5배 이상 더 많은 시간이 소요되는 것을 확인할 수 있었다. 본 실험에서 분산ID의 리졸버(resolver)에 대한 시간은 캐시값에 이미 저장되어 있다고 가정을 했기 때문에, 실험 결과값에는 포함하지 않았다. 만약 리졸버에 대한 시간이 필요하다면 실험에서 측정된 시간량에서 해당 리졸버 시간만큼의 시간이 더 추가될 것이다.

PKI 및 분산ID 기술을 적용한 감염병 예방 디지털 증명서 검증은 Fig.14.와 Fig.15.에서처럼 감염병 예방 디지털 증명서 발행자의 신뢰성과 발급 증명서의 진위 여부 검증을 위한 Root CA 등 상위 기관의 검증 단계 유무에 따른 시간적 차이를 보인다. 분산ID 기반의 감염병 예방 디지털 증명서는 PKI 기반 증명서에서 요구되는 상위 기관의 검증 단계를 거치지 않고, 디지털 증명서에 포함된 발행자와 이용자의 개인키로 전자서명 된 해시 메시지를 유니버셜 온-체인에서 가져온 각 각의 공개키로 바로 복호화하기 때문이다. 따라서 분산ID 기반의 감염병 예방 디지털 증명서는 PKI 기반의 감염병 예방 디지털 증명서 대비 효율적인 성능을 가질 수 있다. 또한 PKI 기반의 시스템은 증명서 검증을 위한 서명문 공개키를 보관하는 게이트웨이가 반드시 필요하다. 그러나 블록체인 방식의 시스템은 공개키를 블록에 바로 저장하고 필요시 이를 가져올 수 있기 때문에 PKI 방식에 반드시 요구되는 게이트웨이를 필요로 하지 않는다는 점에서 차이점을 보인다.

Table 4. Test results (unit : sec)

Test	PKI-based	Decentralized ID-based
1	0.003159	0.001422
2	0.003147	0.001246
3	0.003446	0.001468
4	0.003488	0.001271
5	0.003294	0.001223
6	0.003469	0.001274
7	0.003491	0.001236
8	0.003228	0.001409
9	0.003327	0.001394
10	0.003527	0.001235
Average Time	**0.003358**	**0.001318**

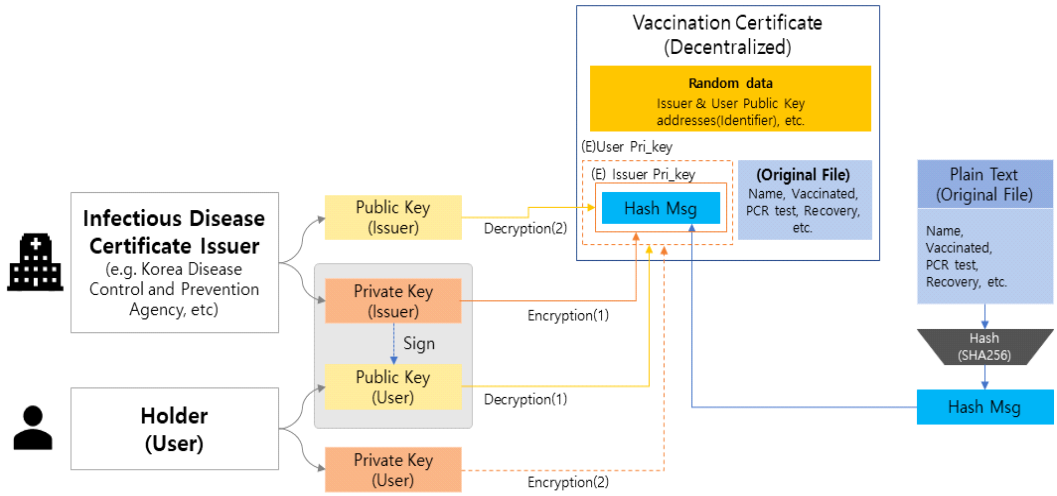

Fig. 15. Verification of digital certificate signature generated by digital certificate based on Decentralized identity

IV. 제안 시스템의 보안 위협 및 요구사항

4.1 제안 시스템의 보안 위협

제안 시스템은 분산ID을 이용한 디지털 감염병 예방 증명서 시스템으로 블루투스 또는 와이파이 다이렉트 무선 통신기술을 사용하며, 본 제안 시스템에 대한 보안 위협은 다음과 같다.

