Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.5, Oct. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.5.959

단거리 무선 통신을 이용한 개인 간 분산 신원증명 시스템 제안*

여 기 호,[1†] 박 근 덕,[2] 염 흥 열[3‡]
[1,3]순천향대학교 (대학원생, 교수), [2]서울외국어대학원대학교 (교수)

Proposal for a Peer Decentralized Identity System Using Short-Range Wireless Communications*

Kiho Yeo,[1†] Keundug Park,[2] Heung Youl Youm[3‡]
[1,3]Soonchunhyang University (Graduate student, Professor),
[2]Seoul University of Foreign Studies (Professor)

요 약

분산 신원증명은 정보주체가 자신의 신원정보를 직접 관리하고, 필요시 제공한다는 자기주권 신원증명의 개념을 기반으로 하고 있다. 하지만, 발급기관으로부터 신원정보를 발급받아 온다는 절차가 필요하고, 발급기관의 관리 소홀로 인한 대량의 정보 유출 우려가 존재한다. 본 논문에서는 정보주체와 발급기관을 일치시켜 1:1 또는 1:N 소규모 그룹에서 참여자들만 신원증명이 가능한 Peer DID 기술을 기반으로 개인 간 분산 신원증명 시스템을 제안한다. 블루투스와 같은 단거리 무선 통신을 이용하여 모바일 디바이스로 직접 연결하고, 정보주체가 직접 자신의 정보를 생성하여 상대방에게 제공하므로 정보의 자기주권을 실현한다. 제안 시스템을 통하여 신원증명 절차를 간소화하고, 보안 및 프라이버시를 개선할 수 있으며, 비용도 절감할 수 있다. 나아가 제안 시스템과 분산 원장을 연결하여 다른 도메인의 이용자와 상호 신원증명 할 수 있도록 확장된 구성도 가능하다. 향후에는 다양한 기술을 기반으로 사람과 사물, 사물과 사물 인증에도 활용할 수 있는 신원증명 시스템에 대한 확장 연구가 필요하다.

ABSTRACT

Decentralized Identity is based on the concept of self-sovereign identity, in which holders manage and provide their own credentials. However, a procedure is required to obtain credentials from issuers, and there is a risk of mess personal information leaking due to negligence of the issuers. In this paper, we propose a peer decentralized identity system based on Peer DID technology that allows only participants to verify their identity in 1:1 or 1:N small groups by matching the holder with the issuer. It is directly connected to a mobile device using short-range wireless communications such as bluetooth, and the holders create and provide their own credentials in person to the other party, thus fully realizing the self-sovereignty identity. The proposed system can simplify the identification process, improve security and privacy, and reduce costs. Furthermore, an extended architecture is possible to connect the proposed system and the distributed ledger to identify users in other domains. In the future, based on various technologies, it is also necessary to expand research on identity systems that can be utilized for human-to-thing and things-to-things authentication.

Keywords: Self-sovereign Identity, Decentralized Identity, Peer DID, Short-range wireless, WPAN

Received(06. 29. 2021), Modified(09. 17. 2021), Accepted(09. 17. 2021)

* 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2021-0-00112, 차세대보안 표준전문연구실)

† 주저자, symbol.yeo@hyundai-autoever.com
‡ 교신저자, hyyoum@sch.ac.kr(Corresponding author)

I. 서 론

현대 사회에서 다양한 오프라인 서비스를 제공받기 위해서는 지갑에 있는 신분증을 제시해야 하는 사례가 빈번하다. 공공기관에서 증명서를 발급받거나 은행 계좌를 개설할 때, 본인을 인증하기 위해 신분증을 제시하기도 하고, 편의점에서 술이나 담배를 구입할 때도 일정 연령을 넘겼다는 것을 증명하기 위해서 신분증을 제시하는 등, 신원증명 또는 자격증명을 위해 법적으로 유효한 신분증을 제시한다. 여기서 법적으로 인정받는 신분증은 주민등록증, 운전면허증, 여권, 외국인등록증으로 각각 개인을 고유하게 구별하기 위해 부여된 고유 식별 정보, 즉 ①주민등록법 제7조의2제1항에 따른 주민등록번호, ②여권법 제7조제1항제1호에 따른 여권번호, ③도로교통법 제80조에 따른 운전면허의 면허번호, ④출입국관리법 제31조제5항에 따른 외국인등록번호[1] 외에도 추가적인 개인정보를 포함하고 있다.

디지털 사회로 전환되면서 온라인 서비스를 제공받기 위해 가장 널리 오랫동안 신분증 역할을 해온 것이 공인인증서였다. 하지만, 2020년 12월 독점적 지위를 상실하면서 FIDO, PKI, 블록체인 등 다양한 기술이 적용된 사설인증 시장이 활성화되고 있다[2]. 실제로 2019년에 공인인증서 발급이 4,203만 건, 신기술이 적용된 사설인증서가 3,706건인데 반해, 2020년 11월말에는 각각 4,676건, 6,646건으로 신기술이 적용된 사설 인증서 사용이 급격히 증가하게 되었다[3]. 이런 현상은 전자서명법 전부 개정이라는 제도적 변화와 함께 COVID-19 팬데믹(pandemic) 현상으로 인한 비대면 인증 요구의 증가를 주요 원인으로 꼽을 수 있다.

국내의 경우 정부의 방역대책 준수와 사회적 거리두기를 유지하면서 현장에서 소비를 통한 서비스를 제공받기 위해서는 방문자의 체온을 측정하고, 수기로 출입명부를 작성하거나 각 개인이 타 기관으로부터 인증 받아 생성한 QR코드를 제시해야만 한다. 이때 감염병예방법 제49조[4]에 따라 감염병 예방 및 전파 차단을 위한 출입명부 목적으로 성명, 휴대전화번호, 식별정보, QR코드정보, QR생성시각, 개인안심번호 등이 수집된다[5]. 여기서 두 가지 방식은 단순히 수기식, 전자식이라는 차이 뿐 아니라, 본인이 스스로 개인정보를 기재한 것과 타 기관에서 인증을 받아 그 정보를 제공하도록 특정 코드를 제출하는 차이점이 있다. 또한, 두 가지 방식의 공통점은 정보 주체가 개인정보의 목적에 따른 이용 및 제공하는데 대한 통제권을 가진다는 자기주권 신원증명(SSI : Self-Sovereign Identity) 개념을 기반으로 한다는 것이다.

이러한 자기주권 신원증명 개념을 적용하여 디지털 환경에서 구현한 가장 대표적인 것이 분산원장 기술을 이용하는 분산 신원증명(DID : Decentralized IDentity) 기술이다. 분산 신원증명 기술은 비대면 환경에서 정보주체가 개인정보를 직접 관리하면서 본인의 신분증명을 제공할 수 있는 디지털 사회의 맞춤형 기술로 조명을 받고 있다[6]. 하지만, 앞서 언급한 것과 같이 일상생활에서는 간편하고 빠르게 소규모 구성원들 사이에서만 인증이 필요한 경우가 더 빈번하게 발생한다. 이런 경우, 굳이 분산원장을 이용하지 않더라도 소규모 당사자들만 참여하여 Peer DID라는 기술을 통해 신원증명을 할 수도 있다.

