Journal of Convergence for Information Technology
Vol. 11. No. 11, pp. 66-74, 2021
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2021.11.11.066

탈중앙화 신원증명에 기반한 본인 인증 모델

김호윤[1], 한군희[2], 신승수[3*]
[1]동명대학교 컴퓨터미디어공학과 학생, [2]백석대학교 컴퓨터공학부 교수, [3]동명대학교 소프트웨어융합보안학과 교수

A Model for Self-Authentication Based on Decentralized Identifier

Ho-Yoon Kim[1], Kun-Hee Han[2], Seung-Soo Shin[3*]
[1]Student, Dept. of Computers & Media Engineering, Tongmyong University
[2]Professor, Division of Computer Engineering, Baekseok University
[3]Professor, Dept. of Software Convergence Security, Tongmyong University

요 약 인터넷이 발달하면서 온라인에서 나를 증명하는 사용자 인증기술은 고도화되고 있다. 기존 ID 방식은 서비스 제공자가 개인정보를 관리하며 보안이 취약할 경우 개인정보 유출의 위협이 있고, 정보 주체가 서비스 제공자에게 있다. 본 연구에서는 온라인 신분 확인 기술이 발전함에 따라 중앙집중 형식에서 오는 개인정보 유출 위협을 낮추고 사용자 주권 강화를 위한 DID 기반 본인 인증 모델을 제안한다. 제안 모델은 발행기관으로부터 발급받은 VC를 통해 사용자가 직접 개인정보를 관리하고 정보 주제가 사용자에게 있어 주권을 강화할 수 있다. 연구 방법으로는 분산원장 기술을 기반으로 한 탈중앙화 신원증명 방법을 이용하여 보안성과 무결성을 보장하는 본인 인증 모델을 제시하고, 공격방식에 대한 보안성을 분석한다. 공개키 암호 알고리즘을 사용하는 DID Auth를 통해 인증하여 스니핑, 중간자공격 등으로부터 안전하며 제안 모델은 실물 신분증을 대체할 수 있다.

주제어 : 블록체인, 공개키 기반 구조, 탈중앙화 신원증명, 인증, 신분증

Abstract With the development of the Internet, user authentication technology that proves me online is improving. Existing ID methods pose a threat of personal information leakage if the service provider manages personal information and security is weak, and the information subject is to the service provider. In this study, as online identification technology develops, we propose a DID-based self-authentication model to prevent the threat of leakage of personal information from a centralized format and strengthen sovereignty. The proposed model allows users to directly manage personal information and strengthen their sovereignty over information topics through VC issued by the issuing agency. As a research method, a self-authentication model that guarantees security and integrity is presented using a decentralized identifier method based on distributed ledger technology, and the security of the attack method is analyzed. Because it authenticates through DID Auth using public key encryption algorithms, it is safe from sniffing, man in the middle attack, and the proposed model can replace real identity card.

Key Words : Blockchain, Public Key Infrastructure, Decentralized Identifier, Authentication, Identity card

*This research was supported by the BB21plus funded by Busan Metropolitan City and Busan Institute for Talent & Lifelong Education(BIT).

*Corresponding Author : Seung-Soo Shin(shinss@tu.ac.kr)

Received September 13, 2021
Revised October 21, 2021
Accepted November 20, 2021
Published November 28, 2021

1. 서론

ICT 기술이 발전함에 따라 오프라인과 마찬가지로 온라인에서도 많은 일을 처리하고, 서비스를 제공하기 때문에 신원확인은 필수적이다. 코로나-19로 인하여 비대면 또는 비접촉 하여 자신의 신원을 확인해야 하는 경우가 많다. 이는 실물 신분증이 가지는 한계점을 드러내며, 온라인 신분 확인 기술의 발전을 촉진한다. 일반적으로 온라인상에서의 신원확인 방법은 웹 사이트별로 사용자가 개인정보를 제공하고, 아이디와 비밀번호를 통해서 인증한다[1]. 즉, 자신의 개인정보를 아이디와 패스워드를 통해 접근한다. 이는 이용하는 서비스가 증가함에 따라 같은 정보를 여러 사이트에 입력해야 하며, 기억해야 할 아이디와 비밀번호 역시 증가한다. 이를 개선하기 위해서 연합 신원 모델의 기술이 발전하고 있다[2].