- 증명서 위·변조(ST1) : 진본 증명서를 발급 받지 않고 백신 접종 완료, PCR 음성 결과 및 사실과 다른 정보를 입력해 증명서를 위·변조 할 수 있다.
- 증명서 개인정보 유출 및 노출(ST2) : 이용자의 단말기에서 서비스 제공자의 단말기로 증명서를 제출할 때, 서비스 제공자가 요구하지 않은 증명서까지 동시에 제출하게 되면 이용자의 불필요한 개인정보가 유출 및 노출될 수 있다. 또한 증명서 자체가 유출되는 경우에도 이용자의 개인정보가 제3자에게 노출될 수 있다.
- 노드 내 이용자 정보 위·변조(ST3) : 본 시스템의 분산ID 네트워크 내의 노드가 악성코드 등에 감염(예: 중간자 공격 등)되면 이용자의 각종 정보가 위변조 될 수 있다. 만약 발행자 노드가 악성코드에 감염되면 발행자는 이용자의 위·변조된 신원정보나 감염병 관련 정보를 오프체인에 전송함으로써 잘못된 정보가 저장된다.
- 증명서 양도 및 도용(ST4) : 증명서 제출 시 증명서 이용자 검증을 할 수 없다면, 증명서 제출자가 해당 증명서의 실제 소유자임을 나타낼 수 없고 타인의 증명서 양도 및 도용이 가능하다.
- 발행자 검증 미흡(ST5) : 증명서 제출 시 발행자의 신뢰성을 검증할 수 없다면, 발급된 증명서의 신뢰성을 검증하기 어렵다.
- 증명서 이용자 개인키 유출 및 유실(ST6) : 본 시스템에서는 증명서제출 시 해당 증명서를 검증하기 위한 개인키가 필요하다. 관리 소홀로 인한 개인키가 유출되거나 유실되면 증명서에 대한 소유권을 상실할 수 있다.
- 전송 데이터의 비인가적 접근(ST7) : 본 시스템은 블루투스나 와이파이 다이렉트를 사용하여 증명서를 제출하기 때문에 무선통신구간이 취약하다면 발생할 수 있는 위협이 존재한다. 무선통신구간이 암호화가 되어 있지 않거나 비 인가된 접근이 가능하게 되면 스니핑(sniffing), 세션 하이재킹(session hijacking) 등과 같은 공격을 통하여 이용자 단말기와 서비스 제공자 단말기 사이에서 통신하는 정보에 접근할 수 있다.

4.2 제안 시스템 보안 요구사항

4.1에서 언급한 보안 위협에 대한 보안 요구사항은 다음과 같다.

- 증명서 진위성 확인(SR1) : 검증자를 통하여 신뢰할 수 있는 발행자가 발급한 증명서 인지를 확인하고, 이용자가 제출한 증명서가 신뢰 할 수 있는 발행자가 발급한 증명서가 맞는지 확인한다. 해당 증명서가 신뢰할 수 있는 기관에서 발급했다면 해당 증명서는 올바른 증명서이다. 또한 증명서 위·변조를 방지하기 위해 암호 키로 암호화를 해야 한다.
- 개인정보 마스킹·익명처리, 암호화(SR2) : 접종증명서와 같이 접종유무만 판단하기 위한 증명서들은 증명서 내에 많은 개인정보를 필요로 하지 않는다. 접종 유무만 확인 하면 되기 때문에 암호 키로 증명서의 진위성만 검증하고, 증명서 내의 개인정보를 마스킹 및 익명처리를 하여 관리하면 증명서가 노출이 되어도 누구의 신원정보인지 확인을 할 수 없다. 다른 방법으로는 신원정보에 대한 암호화처리를 통하여 제 3자에게 노출되는 것을 방지 할 수 있다. 또한 증명서를 제출할 시 서비스 제공자가 원하는 증명서만 제출 할 수 있게 선택적 증명서 제출 기능을 추가하여 불필요한 증명서 제출을 방지 할 수 있다.
- 악성코드 통제(SR3) : 분산ID 네트워크내의 노드에 있어서 악성코드 감염으로 인한 정보의 위·변조 및 유출을 방지하기 위해 보호 대책이 필요하다. PC 백신을 통해 실시간 검사를 하고 치료를 해야 한다. 또한 침입방지시스템(IPS, Intrusion Prevention System)등과 같은 시스템을 이용하여 악의적인 행위로 추정되는 네트워크를 차단하는 등의 조치를 할 수 있다.
- 본인 확인(SR4) : 증명서 제출 시 해당 증명서가 제출자의 소유인지를 판단하기 위한 수단이 필요하다. 모바일 어플리케이션으로 증명서 제출 시 1차적으로 지문, 홍채 인식 등 제 3자가 소유할 수 없는 정보를 통하여 본인임을 검증하고, 2차적으로 디바이스 내에 저장되어 있는 암호 키(개인키)를 사용하여 증명서의 소유자임을 검증한다.
- 발행자 검증(SR5) : 발행자는 증명서에 암호 키(개인키)로 서명 및 암호화하여 이용자에게 발급하고 이용자는 해당 증명서를 사용한다. 이 때 발행자가 신뢰할 수 있는 발행자 리스트에 있고, 암호 키(개인키)가 발행자의 암호 키(개인키)가 맞다면 해당 증명서에 나타나있는 발행자는 신뢰할 수 있다.
- 암호 키 관리(SR6) : 암호 키 유실을 대비하여 암호 키 복사본을 생성한 후 접근 제어가 가능한 암호 모듈이나 운영시스템에 저장하고, 물리적으로 안전한 환경에서 관리한다. 또한 신뢰할 수 있는 수탁 보관자를 이용함으로써 암호 키를 안전하게 보관 및 관리할 수 있다. 디바이스 내에 암호 키는 WBC(White Box Cryptography)[25]를 이용하여 암호 키가 소프트웨어로 구현된 암호 알고리즘 속에 섞여 있어서 암호 키를 쉽게 볼 수 없게 한다.
- 무선통신 단말 패치관리 및 무선통신 암호화(SR7) : 블루투스의 취약점을 이용한 블루본(BlueBorne) 공격은 기기간의 페어링도 필요하지 않고 악성코드를 설치할 필요가 없어서 쉽게 해킹을 당할 수 있다[26]. 이에 대응하는 방법은 인증된 페어링을 기반으로만 암호화통신을 해야 하고 지속적인 패치를 통하여 최신화된 모바일 OS의 보안패치를 최대한 빠르게 적용해야 한다. 와이파이 다이렉트의 경우 출처를 알 수 없는 와이파이 다이렉트에 대한 연결을 지양하고, WPA2(Wi-Fi Protected Access2) 수준의 암호화 연결을 해야 한다.