본 연구에서는 이런 Peer DID 기술을 실제 서비스로 구현 가능한 개인 간 분산 신원증명 시스템을 제안하고자 한다. 분산 신원증명 모델의 소유자(holder)와 발급기관(issuer)을 일치시켜 자기주권 신원증명의 완성도를 높인 새로운 시스템에 대한 구성, 활용사례, 특징비교, 보안 위협 및 요구사항을 분석하였다.

본 논문 제2장에서는 분산 신원증명 기술과 Peer DID 기술에 대해 먼저 알아보고, 제3장에서는 제안하고자 하는 개인 간 분산 신원증명 시스템에 대한 설명과 다른 시스템과의 비교, 활용 사례 등을 설명한다. 제4장에서는 제안 시스템에서 식별할 수 있는 보안 위협을 분석하고, 대응하기 위한 보안 요구사항을 제시한 뒤, 제5장에서는 결론 및 추가 연구 방향에 대해 살펴보고자 한다.

II. 관련 기술

2.1 분산 신원증명 기술

2.1.1 분산 신원증명 데이터 모델

분산 신원증명은 디지털 환경에서 분산원장을 기반으로 정보주체가 스스로 신원에 대한 증명 관리와 신원정보 제출 범위 및 제출 대상을 통제하는 탈중앙화된 디지털 신원증명 체계로, 흔히 분산 ID 또는 DID로도 잘 알려져 있다[7],[8].

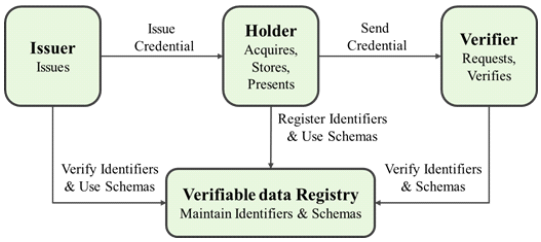

Fig. 1. Basic DID Model of W3C [9]

기본적인 분산 신원증명 모델에 대해서는 웹 기반 기술표준화 기구인 W3C(World Wide Web Consortium)의 표준 문서에서 발급기관(issuer), 소유자(holder), 검증기관(verifier), 신뢰 저장소(verifiable data registry)라는 4개의 구성요소와 그 관계에 대해 잘 설명되어 있다[9].

Fig.1.에 나타난 구성 요소들 사이에서 신원정보의 흐름은 다음과 같다. 정보주체가 본인의 정보를 보관, 관리하고 있는 발급기관으로 신원정보를 요청하면, 발급기관은 인증을 거쳐 요청받은 신원정보를 제공한다. 정보주체는 본인의 신원정보를 자신의 단말기에 저장하고 있다가 서비스를 제공받기 위해 신원정보의 전체 또는 일부를 선별적으로 검증기관으로 보낼 수 있다. 해당 정보를 수신한 검증기관은 검증 데이터 저장소를 통해 발급기관이 해당 정보를 발급했다는 사실을 검증하고 서비스를 제공하게 된다.

2.1.2 분산식별자

W3C에서는 DID라는 용어를 분산식별자(Decentralized Identifier)로 정의되어 있다. 분산식별자는 각 객체를 식별하는 용도 외에도 인증 수단에 사용되는 정보를 포함하는 DID 문서(DID document)를 참조하는 URI(Uniform Resource Identifier) 역할도 한다[10].

Fig.2.는 분산식별자의 간단한 예를 보여준다. 분산식별자는 schema, method, MSI(Method-Specific Identifier) 3부분으로 구성되는 간단한 문자열이다.

- DID schema : URI를 통해 자원에 접근하는 프로토콜
- DID method : DID 문서가 저장된 저장소
- DID Method-specific identifier : DID 문서가 저장된 정확한 위치를 검색하기 위한 정보

Fig. 2. simple example of a Decentralized Identifier (DID) [11]

DID 문서에는 분산식별자와 분산식별자의 소유를 인증하기 위한 공개키와 인증대상, 인증권한 소유자, 인증방식, 서비스를 위한 엔드포인트(endpoint) 정보 등이 포함되어 있다. W3C의 분산식별자에 관한 표준문서에는 Table 1.과 같이 DID 문서의 핵심 속성값 10개가 기재되어 있고, 각 속성마다 다시 여러 세부항목을 통해 분산식별자와 관련된 상세정보를 포함하고 있다[11].

W3C에서 정의하는 분산식별자와 DID 문서로 구성 요소들 간 인증과 데이터 전송 흐름은 다음과 같다. 분산 신원증명 기술이 적용된 기본 모델에서는 구성 요소들 간에 어떤 통신이 이루어지기 전에 분산식별자와 DID 문서를 생성하여 분산식별자의 DID method에 정의된 저장소에 DID 문서를 등록해 놓는다. 그리고 발급기관은 소유자가 신원정보를 요청하게 되면 가장 먼저 DID auth라는 분산식별자 소유 인증을 하게 되고, 인증이 성공하면 요청한 신원정보(verifiable credential)를 제공하게 된다. 서비스를 제공받기 위해서도 가장 먼저 DID auth라는 분산식별자 소유 인증 과정을 거쳐 검증기관이 먼저 서비스에 필요한 신원정보 항목을 요청하면, 소유자가 보관하고 있던 신원정보(verifiable

Table 1. Core Properties of DID document [11]

Group	Property	Required
Identifiers	id	yes
	alsoKnownAs	no
	controller	no
Verification Methods	verificationMethod	no
Verification Relationships	authentication	no
	assertionMethod	no
	keyAgreement	no
	capabilityInvocation	no
	capabilityDelegation	no
Services	service	no

credential) 중에 해당 서비스에 필요한 항목(verifiable presentation)을 제출한다. 여기서도 검증기관이 분산식별자에 포함된 DID Method에 정의된 저장소, 즉 검증 데이터 저장소에 있는 DID 문서를 통해 발급기관에 의해 발급된 신원정보임을 검증하고, 성공하면 서비스를 제공하게 된다[10].

2.1.3 분산 신원증명 모델의 완성

W3C의 분산 신원증명 모델에서는 정보주체가 자기 정보에 대한 통제권을 가지고 있어 자기주권 신원증명이 적용된 것으로 간주한다. 하지만, 현재까지 나와 있는 대부분의 분산 신원증명 모델이 적용된 서비스를 보면, 아직까지 정보주체의 신원정보가 발급기관에 존재하는 것이 사실이다. 이런 경우에는 분산 신원증명 모델의 3개 구성 요소가 각각 분리되어 정보주체가 자신의 정보를 직접 생성하는 것이 아니라, 각종 기관 및 조직(공공기관, 교육기관, 의료기관이나 회사 등)으로부터 발급받아 필요한 곳에 제출하는 형태의 서비스 모델이다. 다른 관점으로 말하자면, 정보주체가 서비스를 제공받기 위해 검증기관에 제출하는 본인의 신원정보가 신뢰성이 있어야하고, 그러기 위해서는 신뢰할 수 있는 발급기관으로부터 신원정보를 발급받아야 한다는 생각이 반영되었다[12]. 최근 많은 주목을 받고 있는 백신여권[13]이나 모바일 운전면허증[14]과 같이 국가(정부기관)로부터 자격을 인정받거나 대학으로부터 졸업증명서를 발급받고, 회사로부터 재직증명서를 발급받는 형태가 대표적인 사례이다.