연합 신원 모델(SSO: Single Sign On, 통합로그인)은 OpenID, OAuth 등을 기반으로 SNS 서비스 또는 포털사이트의 계정(IdP: Identity Provider)을 이용하여 RP(Relying Party) 웹 사이트에 회원가입 및 로그인을 할 수 있는 기술이다[3]. 중앙집중화된 IdP는 사용자에게 편리함을 제공하지만 사용자가 어떤 서비스를 얼마나 이용하는지와 같은 정보는 물론 모든 활동의 추적이 가능하며, 해킹 사고 시 많은 피해가 발생한다.

중앙집중식의 문제점을 해결하기 위해 분산원장 기술(DLT: Distributed Ledger Technology)의 발달과 이슈로 중앙화된 시스템에서 점차 탈중앙화 시스템으로 변화하며 발전하고 있다. 특히, 자기주권 신원증명(SSI: Self- Sovereign Identity)이 가능한 탈중앙화 신원증명(DID: Decentralized Identifier)이 주목받고 있다[4,5]. 자기주권 신원증명은 탈중앙화 구조를 바탕으로 사용자가 직접 자신의 ID를 관리할 수 있고, 데이터의 주권을 ID 주인에게 부여하는 기술이다. 사용자는 자신의 ID를 직접 제출하면서 관리하는 권한을 가지고, 기존 ID 기술과는 달리 신분증에서 필요한 정보만 공개하거나 영지식 증명을 통해 정보를 공개하지 않고도 신원인증이 가능한 기술이다[6,7].

DID는 데이터산업 활성화를 위한 우리나라의 데이터 3법 개정 및 시행(2020년 8월 5일), 2016년 5월 유럽(EU)의 개인정보보호규정(GDPR: General Data Protection Regulation) 시행(2018년 5월 25일), 2018년 6월 28일 미국 캘리포니아주 소비자프라이버시법(CCPA: California Consumer Privacy Act of 2018)의 시행(2020년 1월 1일), 마이데이터 산업 대두 등 개인정보에 대한 주체의 권한이 강화되고 있다[8-11].

본 논문에서는 사용자의 자기주권 강화와 개인정보 노출 방지를 위해 탈중앙화 신원증명 기반의 본인 인증 모델을 제안한다. 사용자는 제안하는 모델을 통해 개인정보를 직접 관리하고 영지식 증명으로 서비스 이용 시 개인정보 노출을 방지한다. DID document를 관리하는 레지스트리를 Hyperledger 플랫폼으로 관리하여 사용자의 승인 없이는 변경하여 사용하지 못하도록 한다.

2. 관련 연구

본 장에서는 자기주권 신원증명을 실현하게 해주는 DID, Hyperledger와 인증기술 관련 연구를 기술하였다.

2.1 Hyperledger

블록체인은 일반적으로 참여 방법에 따라 허가형, 비허가형으로 분류된다. Hyperledger는 허가형 블록체인으로 네트워크에 참여하여 원장의 내용을 읽는 것뿐만 아니라 블록을 생성하고 원장에 기록하기 위해서도 그룹의 허가가 필요하다. 대표적으로 Hyperledger Fabric, Hyperledger Indy 등이 있고 Hyperledger Fabric은 Chain Code라는 Ethereum의 Smart Contract 개념으로 Chain Code를 중심으로 관리한다. 특히 Hyperledger Indy는 DID에 특성화된 플랫폼이다[12,13].