Table 5.는 제안 시스템에서 발생할 수 있는 보안 위협과 그에 대응하는 보안 요구사항을 1:1 또는 1:N으로 매핑한 표이다. 설계 당시에 국제 표준에 근거해 허점 없이 설계 한다면 제안 시스템에 대한 보안 위협들은 현저히 줄어들 것이다. 또한 제안 시스템은 근거리 무선 통신을 사용하기 때문에 악의적인 공격자가 주변에 있지 않는 이상 보안 위협에 노출될 가능성이 낮다. 하지만 위에서 언급한 보안 요구사항을 준수하고 국가 또는 보안 기관에서 지정한

Table 5. Mapping between security threats and security requirements

Security Threats	Security Requirements						
	SR1	SR2	SR3	SR4	SR5	SR6	SR7
ST1	O				O		
ST2		O					O
ST3			O				
ST4				O		O	
ST5					O		
ST6						O	
ST7							O

보안 규정을 잘 이행 해야만 예기치 못한 보안 위협에 대응할 수 있다.

V. 결 론

이 논문이 제안하는 감염병 예방 디지털 증명서 시스템은 무선 근거리 통신 기술과 분산원장기술에 기반을 두고 구축된 시스템으로, 상호연동이 가능한 증명서 서명용 공개키를 블록체인 저장하고 이를 쉽게 가져와 검증하는데 강점이 있다. 그리고 QR 코드 기반의 디지털 증명서 시스템의 보안 취약점을 해결하고, 국가 간 디지털 증명서 시스템의 상호 연동과 편리성을 동시에 충족한다. 다만, 이 논문의 감염병 예방 증명서 시스템이 포함하는 정보는 국가나 WHO가 요구하는 정해진 정보만을 기준으로 가정하여 제시되었으므로 분산ID의 가장 큰 장점으로 평가되는 이용자 선택에 대한 자기주권신원(Self sovereign identity)에 대한 부분은 향후 연구 과제에서 영지식 증명(Zero-knowledge proof)이나 사후 신원 바인딩(Late identity binding) 기법을 이용해 다루고자 한다.