자기주권 신원증명의 개념을 보다 충실하게 적용하기 위해서는 발급기관에 보관되어 있는 정보를 받아오는 것뿐만 아니라, 본인 스스로 생성한 정보를 신원증명이 필요한 대상에게 제출하는 경우도 고려되어야 할 것이다. 즉, 발급기관(issuer)과 소유자(holder)가 동일한 경우도 충족해야 진정한 자기주권 신원증명이 구현된 것이라 볼 수 있다.

2.2 Peer DID 기술

실제로 일상생활에서는 1:1 또는 1:N의 소규모 그룹에서 신원인증 사례가 더 빈번하게 발생한다. 이런 경우에는 Fig.3.에서 보듯이 검증 데이터 저장소가 반드시 블록체인과 같은 분산원장일 필요는 없다.

이때, 1:1과 같이 정해진 대상과 신원증명에 사용

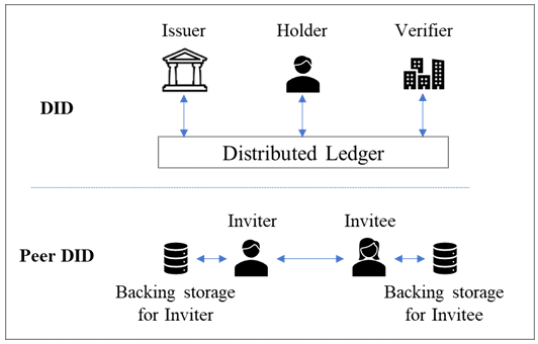

Fig. 3. A comparison of DID and Peer DID

되는 DID는 Pairwise DID라고 하고, 1:N 또는 N:N과 같이 N명의 대상들 간에 사용되는 DID는 N-wise DID, 알 수 없는 숫자의 대상들 사이에 사용되는 DID를 Anywise DID라고 한다[15]. 여기서 Anywise DID가 앞서 얘기한 분산원장을 사용하여 누구나 접근 가능한 검증 데이터 저장소로 활용하는 경우에 해당한다.

Fig.4.에서 보듯이 Peer DID는 크게 method prefix와 MSI(Method-Specific Identifier)로 구성된다. MSI는 다시 numalgo, transform, encnumbasis로 구성되고, encnumbasis는 numeric basis와 multicodec로부터 생성이 된다.

- method prefix : URI가 자원에 접근하기 위해 사용하는 프로토콜 (분산식별자의 DID schema과 동일한 역할)
- numalgo : numeric basis를 생성하는 방법으로 0,1,2 의 고정된 값으로 표시
- transform : 고정된 값, 'z' 이후의 데이터가 인코딩된 방식.
- encnumbasis : numeric basis를 base58btc 방식으로 인코딩한 값

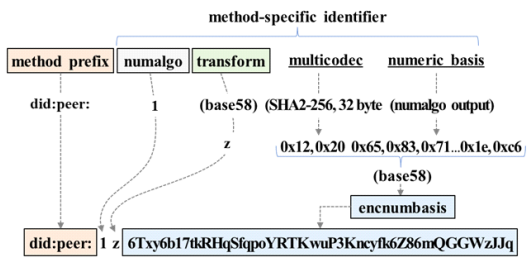

Fig. 4. Composition of a peer DID value [15]

여기서 numalgo 값이 '1'이면, multicodec은 0x12 0x20 바이트가 되고, 그 뒤에 오는 문자열은 32바이트 크기의 SHA2-256 해시 값이라는 것을 의미한다. 이때, 공개키를 이용하여 만들고, Peer DID가 포함되지 않은, JSON 형식의 Peer DID 문서 최초 버전(genesis version)을 Stored variant라고 하는데, 이 값을 SHA2-256으로 해시한 값에 multicodec 값을 앞에 붙여주면 numeric basis가 생성된다. W3C의 Peer DID에 관련된 표준문서에는 이러한 알고리즘을 통해 Peer DID가 생성되어야 한다는 것을 명시하고 있다[15].

Table 2.와 같이 DID의 소유권을 증명할 수 있는 인증수단을 포함하는 Peer DID 문서는 크게 4가지 속성을 가지고, 각 속성이 앞서 2.1.2에서 설명한 DID 문서에 있는 속성과 유사하다.

참여자(Inviter, Invitee)와 Peer DID, Peer DID 문서들 간의 관계와 신원증명 흐름의 개요는 Fig.5.에 잘 나타나 있다.

Peer DID를 적용한 신원증명을 위해서는 먼저 참여자들의 Peer DID와 Peer DID 문서를 안전하게 생성하고 교환해야 해야 한다. Peer DID 정보를 교환하는 방법은 다양하지만, 여기서는 Hyperledger Aries에서 정의한 DID Exchange Protocol 1.0을 기준으로 설명한다[17]. DID Exchange Protocol을 적용하면 Invitation, Exchange request, Exchange response라는 3종류의 메시지 교환을 통해 Peer DID 정보를 교환한다. 메시지 교환 과정은 Fig.6.에 잘 나타나 있다.

① Invitee가 Peer DID를 교환할 대상에게 Request invitation을 전송

Table 2. Properties of Peer DID document [15]

Property	sub-value
verificationMethod	*sub-value : id, type, controller, publicKey
authentication	- includes keys that only references are allowed
authorization	- governs how DID docs are updated and DIDComm trust flows *sub-value : profiles, rules
service	- includes serviceEndpoint *sub-value : id, type, serviceEndpoint

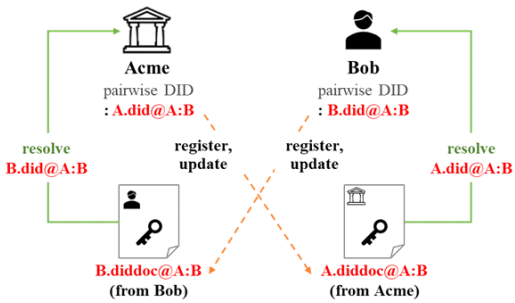

Fig. 5. Identity Flow using Peer DID [16]

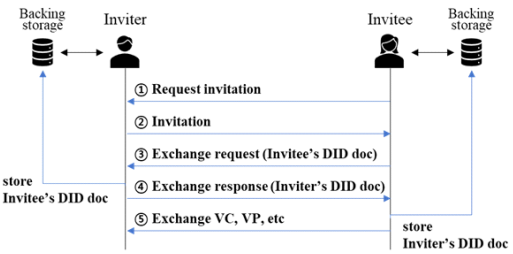

Fig. 6. Exchange process of Peer DID & Peer DID document [10]

② Inviter는 DID Exchange Protocol에 정의된 양식에 따라 메시지의 타입, 메시지 id, 메시지, 메시지 수신자, 이후 Exchange 메시지를 암호화할 키가 포함된 Invitation 메시지를 Invitee에게 전송.