2.2 DID

DID는 분산원장 기술을 기반으로 한 신원증명이며, 중앙시스템에 통제받지 않고 개인이 자신의 정보에 완전한 통제권을 갖도록 하는 디지털화된 신원 관리 체계 기술이다. 사용자가 분산원장에 연동된 디지털 지갑 안에 자신의 개인정보를 담아 필요할 때 개인키를 입력해 자신을 증명하는 방식이다. 분산원장 기술을 기반으로 하는 DID는 DIF(Decentralized Identity Foundation)의 주도로 개념과 설계가 세워졌으며 W3C(World Wide Web Consortium)가 주도하에 국제 표준(Decentralized Identifiers Standards)이 제정되고 있다[14,15].

DID 서비스의 참여자는 사용자(Holder), 발행기관(Issuer), 검증인(Verifier)으로 구성된다. 사용자는 모바일기기 전자지갑 앱을 통해 개인정보를 직접 관리한

다. 발행기관은 사용자가 신분증, 증명서 등의 발행을 요청할 경우 사용자를 검증한 후 요청자료를 발행한다. 검증인은 서비스를 제공하는 기업이나 기관이며, 사용자가 제출한 신분증 또는 증명서를 검증한 후 서비스를 제공한다[16].

2.3 생체인증

본인 인증 방법에는 여러 가지가 있다. 지식기반, 소유기반, 생체기반 등이 있으며 ID/PW, OTP, PIN, 공인인증서, 생체인증 등의 다양한 방법이 있다.

생체인증 방법에는 지문, 홍채, 정맥, 얼굴 등이 있으며, FIDO(Fast IDentity Online) 표준을 기반으로 한다. FIDO 표준은 2가지를 제정하여 2014년 12월 공개하였다. FIDO는 패스워드 외에 모든 인증 방식을 사용할 수 있다. FIDO의 인증 방식은 U2F(Universal 2nd Factor), UAF(Universal Authentication Factor)가 있으며, U2F는 Authenticator가 기기에 포함되지 않고 UAF는 포함된 형태이다. 생체인증은 UAF 기반으로 수행한다[17]. 최근에는 블록체인을 활용한 인증기술이 지속적으로 연구되고 있다.

3. 자기주권 본인 인증 관리 모델

본인 인증은 여러 기술을 통해 실현되고 있으나 여전히 문제점들이 있다. 본 논문에서는 DID에 기반한 자기주권 신원증명의 실현으로 개인정보의 주체가 사용자에게 있으며 외부 기관에 통제받지 않고 오늘날 ID 기술의 부족한 부분을 개선할 수 있다.

3.1 본인 인증 모델 구성

자기주권 신원증명 플랫폼의 주요 참여자는 발행기관(Issuer), 사용자(Holder), 검증인(Verifier), 그리고 DID 관련 정보를 저장하는 분산저장소로 Verifiable Data Registry가 있다. 발행기관은 신뢰기관으로써 사용자가 요청한 신원증명을 DID를 통하여 검증 후 발행한다. 사용자는 신원증명을 필요한 항목만으로 검증인에게 제출하기 위해 재가공한다. 검증인은 서비스 제공자이며 사용자로부터 제공 받은 신원증명의 진위 여부를 분산저장소를 통해 검증한 뒤 서비스를 제공한다. 제안하는 모델은 Issuer, Holder, Verifier, 그리고 Verifiable Data Registry가 있고 12단계의 절차로 이루어지며 Fig. 1과 같다.

3.2 모델 구성요소

SSI 플랫폼의 구성요소는 식별자 및 인증수단을 위해 이용되는 DID, DID document가 있고, 사용자가 보관하는 신원증명 ID 속성인 검증 가능한 자격증명(VC: Verifiable Credential), 그리고 검증인에게 제출하기 위한 속성 ID로 검증 가능한 제공 ID 데이터 집합(VP: Verifiable Presentation)이 있다.