이 논문은 보다 안전한 감염병 예방 디지털 증명서 시스템과 서비스 제공을 위하여 제안된 시스템이 가진 모든 취약점을 도출하고 해당 취약점을 해결할 수 있는 보안 요구사항을 제시하였다. 또한 본 시스템은 분산원장기술 기반의 분산ID를 이용한 이용자 편의성과 보안성을 모두 고려한 감염병 예방 디지털 증명서 시스템이다. 이는 WHO의 DDCC:VS, EU의 DCC, 그리고 한국의 쿠브 등 기존의 감염병 예방 디지털 시스템과 달리 블루투스나 와이파이 다이렉트를 이용한 무선 통신 기반의 증명서 제출 방식을 적용하고, 단 한 번의 증명서 제출을 통해 신원 인증을 비롯한 여러 증명서의 검증을 동시에 처리함으로써 보다 편리하고 안전한 증명서 사용을 가능하게 한다. 개인정보에 대한 보안 이슈는 국내에 비해 미국, 유럽, 캐나다 등 서구권 국가에서 보다 민감한 이슈로 다루어진다. 따라서 감염병 예방 디지털 증명서 시스템의 글로벌 상용화를 고려한다면, 민감 정보에 해당하는 개인의 특정 의료 정보를 검증하기 위한 신뢰 모델과 이 논문이 제시하는 분산ID 기반의 여러 국가 간 연동 가능한 시스템 구축이 필요할 것이다. 향후 본 시스템에 연동되는 다양한 증명서의 일괄 검토를 위한 시스템 구현과 실증에 대한 추가 연구가 진행될 것으로 기대한다.

References

[1] Aidan Findlater, Isaac I. Bogoch, "Human mobility and the global spread of infectious Ddseases: A focus on air travel", Trends in Parasitology, vol.34, Issue 9, pp 772-783, Sep. 2018

[2] Johns Hopkins Coronavirus Resource Center, "Johns hopkins COVID-19 Map", https://coronavirus.jhu.edu/map.html, Dec. 30. 2021

[3] Korea Internet & Security Agency, COVID-19 Vaccine Passport Global Status of Use, Privacy and Regulations, Monthly Privacy Report June 2021

[4] WHO, "who smart vaccination certificate", https://www.who.int/groups/smart-vaccination-certificate-working-group, Dec. 30. 2021

[5] "Fake Covid Vaccination Cards Are on the Rise in the U.S., Europe", The Wall Street Journal, Aug. 7. 2021 https://www.wsj.com/articles/fake-covid-vaccination-cards-are-on-the-rise-in-the-u-s-europe-11628341203?mod=searchresults_pos8&page=1

[6] Kim Jihoon et al., Framework for Identity Management Using Decentralized Identity - Part 1: Framework Architecture and Model, TTAK.KO-12.0359-Part1, Dec. 10. 2020

[7] Kiho Yeo, Keundug Park and Heung Youl Youm, "Proposal for a Custody and Federated Service Model for the Decentralized Identity", Journal of The Korea Institute of Information Security & Cryptology vol.30, no.1, pp.513-525, Feb. 2020

[8] GSMA Hompage, "W3C dectralised identity", https://www.gsma.com/identity/decentralised-identity, Nov. 2. 2021

[9] "Decentralized Identifiers (DIDs) v1.0

Core architecture, data model, and representations", W3C Proposed Recommendation 03 August 2021, W3C, Aug. 2021 https://www.w3.org/TR/2021/PR-did-core-20210803/#terminology

〔10〕 "Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web", W3C Recommendation 19 November 2019, W3C, Nov. 2019 https://www.w3.org/TR/vc-data-model

〔11〕 Kaliya Young et al., "The COVID-19 C redentials Initiative: Bringing emergi ng privacy-preserving technology to a public health crisis" Future of Privacy Forum, Oct. 2020 https://fpf.org/wp-content/uploads/20 20/10/10-CovidCredentials.pdf

〔12〕 Jung Woojin, "Coov Mobile Vaccination Certificate", Korea Disease Control and Prevention Agency, Aug. 11. 2021 https://www.itu.int/en/ITU-T/Worksh ops-and-Seminars/2021/0811/Documen ts/Woojin%20Jung_Presentation.pdf?cs f=1&e=7kSMqU

〔13〕 Rice, Evan S., The Wayfarer's Handbook: A Field Guide for the Independent Traveler, New York: Hachette Book Group. pp.256, Nov. 2020

〔14〕 "Digital Documentation of COVID-19 Certificates: Vaccination Status TECHNICAL SPECIFICATIONS AND IMPLEMENTATION GIDANCE - Web Annex B. Technical briefing", WHO, Aug. 2021

〔15〕 "Facilitation panel(FALP) Twelfth meeting - The visible digital seal for non-constrained environments for travel related public health proofs", FALP/12-WP/10, International Civil Aviation Organization(ICAO), June 2021 https://www.icao.int/Meetings/FALP/ Documents/FALP12-2021/WP/WP10/W P10_VDS.pdf

〔16〕 "eHealth Network Guidelines on Paper version of the EU Digital COVID Certificate, V1.0.2", European Commision, May. 2021 https://ec.europa.eu/health/sites/defa ult/files/ehealth/docs/covid-certificate_ paper_guidelines_en.pdf