③ Invitee는 Invitation 메시지에 있던 상대방의 암호키로 자신의 Peer DID와 Peer DID 문서정보를 Exchange 메시지에 넣고, 암호화하여 Inviter에게 전송

④ Inviter는 자신의 Backing storage에 Invitee의 Peer DID 문서를 저장. 자신의 Peer DID 문서를 Exchange response에 넣고, Invitee가 보내온 Peer DID 문서에 포함된 공개키로 암호화하여 전송

⑤ Invitee도 자신의 Backing storage에 Inviter의 Peer DID 문서를 저장. Peer DID 문서를 상호 교환한 참여자들은 이후부터 Peer DID로 서로 식별하면서 신원정보 교환 가능

III. 단거리 무선 통신을 이용한 개인 간 분산 신원증명 시스템 제안

3.1 제안 시스템 구성

본 논문에서 제안하는 시스템은 분산 신원증명을 기반으로 1:1 또는 1:N의 소규모 그룹 내에서 참여자들 간 신원증명을 위해 Peer DID 개념을 차용한다. WPAN(Wireless Personal Area Network) 환경에서 참여자들 간 DID 정보를 교환하기 위해서는 블루투스(bluetooth)와 와이파이 다이렉트(WiFi Direct) 같이 디바이스 간 직접 연결하는 단거리 무선 통신을 이용하고, 오프체인(off-chain)이나 온체인(on-chain)에 접속하기 위해서는 와이파이(WiFi)나 LTE 통신을 이용한다. 장소에 관계없이 쉽게 휴대 가능한 모바일 디바이스를 이용하므로 모바일 폰, 패드, 워치 등에서 사용하기 적합하다. Fig.7.은 제안하는 시스템의 전체적인 구성을 나타낸다.

- 신원증명서 관리 모듈(Identity Certificate Management Module) : 대상 참여자들 간 상호 신원증명을 위한 전자서명된 신원증명서를 보관 및 관리. 본 논문에서 신원증명서(Certificate)는 이용자의 개인정보를 개인키로 전자서명한 증명서를 의미
- 개인정보 관리 모듈(PII Management Module) : 모바일 디바이스의 소유자가 정보주체로서 직접 자신의 신원정보를 입력하고 개인정보는 암호키 관리 모듈에서 받은 암호키로 암호화 저장하여 관리
- 암호키 관리 모듈(CryptoKey Management Module) : 전자서명을 위한 공개키 쌍을 생성하고, 자신이 생성한 개인정보를 암호화하는 키를 생성하고 관리
- 무선 통신 모듈(Wireless Communication Module) : 신원증명을 위해 다른 참여자들과 신원증명서를 주고받기 위한 단거리 통신 모듈. 모바일 디바이스 간 직접 연결이 가능한 블루투스나 와이파이 다이렉트 등을 이용
- 오프체인(off-chain) : 신원증명을 위해 제안 시스템의 이용자들만이 접근 가능한 저장소. 개인정보 없이 이용자 식별자, 모바일 디바이스 식별자, 이용자의 공개키 등의 정보를 보관
- 온체인(on-chain) : 제안 시스템이 다양한 도메인에 적용되어 도메인 간 신원증명이 필요한 경우 확장 및 연계를 위한 신뢰 저장소.

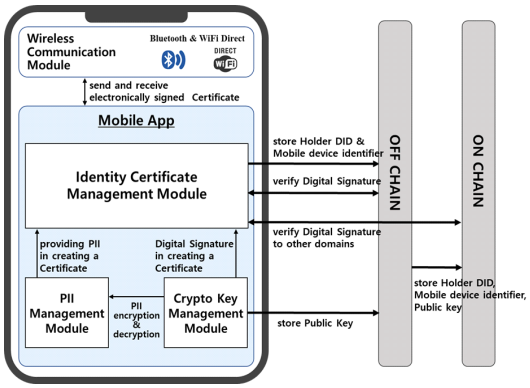

Fig. 7. Overview of proposed system

최근에 출시되는 거의 모든 모바일 디바이스에는 단거리 무선 통신 모듈이 탑재되어 있다. 신원증명서 및 개인정보, 암호키를 관리할 수 있는 모바일 앱을 구현하고, 오프체인은 모바일 앱 서버의 저장소로 구축한다. 즉, 오프체인은 해당 앱을 다운로드 및 설치하여 사용하는 참여자들만이 함께 사용하는 데이터베이스 저장소가 되고, 온체인은 누구나 접속 가능한 퍼블릭 분산원장을 활용할 수 있다.

3.2 제안 시스템 동작 원리

제안하는 시스템을 이용하여 1:1 또는 1:N의 소규모 그룹의 구성원들 간 필요한 목적에 따라 신원증명을 위해서 우선 개인 간 상호 인증을 통해 전자서명된 신원증명서를 교환하는 기능을 제공한다. 먼저, Fig.8.에서는 단거리 무선 통신을 통한 이용자들 간 상호 인증하는 기능에 대해 설명한다.

여기서 제안 시스템은 이용자들의 디바이스 간 직접 연결이 가능해야 하므로 Broadcast 연결이 가능한 블루투스 LE(Low Energy)를 기준으로 설명한다. 우선 디바이스 간 통신이 연결되기 전에 각 이용자들은 Peer DID와 공개키를 포함한 Peer DID 문서를 오프체인에 저장한다. 이용자의 모바일 디바이스는 블루투스 통신을 통해 페어링(pairing) 될 때 서로 블루투스 주소(BD_ADDR), 이름(name), 프로파일(profiles)을 교환하고 저장한다. 페어링은 이용자가 원하는 장치만 연결이 될 수 있도록 인증 PIN 코드를 요구하거나 자동 인증 처리가 가능하고, 페어링이 되면 디바이스 간 연결된 통신 암호키

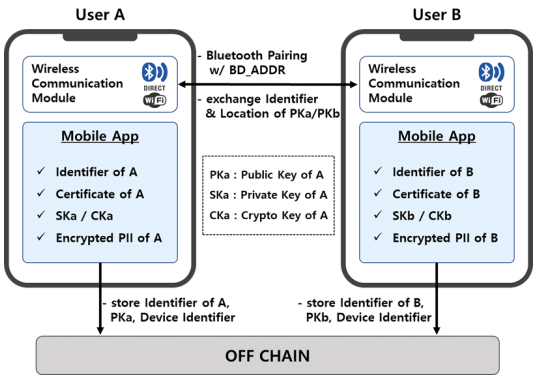

Fig. 8. Authentication between Individuals

를 생성한다[18]. 사실 페어링 과정에서 이미 디바이스 간 인증을 완료하고 암호키를 교환한 후, 본딩(bonding) 상태에서 이용자의 Peer DID와 Peer DID 문서에 접근할 수 있는 위치(location) 정보를 상호 교환하야 개인 간 인증 과정은 완료된다.

이러한 페어링 과정에서는 DID Exchange Protocol과 유사한 방식으로 이용자들의 디바이스 간에 페어링 요청 메시지(pairing request message)와 페어링 응답 메시지(pairing response message)를 주고받게 된다. 또한, 블루투스 2.1부터 적용된 SSP(Secure Simple Pairing) 기능을 통해 통신 연결을 암호화하는 키를 생성하기 전, 각 디바이스에서 ECDH(Elliptic Curve Diffie-Hellman) 공개키 쌍을 생성하여 키 교환 및 난수 생성 과정을 통해 인증 단계에서 보안성이 강화되었다[19].