Fig. 1에서 사용자와 발행기관은 각각 DID를 생성하고, DID document는 분산저장소에 저장한다. 사용자는 VC를 발급받기 위해 발행기관에 요청한다.

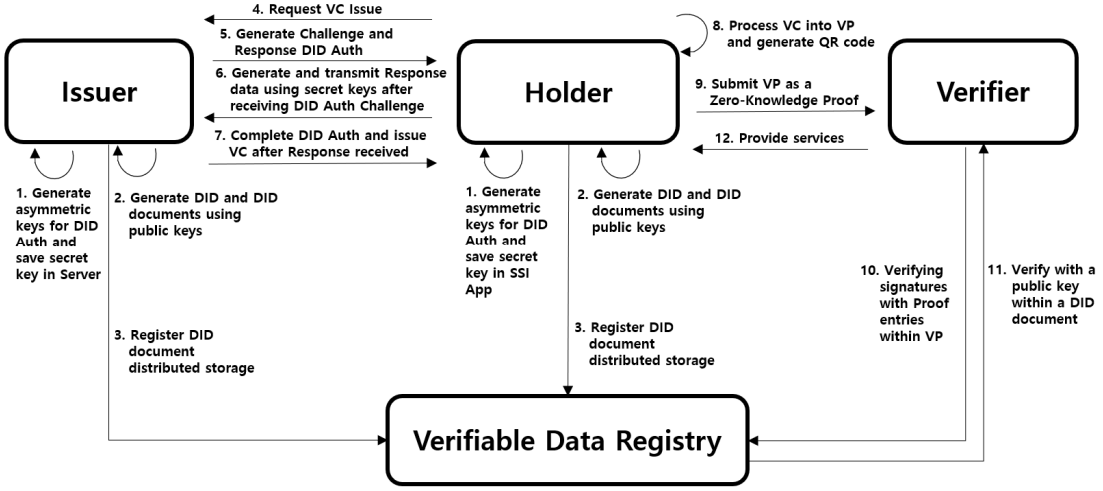


Fig. 1. Proposed System Scenario

우선 발행기관은 1차 적으로 사용자에게 본인 인증 확인을 요청한다. 본인 인증은 모바일 인증과 PIN 등으로 수행한다. 이후 VC를 발급하기 위해 Challenge DID Auth를 사용자에게 요청하고 사용자는 응답으로 Response를 생성하여 전송한다. DID Auth가 완료되면 발행기관은 사용자에게 VC를 발급하고 사용자는 VC를 검증인에게 제출할 필요한 항목만 VP로 재구성한다. 사용자는 VP를 영지식 증명으로 검증인에게 제출하고 검증인은 분산저장소를 통해 VP를 검증한 뒤 사용자에게 서비스를 제공한다.

3.2.1 DID

DID는 DID document의 위치를 나타낼 수 있는 주소이다. DID는 세 부분인 Scheme, Method, Method- Specific Identifier로 구성된다. Scheme는 DID 식별자임을 표시하는 것으로 URI가 어떠한 종류의 프로토콜을 사용하여 자원에 접근하는지 명시하며 모든 DID Scheme는 did로 시작한다. Method는 DID document가 어느 저장소이고 어디 저장되어 있는지 보여주며, DID가 생성, 읽기, 업데이트, 삭제 CRUD (Create, Read, Update, Delete)를 수행하는 방법을 지정한다. Method-Specific Identifier는 저장소 내에 DID document가 저장된 위치를 검색하기 위한 주소이다. DID를 이용하면 자기주권 신원증명을 실현할 수 있다. DID의 예시 구조는 Fig. 2와 같다.

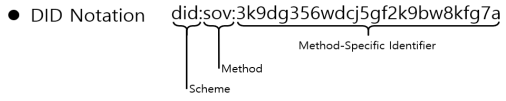


Fig. 2. Decentralized ID Structure Example

3.2.2 DID document

DID는 DID 주소 값과 1:1 관계를 가지는 DID document가 있으며, 이는 분산저장소에 저장된다. 분산저장소로는 블록체인을 사용하며, Bitcoin, Ethereum과 같은 비허가형 네트워크뿐만 아니라 Indy-node와 같이 DID에 특화된 네트워크도 사용하며, W3C DID 표준 명세에서는 Verifiable Data Registry라고 정의한다.