〔17〕 "EU Digital COVID Certificate Factsh eet" Euroupean Commission, June 2021 https://ec.europa.eu/commission/press corner/detail/en/FS_21_2793

〔18〕 "Commission implementing decision- Laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council", Official Journal of the European Union, June 2021 https://eur-lex.europa.eu/legal-conten t/EN/TXT/HTML/?uri=CELEX:32021 D1073&from=EN

〔19〕 COVID-19 Vaccination : National Cen ter for Mental Health Hompage, "Coo v", Dec. 1. 2021 https://ncv.kdca.go.kr /coov

〔20〕 Korea Civil Aviation Association Airpo rtal, "covid-19 EU DCC global stadar d" https://www.airportal.go.kr/covid19 /covid19_view.jsp?seq=71387, Sep. 10. 2021

〔21〕 "ITU/WHO Workshop on Digital Vacci nation Certificate Summary and resul ts", ITU-T, Aug. 2021 https://www.it u.int/en/ITU-T/Workshops-and-Semin ars/2021/0811/Documents/Workshop% 20Outcomes.pdf

〔22〕 "Draft Report of the eighth TSAG meeting (virtual, 25-29 October 2021) TSAG TD 1020", ITU-T, Oct. 2021

https://www.itu.int/md/T17-TSAG-211025-TD-GEN-1020/en

〔23〕 Housley, R., Ashmore, S., Wallace, C., "Trust Anchor Format", RFC 5914, June 2010

〔24〕 Kiho Yeo, Keundug Park and Heung Youl Youm, "Proposal for a custody and federated service model for the decentralized identiyt", Journal of The Korea Institute of Information Security & Cryptology vol.30, no.3, June. 2020

〔25〕 Shin Hyo Kim, Yun-kyung Lee and Byung Ho Chung, "Analysis on Trends for White-Box Cryptography and Its Application Technology", Electronics and Telecommunications Trends, 25(5) May, 2010

〔26〕 Ben Seri and Gregory Vishnepolsky, " BlueBorne Technical White Paper" Armis , Nov. 2017

〈저자소개〉

박 성 채 (Sung-chae Park) 종신회원
2008년 2월: 순천향대학교 정보보호학과 학사
2020년 2월~현재: (주)보다비 AI연구소
2021년 3월~현재: 순천향대학교 정보보호학과 석박사과정
〈관심분야〉 분산원장기술 보안, AI 보안, 정보보호관리체계, 개인정보보호

이 주 현 (Ju hyun Lee) 학생회원
2022년 2월 : 순천향대학교 정보보호학과 학사
〈관심분야〉 분산원장기술 보안, IoT 보안, 네트워크 보안, OT 보안

박 근 덕 (Keundug Park) 종신회원
1992년 2월: 동아대학교 전산공학과 학사
2015년 8월: 순천향대학교 대학원 정보보호학과 석사
2018년 2월: 순천향대학교 대학원 정보보호학과 박사
2018년 9월~현재: 서울외국어대학원대학교 국제교양학과 교수
2018년 3월~현재: 서울외국어대학원대학교 AI블록체인연구소 소장
2020년 9월~현재: 분산신원증명(DID) 기술 및 표준화 포럼 정책분과 위원장
2018년 9월~현재: TTA PG502 특별위원, PG1006 특별위원/간사
2018년 6월~현재: ISO/IEC JTC 1/SC 27 전문위원/WG5그룹장
2017년 8월~현재: ISO/TC 307 전문위원
2017년 8월~현재: ITU-T JCA-IdM 공동의장
2017년 2월~현재: ITU-T SG17 위원/간사, Q10 부의장
2012년 2월~현재: 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 심사원
〈관심분야〉 분산원장기술 보안, 탈중앙화 신원 관리, 탈중앙화 금융 보안, 정보보호관리체계, 개인정보보호, 클라우드 보안

염 흥 열 (Heung Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 학사
1983년 9월: 한양대학교 대학원 전자공학과 석사
1990년 2월: 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월: 한국전자통신연구원 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월: 한국정보보호학회 회장(역), 명예회장(현재)
2007년 3월~현재: 한국인터넷진흥원 ISMS/PIMS 인증위원회 위원장
2009년~2016년: ITU-T SG17 부의장, ITU-T SG17 WP2/WP3 의장
2017년~현재: ITU-T SG17 의장
2020년 8월~현재: 분산신원증명기술·표준화포럼 의장
〈관심분야〉 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜, 5G 보안, 분산원장기술 보안