개인 간 상호 인증이 완료되면, 이용자들은 신원증명 과정을 거치게 된다. Fig.9.을 보면, 이용자들은 정보주체로서 자신의 정보를 직접 입력하여, 제안 시스템을 사용하는 각자의 목적에 따라 필요한 증명서(Ⅰ,Ⅱ,Ⅲ,Ⅳ,Ⅴ)를 미리 생성해 놓는다. 그리고 상황에 따라 필요한 증명서를 선택하여 자신의 개인키로 전자서명을 하여 상호 교환하고, 사전에 오프체인에 저장되어 있는 상대방의 Peer DID 문서로 접속하여 상대방의 공개키를 이용해 해당 증명서를 검증하게 된다. 이러한 동작 원리는 1:1 인증이든 1:N 인증이든 동일하게 적용되지만, 1:N의 경우 1차적으로 상호 간 인증 이후에 필요한 추가적인 증명서를 발급할 수 있다. 그 부분은 다음에 나오는 활용사례를 통해 설명한다.

3.3 제안 시스템 활용 사례

제안 시스템에서 디바이스 간 서비스 가능한 거리는 모바일 디바이스에 탑재된 블루투스 모듈의 전파 강도에 따라 결정된다[20]. 클래스(class) 1이 적용된 디바이스로는 전파가 100미터까지 전달되지만, 전력소모가 심한 단점이 있다. 전파 도달 거리가 1미터도 되지 않는 클래스 3,4는 제외하고, 저전력으로 10미터까지 전파가 전달되는 클래스 2가 가장 많은 제품에 적용되어 있다. 블루투스 4.2에 비해 전송속도는 2배, 도달거리는 4배 늘어난 블루투스 5가 적용된 모바일 디바이스라면 40미터 정도 범위 내에서는 충분히 서비스가 가능하다. 여기서는 근거리에서 제안 시스템을 이용하여 신원증명을 하는 실제 적용 가능한 사례를 알아본다.

Fig.10.에서 이용자들은 제안 시스템의 모바일 앱에서 생성 가능한 증명서 중에 디지털 명함을 선택하여 전달하고자 하는 자신의 정보를 미리 입력하고,

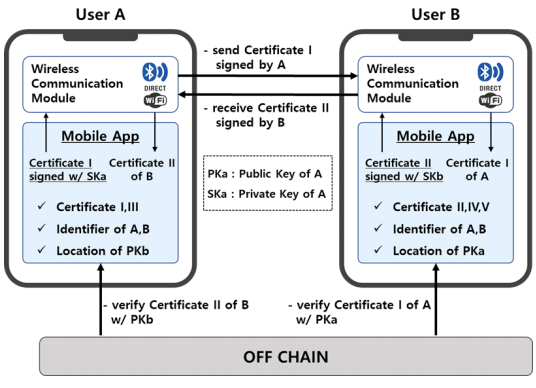

Fig. 9. Exchange & verify each Certificate

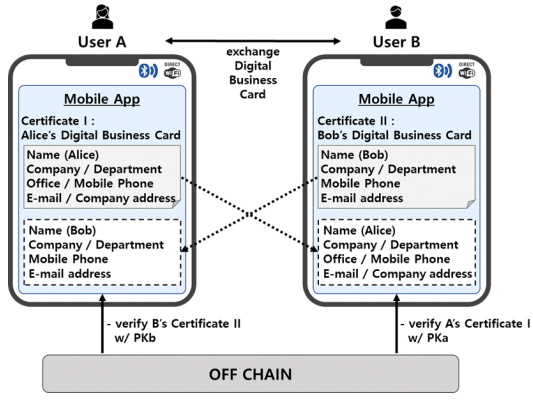

Fig. 10. Use case of Digital business card

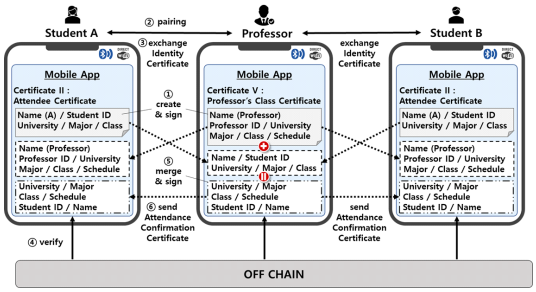

Fig. 11. Use case for issuing an attendance certificate

개인키로 전자서명을 해 놓는다. 모바일 디바이스를 인식할 수 있는 범위 내에서 단거리 무선 통신을 이용하여 디바이스를 직접 연결하여 상호간 디지털 명함을 교환하고 상대방의 공개키로 검증한다.

디지털 명함과 같은 1:1 신원증명을 하는 사례는 미리 생성해 놓은 증명서를 교환하는 경우이고, 해당 신원증명 과정 이후에 참여자들 간에 필요한 추가적인 증명서를 생성하여 교환하는 경우도 있다. Fig.11.은 대학 강의실에서 교수와 학생들 간 1차적으로 신원증명 후, 2차적으로 출석 증명서까지 발급 및 교환하는 1:N의 경우를 설명한다.

우선 디바이스 연결 전에 ①교수는 자신의 정보와 강의 정보를 포함한 강의 증명서를, 학생은 자신의 정보를 포함한 학생 증명서를 사전에 생성하고, 각자의 개인키로 전자서명을 해 놓는다. ②강의 당일 참석한 교수와 학생들은 서로 블루투스를 통해 디바이스 연결 후, ③강의 증명서와 학생 증명서를 교환하고 ④각각 상대방의 공개키로 이를 검증한다. 이로써 출석 확인을 위한 상호간 신원증명은 완료되었고, 출석 확인 이후 또는 강의가 종료되는 시점에 ⑤교수는 자신이 생성한 강의 증명서와 학생으로부터 받은 학생 증명서를 조합하여 출석 확인 증명서를 발급하고 전자서명 한 후에, ⑥학생들에게 다시 전송하여 2차 신뢰 증명서를 제공할 수 있다. 학생들은 수신한 출석 확인 증명서에 전자서명하여 목적에 맞는 증명서를 보관한다.

Fig.12.는 교수가 발급하는 출석 확인 증명서의 데이터 항목 및 구조를 예시로 나타낸 것이다. 출석 확인 증명서는 학생이 제출한 학생 증명서와 교수 자신이 발급한 강의 증명서에서 필요한 항목을 추출하여 교수의 서명 정보와 함께 학생에게 전달하는 일종의 VP(Verifiable Presentation)[9]이다.

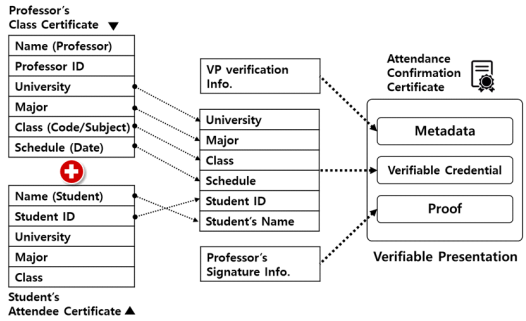

Fig. 12. Sample of attendance certificate

3.4 제안 시스템 확장 및 연계

제안 시스템이 각각 다른 도메인에 적용되어 도메인을 넘어서 사용자간 상호 신원증명이 필요한 경우가 발생할 수 있다. 이런 경우에는 모든 도메인에서 접근 가능한 온체인이 가교 역할을 하게 된다.