DID document는 DID 소유 인증에 사용되는 PublicKey 값을 포함하고 있다. 그리고, 분산저장소마다 DID document를 읽고 쓰는 방법이 다르기 때문에 각 분산저장소마다 액세스 방법을 정의한 명세가 필요한데 이를 DID method라고 한다. DID document는 상대방과의 인터랙션 과정에서 서명 확인이나 Challenge 암호화와 같은 동작을 위해서 대상 DID와 연관된 Public-Key 값을 조회하기 위한 목적과 DID와 연관된 Service -Endpoint 정보를 디스커버리하기 위한 목적으로 사용한다.

일반적으로 분산저장소에 기록되는 DID document의 속성은 PublicKey, Authentication, Service가 있다. DID를 생성할 때 만드는 Public-Key 값은 DID document 데이터 구조체 안에 “PublicKey” 속성에 추가되고 해당 내용이 기록된다. 상세한 DID document 구조 예시는 Fig. 3과 같다.

```
{
    "@context": "https://www.w3.org/ns/did/v1",
    "id": "did:ethr:1234",
    "publicKey": [{
        "id": "did:ethr:1234#keys-1",
        "type": "RsaVerificationKey2018",
        "controller": "did:ethr:1234",
        "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
    }, {
        "id": "did:ethr:1234#keys-2",
        "type": "Ieee2410VerificationKey2018",
        "controller": "did:ethr:1234",
        "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
    }, {
        "id": "did:ethr:1234#keys-3",
        "type": "RsaVerificationKey2018",
        "controller": "did:sov:ABCD",
        "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
    }],
    "authentication": [{
        "did:ethr:1234#keys-1",
        "did:ethr:1234#keys-2",
        "did:ethr:1234#keys-3"
    }],
    "service": [{
        "id": "did:ethr:1234#KeyRotation",
        "type": "RotateUserKey",
        "serviceEndpoint": "https://example.com/keyrotation/"
    }]
}
```

Fig. 3. DID Document Structure

3.2.3 VC

VC(Verifiable Credential)는 신분증, 졸업증명서, 재직 증명서, 자격증 등의 ID 속성이 포함된다. VC는 Credential Metadata, Claim, Proof로 구성된다. Credential Metadata는 VC를 발행한 기관, VC가 명시하는 객체(Credential subject), VC의 만료 기간, VC의 폐기 방법 등이 정의된다. Claim에는 Credential subject의 ID 속성에 대한 정보로 Subject-Property-Value 방식으로 저장된다. Proof는 진위여부 검증에 대해 필요한 값으로 RSA, ECDSA, 생체인증 등으로 다

양한 암호 기법이 사용된다. VC 항목의 구성요소는 Fig. 4와 같다.

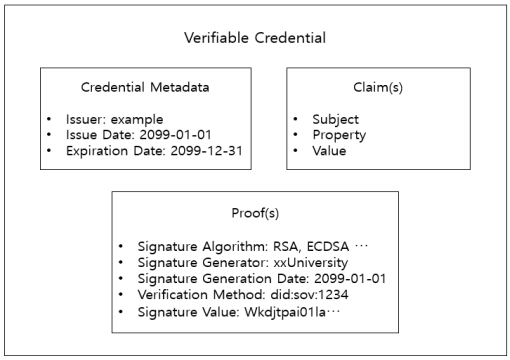


Fig. 4. VC Element

3.2.4 VP

사용자는 검증인에게 자신(Identity)을 증명하기 위해 VC를 직접 제출하지 않고 자신이 소유한 VC를 VP로 재가공하여 제출한다. VP는 Presentation Metadata, Verifiable Credential, Proof로 구성된다. Presentation Metadata는 해당 데이터가 VP라는 것을 명시한 Type, 이용약관, Evidence 등 VP 검증에 참고할 수 있는 데이터가 포함된다.