Fig.13.에 나타난 것과 같이 도메인 A, B에서 각각 오프체인 A, B를 통해 신원증명을 하던 사용들이 다른 도메인에 있는 사용자와 신원증명을 하게 되는 경우, 각 도메인의 오프체인에 보관하고 있던, 사용자들의 분산식별자와 그 소유를 인증할 수 있는 공개키를 온체인으로 보낸다. 그리고 오프체인은 해당 정보를 저장한 위치를 사용자들에게 공유하여 다른 도메인 사용자의 증명서를 받아 검증할 수 있게 된다. 이렇게 함으로써 제안 시스템을 적용할 수 있는 범위를 확장하고 각자 필요에 의해 다른 도메인에 제안 시스템을 구축하게 되더라도 도메인 간 신원증명 연계가 가능하게 된다.

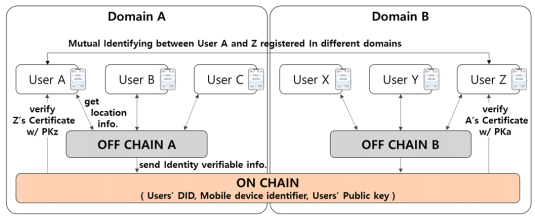

Fig. 13. Extending the proposal system over domains

3.5 다른 신원증명 시스템과 비교

제안 시스템을 구현하여 사용하게 되면, 분산 신원증명(DID)이나 공동인증서와 같이 유사한 기술을

이용하는 다른 신원증명 시스템에 비해 다음과 같은 장점이 있다.

- 간편한 신원증명 절차 : 제안 시스템에서는 발급기관(issuer)과 소유자(holder)가 분리되지 않고 일치한다. 정보주체는 발급기관(issuer)으로부터 신원정보를 요청하거나, 인증기관으로부터 인증서 발급받는 절차가 필요하지 않다. 또한 원거리 통신을 통해 데이터를 주고받기 위해 매번 인증을 거칠 필요 없이 근거리에서 빠른 무선 연결을 통해 디바이스를 인증하므로 전체적인 신원증명 절차가 간소화된다.
- 보안 및 프라이버시 개선 : 신원증명이 필요한 당사자들만 DID 관련 데이터에 접근할 수 있고, 또 단거리 통신 범위 내 현장에서만 데이터 교환이 발생하기 때문에 정보 유출에 대한 가능성이 현저하게 낮아진다. 또한 통신 세션마다 매번 다른 Peer DID를 사용할 수 있어 프라이버시가 보장된다[10].
- 비용 절감 : 인증서 발급을 위해 필요한 시스템을 별도 구축할 필요가 없어 비용이 절감된다. 또한, 신원증명이 필요한 소수의 이용자들만 이용하므로 분산원장을 사용할 필요가 없어 트랜잭션 비용이 없다[10]. (온체인을 이용한 도메인 간 연계 및 확장 시에는 비용 발생)

Table 3. Comparison of proposed system with other Identity systems

Category	Proposed system	DID	Joint PKI Certificate[21]
Issuer	User	Institution or Company	Certificate Authority
Network	WPAN (bluetooth, WiFi direct)	LAN, WAN (Internet)	WAN (Internet)
Certificate Storage	Mobile Device only	Mobile Device	Mobile Device, PC, USB, Token
Organization	N/A	Alliance : Initial, MyID, DID, Mykeepin	KISA
Business Body	N/A	SK Telecom, Raon Secure, ICON loop, Coinplug etc.	Certificate Authorities (6EA)

제안 시스템은 분산신원증명(DID)이나 공동인증서와 같이 PKI 기반의 전자서명을 이용한다는 공통점은 있지만, Table 3.과 같이 몇 가지 항목을 기준으로 차이점에 대해 살펴보면 이제까지는 없던 처음으로 제안하는 시스템인 것을 알 수 있다.

제안 시스템과 기존의 신원증명 시스템은 활용영역이나 통신 방식에서 모델이 다르다 보니 관련 사업자나 기관이 없다. 제안 시스템은 이용자가 간편하게 자신의 정보를 입력하여 증명서를 발급하고 1:1 또는 1:N의 소규모 그룹에서 빠르게 신원증명을 할 수 있는 다양한 분야에서 활용이 가능하다. 앞서 언급한 개인 간 디지털 명함 교환이나 교수-학생 간 출석확인을 포함하여 규모가 큰 컨퍼런스 같은 행사 참석 확인이나, 소규모 회의 또는 동창회, 동호회 등의 모임 참석 확인, 지자체에서 홍보하는 여행지, 관광지 방문 확인, 음식점 방문 확인 등과 같이 근거리 무선 통신 범위 안에서 해당 디바이스를 소유한 이용자가 현장에 있었다는 내역 확인이 필요한 서비스에 적합하다. 반면에 자신의 정보를 자신이 입력하여 그 정보에 대해 보증을 해 주는 제3의 기관이 없다보니, 금융서비스나 공공서비스 등과 같이 공식적으로 실명확인이 필수적인 분야에는 적합하지 않다.

IV. 제안 시스템의 보안 위협 및 요구사항

4.1 제안 시스템의 보안 위협 식별

제안 시스템은 사용자가 직접 개인정보를 입력하여 보관하는 모바일 앱 기반의 신원증명 시스템으로 보안 위협 및 요구사항도 모바일 디바이스로 한정하고, 일반적인 데이터베이스로 구현된 오프체인과 분산원장 기술로 구현된 온체인에 대한 위협은 다루지 않는다. 이런 관점에서 제안 시스템에 대한 보안 위협은 다음과 같다.

- 신원정보의 위조(ST1) : 제안 시스템의 활용 사례에 따라서 자신의 신원을 위조할 이유가 없는 경우도 있지만, 악의를 가지고 최초 입력하는 정보를 사실과 다르게 입력하는 경우가 있을 수 있다. 위조된 정보를 포함한 증명서는 신원증명 과정까지 위조되어 시스템의 신뢰성을 저하시킬 수 있다.
- 신원정보의 탈취(ST2) : 이용자의 신원정보는 모바일 디바이스에 보관되어 필요에 따라 이용자가 제출 및 교환한다. 이 과정에서 신원정보가

탈취 및 도용될 수 있다.

- 키 유출(ST3) : 모바일 디바이스에는 신원정보를 안전하게 보관하기 위한 암호키와 신원증명서에 전자서명을 위한 개인키가 필요하다. 관리 소홀로 인한 키 유출시 신원정보가 노출될 수 있다.
- 모바일 앱 위·변조(ST4) : 제안 시스템은 모마일 앱을 기반으로 서비스를 제공한다. 모바일 앱이 해킹에 의해 변경되거나 악성코드에 감염이 되는 경우, 서비스 중단이 발생할 수 있다.
- 무선 통신 모듈 보안 위협(ST5) : 모바일 디바이스 단거리 무선 통신 기술에 대한 보안위협은 통신 기술 뿐 아니라, 디바이스 제조사, 모바일 OS 벤더, 퍼블릭 앱 스토어, 앱 서버 등 측면에서 살펴봐야 한다[22]. 그 중에 제안 시스템에서 사용하는 블루투스라는 특정 기술에 대해서도 수많은 보안위협에 대한 안내가 되어 있다[23].

4.2 제안 시스템 보안 요구사항

앞에서 살펴본 모바일 앱 기반의 제안 시스템의 보안 위협에 대해 대응하기 위한 보안 요구사항은 다음과 같다.

- 본인확인(SR1) : 제안 시스템에서는 제3의 신원보증기관이 없어 이용자가 고의로 위조된 정보를 입력하는 경우를 즉시 밝혀내기는 쉽지 않다. 다만, 특정 신원증명서 생성 시에는 최소한의 휴대폰 본인인증을 거쳐 위조할 수 없는 기본 정보를 함께 전달하여 필요시 감사추적성을 제공할 수 있다. 디바이스 제조사에서 제공하는 IMEI(International Mobile Equipment Identity)[24]나 블루투스 주소(BD_ADDR)와 같은 디바이스 식별정보 또는 그 값들을 조합하거나 단방향 암호화하여 이용할 수도 있다. 제안 시스템의 모바일 앱에서 이런 정보를 확인하면 식별 및 중복 감지도 구현 가능하다.
- 데이터 암호화(SR2) : 이용자가 직접 자신의 신원정보를 입력하여 모바일 디바이스에 보관하므로 안전한 암호화 알고리즘을 이용하여 신원정보 암호화가 필수적이다. 모바일 환경임을 고려하여 안전한 경량 암호 알고리즘 적용도 가능하다.
- 안전한 저장소(SR3) : 암호화된 데이터를 포함하여 제안 시스템에서 처리되는 다양한 정보를 모바일 디바이스라는 한정된 저장 공간에 안전하게 보관하기 위한 저장소가 필요하다. 전자지갑을 만들어 지갑에 대한 암호화 및 접근제어를 적용할 수 있다.
- 안전한 키 관리(SR4) : 제안 시스템에는 최소한 2개의 키가 활용되고, 키가 유출되지 않도록 안전하게 관리되어야 한다. 하드웨어 기반의 TPM(Trusted Platform Module)[25], TEE(Trust Execution Environment), SE(Secure Element)[26] 등을 적용하는 것이 보다 안전하겠지만, 이는 모바일 디바이스 제조사와도 관련된 문제이므로 제안 시스템에서 해결 할 수 있는 영역은 아니다. 모바일 앱 구현하는 과정에서 암호키를 소프트웨어로 구현된 암호 알고리즘 속에 섞어 공격자가 키를 쉽게 알 수 없도록 소프트웨어 기반의 WBC(WhiteBox Cryptography)[27]을 적용할 수 있다.
- 악성코드 통제(SR5) : 모바일 앱 또는 디바이스는 악성코드 감염으로 인한 정보 유출을 방지하기 위해 보호 대책이 필요하다. 모바일 백신이나 앱 난독화 등의 조치가 적용될 수 있다.
- 패치 관리(SR6) : 사실 무선 통신 모듈에 대한 보안 위협에 대해 제안 시스템 측면에서 대응할 수 있는 가장 효과적인 방법이다. 블루투스의 사례를 보더라도 모바일 OS 및 서버 OS 차원에서 블루투스 취약점을 조치한 보안패치를 최대한 빠르게 적용하는 것이 필요하다.
- 효과적인 보안 교육(SR7) : 편리하지만, 보안위협을 내포하고 있는 단거리 무선 통신 기술을 활용하는 제안 시스템의 이용자들에게 적합한 보안 교육이 지속적으로 실시되어야 한다. 실제로 앱을 사용할 경우에만 블루투스 통신사용을 설정한다면, 보안위협이 공격으로 연결되는 가능성은 현저하게 낮아진다. 보안 교육에 대한 부분은 제안 시스템을 개발 및 운영하게 되는 인원이나 모바일 앱을 사용하는 이용자들에게 그 역할에 맞는 적절한 내용으로 적용되어야 한다.

Table 4.는 제안 시스템에서 보안 요구사항을 충족하면, 각각의 보안 위협을 경감시킬 수 있음을 나타낸다. 그리고 제안 시스템이 1:1 또는 1:N 이용자들끼리 단거리 무선 통신이 가능한 일정 범위, 즉 수 십 미터 내 현장에서 작동한다는 것은 상시 인터넷으로 연결된 환경에 비해서는 보안사고 발생 확률은 현저히 낮다. 하지만, 이용자가 소지하는 모바일

Table 4. Security Requirements for Security Threats for the Proposed System

Security Threats	Security Requirements						
	SR1	SR2	SR3	SR4	SR5	SR6	SR7
ST1	△						△
ST2		○	△	△			
ST3			△	○			
ST4					○		△
ST5						○	○

디바이스가 항상 LTE 또는 WiFi에 연결되어 있는 상태이므로 평상시 모바일 디바이스를 사용하는데 있어 보안 준수 사항을 잘 지키고 생활화 되어 있는지 여부가 중요한 보안 대응 방안이 될 수 있다.

V. 결 론

본 논문에서는 Peer DID 기술과 단거리 무선 통신을 이용한 모바일 앱 기반의 제안 시스템의 구성과 동작 원리, 활용 사례를 설명하고, 그 보안 위협과 요구사항에 대해서도 알아보았다. 제안 시스템이 가지는 의미는 제 3의 신뢰기관(trust anchor) 없이 사용자가 직접 자신의 정보를 생성하여 발급기관(issuer)과 소유자(holder)를 일치시킴으로써 자기주도 신원증명의 개념을 강화한 것이다. 제안 시스템을 활용하면, 신원증명에 참여하는 이용자들끼리 모바일 디바이스로 직접 연결하므로 신원증명에 필요한 절차를 간소화하고, 보안 및 프라이버시 개선, 비용 절감의 효과가 있다. 또한 서비스 사례에 따라 단순한 신원증명 뿐 아니라, 추가적으로 필요한 신뢰할 수 있는 증명서를 발급받을 수도 있고, 분산원장 기술을 적용 시 여러 도메인의 사용자와 신원증명 서비스도 가능하다.

향후 연구 과제로는 제안한 시스템이 아직 구현되지 않고, SW 및 통신 설계 구성만으로 보안 위협과 요구사항을 제시했다는 한계가 있으므로, 이를 실제로 구현하는 과정을 통해 실증 연구를 추진할 필요가 있다. 모바일 앱 개발 및 서버 시스템을 구축하는 과정에서 보완하거나 고려해야 할 사항에 대해 대응이 필요할 것으로 예상된다. 시스템의 확장 및 연계를 위해 온체인(분산원장)을 활용하는 방안을 제시하였지만, 오프체인과 온체인 간 주고받는 메시지 규격에 대해서도 보다 상세한 정의가 필요하다.