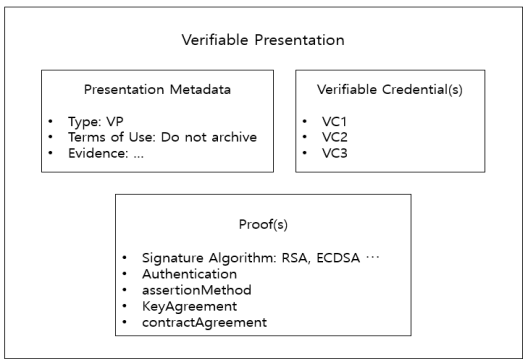


Fig. 5. VP Element

Verifiable Credential은 VC가 포함된다. 검증인이 요구하는 ID 속성을 가진 VC를 선택하여 Verifiable Credential 항목에 넣을 수 있다. VC 내에 검증인이 요구하는 Claim만 선택하여 Verifiable Credential에 포함 시켜 사용자의 Privacy를 보호한다. VP를 수신한 검증인은 VC 내에 포함된 Proof 항목으로 VC의 진위를 검증한다. VC의 Proof 항목에는 발행기관의 서명이 들어가며 VP의 Proof 항목에는 사용자의 서명이 들어간다. VP 항목의 구성요소는 Fig. 5와 같다.

3.3 본인 인증 모델 시나리오

제안하는 모델의 시나리오는 사용자, 발행기관, 검증인, 그리고 분산저장소가 있다. 흐름도는 Fig. 6과 같고 구체적인 시나리오 흐름도 설명은 다음과 같다.

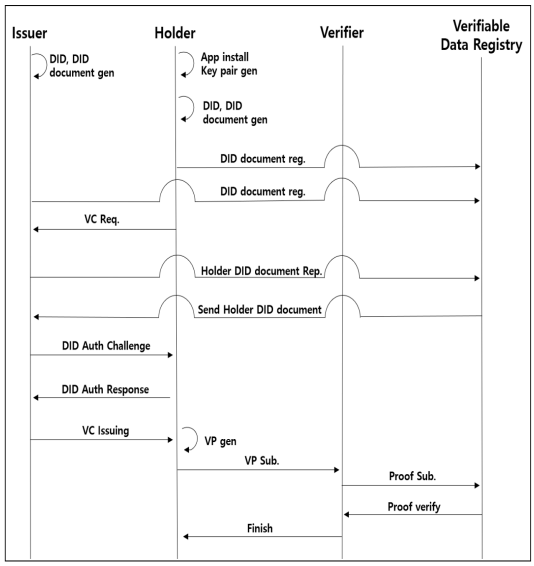


Fig. 6. Proposed System Flow Chart

사용자와 발행기관은 DID 소유권 증명을 위해 DID Auth에 사용할 비대칭키를 생성한다. 비대칭키의 개인키는 각 서버와 SSI Wallet App에 저장한다. 비대칭키에서 공개키는 DID 및 DID document를 생성하는데 사용한다. 이후 DID와 DID document를 생성한 후 DID document는 분산저장소에 등록한다.

사용자는 자신의 DID를 이용하여 전자주민증 VC 발급을 발행기관에 요청한다. 요청 시 본인 인증은 모바일 인증, 공동인증서, PIN 등으로 한다. 발행기관은 사용자의 DID로부터 DID document가 저장된 위치를 확인하며, DID document를 획득하여 Challenge를 생성한 후 사용자에게 DID Auth를 요청한다. DID Auth의 Challenge를 수신한 사용자는 개인키를 이용하여 Response 데이터를 생성한 후 발행기관에 전송한다. 발행기관은 자신이 요청한 Challenge 데이터에 부합하는 Response 데이터를 수신하면 DID Auth를 완료한 후 사용자가 요청한 전자주민증 VC를 발급하

고, 사용자는 VC를 SSI Wallet App에 저장한다.