추가적으로 활용도를 높이기 위해서는 자체 모바일 앱 개발 이외에도 SDK 제공을 통해 다른 사설 인증 서비스를 기본으로 제공하는 앱에 탑재하는 인앱(in-app) 방식이나 활용도가 높은 다른 모바일 앱과 연동하는 앱투앱(app-to-app) 방식도 생각해 볼 수 있다. 나아가 이용자들의 모바일 디바이스 간 신원증명 뿐 아니라 디바이스 범주를 확장하여 사람과 사물, 사물과 사물 간 상호 인증에 활용할 수 있다. 대표적인 사례로 커넥티드(connected) 환경에서의 차량(vehicle)에 대해 운전자와 차량, 차량과 차량, 차량과 주변 센서(sensor)간 인증은 보안에서 필요한 영역이다.

COVID-19로 인한 초유의 팬데믹 현상이 사회의 많은 부분을 디지털로 전환시키는 디지털 트랜스포메이션(Digital Transformation) 시대를 앞당기고 있다. 이러한 시점에 신원증명 방식도 다양한 기술을 이용하여 디지털화, 분산화, 자기주권화 되고 있어 본 논문에서 제안하는 단거리 무선 통신을 이용한 개인 간 신원증명 시스템과 같은 추가적인 연구가 필요하다.

References

[1] Personal Information Protection Commission, "Enforcement Decree of the Personal Information Protection Act, Article 19," National Law Information Center, Ministry of Legislation, Presidential Decree No. 31429, Feb. 2021

[2] Computer World, "[Focus] Abolition of monopoly status of accredited certificates, Private authentication market opens," https://www.comworld.co.kr/news/articleView.html?idxno=49867, Accessed : June 2021

[3] MSIT release, "December 10, Abolition of the Accredited Electronic Signature system," Ministry of Science and ICT, Dec. 2020

[4] Korea Disease Control and Prevention Agency, "Act on the Prevention and Management of Infectious Diseases, Article 49," National Law Information

Center, Law no. 17920, Mar. 2021
[5] Kanghyo Lee, "The need for DID-based mobile ID for the post-corona era," Korean Internet & Security Agency, KISA Report, vol.10, 2020
[6] Joint of Relevant Ministries, "Blockchain technology diffusion strategy," Ministry of Science and ICT, June 2020
[7] Security Technology Research Team, "The concept and overseas technology trend of decentralized ID," e-Finance and Financial Security no. 16, pp. 15-39, Financial Security Institute, April 2019
[8] Hee-won Shim, "Domestic and overseas trends and implications of decentralized ID technology," Korea Financial Telecommunications & Clearings Institute, no. 73, Dec. 2019
[9] Manu Sporny, Dave Longley and David Chadwick, "Verifiable credentials data model 1.0," W3C Recommendation, Nov. 2019
[10] DaeGeun Yoon, Self-sovereign identity verification structure analysis, Jpub, July 2020
[11] Drummond Reed, Manu Sporny, Dave Longle, Christopher Allen, Ryan Grant, Markus Sabadello, "Decentralized Identifiers (DIDs) v1.0," W3C Recommedation Draft, June 2021
[12] HyoKwan Kang, "Status of domestic authentication technology and service," Korea Institute of Information Security and Cryptology, vol. 30, no. 3, pp. 31-36, June 2020
[13] "〔Forum〕 Inoculation certificate, mutual recognition between countries is urgently needed," THE DIGITAL TIMES, http://www.dt.co.kr/contents.html?article_no=2021052802102369073001, Accessed : May 2021
[14] Korea Policy Briefing, "Pilot implementation of mobile driver's license from year-end …Nationwide expansion next year," https://www.korea.kr/special/policyFocusView.do?newsId=148886928&pkgId=49500747, Accessed : May 2021
[15] Oskar Deventer, Christian Lundkvist, Márton Csernai, Kyle Den Hartog, Markus Sabadello, Sam Curren, Dan Gisolfi, Mike Varley, Sven Hammann, John Jordan, Lovesh Harchandani, Devin Fisher, Tobias Looker, Brent Zundel, Stephen Curran, "Peer DID Method Specification," W3C, April 2021
[16] SSImeetup Identity Webinar, "Peer DIDs: a secure and scalable method for DIDs that's entirely off-ledger," https://ssimeetup.org/peer-dids-secure-scalable-method-dids-off-ledger-daniel-hardman-webinar-42, Accessed : May 2021
[17] Ryan West, Daniel Bluhm, Matthew Hailstone, Stephen Curran, Sam Curren, Stephen Curran, George Aristy, "Aries RFC 0023: DID Exchange Protocol 1.0," https://github.com/hyperledger/aries-rfcs/tree/master/features/0023-did-exchange, Accessed : May 2021
[18] Core Specification Working Group, "Bluetooth Core Specification," Bluetooth Special Interest Group, v5.2, Dec. 2019
[19] Kai Ren, "Bluetooth Pairing Part 4: Bluetooth Low Energy Secure Connections - Numeric Comparison," Bluetooth Blog, https://www.bluetooth.com/blog/bluetooth-pairing-part-4/, Accessed : June 2021
[20] Y.H. Kwon, "5th generation Bluetooth technology for wearable devices,"

Institute of Information & communications Technology Planning & Evaluation, Weekly ICT Trend, vol. 1961, Aug. 2020

[21] Korea Certification Authority Central, https://www.rootca.or.kr/, Korea Internet & Security Agency, Accessed : June 2021

[22] Joshua M Franklin, Christopher Brown, Spike Dog, Neil McNab, Sharon Voss-Northrop, Michael Peck, Bart Stidham, "Assessing Threats to Mobile Devices & Infrastructure," National Institute of Standards and Technology, Interagency Report 8144, Sep. 2016

[23] John Padgette, John Bahr, Mayank Batra, Marcel Holtmann, Rhonda Smithbey, Lily Chen, Karen Scarfone, " Guide to Bluetooth Security," National Institute of Standards and Technology, Special Publication 800-121, May 2017

[24] Seon-Joo Kim, "Secure Management Method for Private Key using Smartphon's Information," The Korea Contents Association vol. 16, no. 8, pp. 90-96, Aug. 2016

[25] Trusted Computing Group, "TPM 2.0 Mobile Reference Architecture," TCG specification, Dec. 2014

[26] Gil Bernabeu, "TPM & TEE - working together in harmony," https://globalplatform.org/tpm-tee-working-together-in-harmony/, Accessed : June 2021

[27] S.H. Kim, Y.K. Lee, B.H. Chung, "Analysis on Trends for White-Box Cryptography and Its Application Technology," Electronics and Telecommunications Research Institute, Electronics and Telecommunications Trends Analisys, vol. 25, no. 5, Oct. 2010

〈저 자 소 개〉

여 기 호 (Kiho Yeo) 종신회원
1999년 2월: 서강대학교 컴퓨터공학과 학사
2012년 8월: 건국대학교 정보통신대학원 정보보안전공 석사
2016년 2월: 순천향대학교 대학원 정보보호학과 박사과정 수료
2013년 3월~현재: 현대오토에버 블록체인서비스개발팀 책임
〈관심분야〉 분산원장기술 보안, 자동차 보안, IoT 보안, 클라우드 보안, 정보보호관리체계

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
2016년 5월~현재: 개인정보보호표준포럼 의장
〈관심분야〉 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜, 5G 보안, 분산원장기술 보안