검증인은 사용자에게 필요한 인증 항목을 요청하고, 사용자는 요청 항목을 만족하는 VP를 자신이 보유한 VC로 생성한다. VP는 QR코드로 변환한다. 사용자는 검증인에게 VP를 영지식 증명을 통해 제출한다. 검증인은 VP를 검증한다. 검증은 VP에 포함된 VC의 Proof 항목으로 VC를 발행한 발행인이 올바른지 검증, VC CredentialSubject와 DID Auth로부터 VC가 가리키는 객체가 사용자가 맞는지 검증, VP Proof 항목으로 VP를 제출하는 사용자가 본인이 맞는지 검증한다. 검증인은 분산저장소에 등록된 DID document의 공개키를 이용하여 Proof 항목을 검증한다. 검증이 완료된 검증인은 사용자에게 서비스를 제공한다.

제안하는 모델은 기존 모델과 달리 DID Auth를 수행하기 전 1차 적으로 본인 인증을 한 번 더 수행하여 보안을 강화하고, 개인키가 담겨있는 사용자의 모바일 전자지갑 접근 시 생체인증을 수행하여 사용자 보안을 강화한다. 사용자는 검증인에게 VP를 제출할 때 영지식 증명을 통해 개인정보 노출을 최소화하고 오프라인에서는 QR코드로 변환하여 제출한다.

3.4 본인 인증 시뮬레이션

본 장에서는 본인 인증 모델의 간단한 시뮬레이션을 통해 확인한다. 시뮬레이션은 Hyperledger Indy 플랫폼 예제를 참고한다.

3.4.1 시뮬레이션 환경

개발을 위한 PC는 LG 그램17 노트북으로 CPU는 8세대 i7-8565U 1.8GHz이고 RAM은 16GB이다. 개발 소프트웨어의 자세한 구성은 Table 1과 같다.

Table 1. Software Development Environment

OS	Windows 10 Home 64bit
VMware Workstation	version 16.1.2
Ubuntu	version 20.04.3 LTS
Golang	version 1.16.5
VS Code	version 1.57.1
NPM	version 6.14.4
Node	version 10.19.0
cURL	version 7.68.0

3.4.2 DID 발급

사용자는 우선 SSI Wallet App을 통해 DID, VC, 인증키 등을 보관한 지갑을 생성한다. App은 사용자 본인만 접근 가능하며 생체인증을 통해 접근한다. App에는 config와 credentials의 매개변수가 있다.

config는 지갑을 식별할 id, 지갑 데이터 저장소를 정의하는 storage_type, 그리고 storage config 관련 정보가 JSON 데이터로 입력된다.

credentials는 인증키 및 비밀번호가 입력되며, 키 생성 방법과 키를 저장하는 저장소 등의 정보가 JSON 데이터로 입력된다.

지갑 생성 후 DID Auth에 사용할 비대칭키를 생성하고, DID 및 DID document를 생성한 뒤 DID document는 Verifiable Data Registry에 등록한다. Indy의 경우 Method-specific identifier의 주소가 공개키의 일부(처음 16바이트)이다. DID 발급 예시는 Fig. 7과 같다.

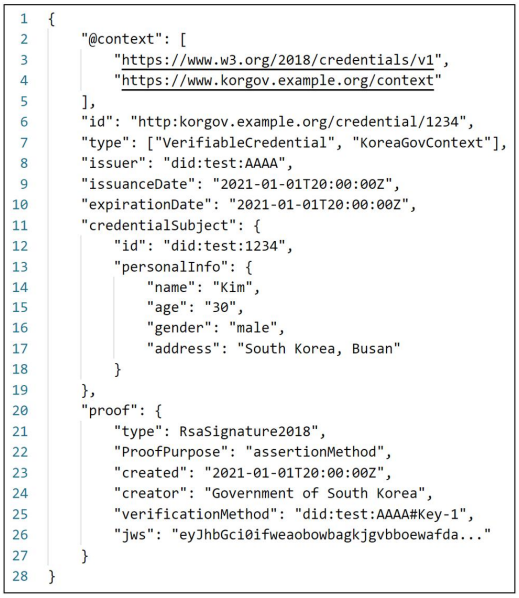
```
{
    "@context": "https://www.w3.org/ns/did/v1",
    "id": did:test:1234",
    "publicKey": [{
        "id": "did:test:1234#keys-1",
        "type": RsaVerificationKey2018",
        "controller": "did:test:1234",
        "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
    }],
    "authentication": [
        "did:test:1234#keys-1"
    ]
}
```

Fig. 7. Example of issuing a DID

3.4.3 VC 발행

VC 발행 요청은 기본적으로 비대면으로 진행한다. VC 발행을 위한 사용자는 발행기관에게 본인 확인 절차로 휴대폰 인증, I-PIN, 공동인증서 등으로 인증한다. 발행기관은 사용자의 DID 소유권을 증명하기 위해 DID Auth를 진행한다. DID 주소를 통해 Verifiable Data Registry에 저장된 DID document를 가져와 DID Auth를 수행하며, Challenge 및 Response를 인증한 후 VC를 발행해준다. DID document에 포함된 PublicKey와 authentication 항목 등을 사용하며 PublicKey 항목에 생체 데이터, 문자 인증 데이터 등을 입력하여 사용할 수 있다. VC를 발행받은 사용자는

VC를 Wallet App에 저장하고 검증인이 요구하는 정보만을 선택적으로 재가공하여 VP를 생성한다. VC 발행 예시는 Fig. 8과 같다.



```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://www.korgov.example.org/context"
    ],
    "id": "http:korgov.example.org/credential/1234",
    "type": ["VerifiableCredential", "KoreaGovContext"],
    "issuer": "did:test:AAAA",
    "issuanceDate": "2021-01-01T20:00:00Z",
    "expirationDate": "2021-01-01T20:00:00Z",
    "credentialSubject": {
        "id": "did:test:1234",
        "personalInfo": {
            "name": "Kim",
            "age": "30",
            "gender": "male",
            "address": "South Korea, Busan"
        }
    },
    "proof": {
        "type": RsaSignature2018",
        "ProofPurpose": "assertionMethod",
        "created": "2021-01-01T20:00:00Z",
        "creator": "Government of South Korea",
        "verificationMethod": "did:test:AAAA#Key-1",
        "jws": "eyJhbGci0ifweaobowbagkjgvbboewafda..."
    }
}
```

Fig. 8. Example of issuing VC

3.4.4 VC 폐기

VC 폐기에는 다양한 이유가 있다. 전자주민증은 이사 후 주소가 바뀌는 등이 있고 재직 증명서의 경우 회사를 이직, 퇴사 등이 있으며 모바일 기기 분실, 변경 등이 있다. VC 폐기를 위해 Tails file, Accumulator, Witness 3가지 요소가 있다. Tails file은 발행한 VC에 해당하는 인수(Factor) 목록이다. 몇 개의 VC를 발행할지 정한 뒤 발행할 개수만큼 VC의 인수가 저장된 Tails file을 생성한다. Accumulator는 생성된 Tails file 인수 중 VC 발행에 사용한 인수들을 이용한 연산 결괏값이다. VC에 대한 인수를 이용하여 Accumulator를 업데이트한다. Witness는 VC의 인수를 제외한 나머지 인수들을 이용한 결괏값이다. 예시로 V2의 Witness를 구하는 식은 다음과 같다.

$$\begin{aligned} &VC1*VC2*VC3 = Accumulator \\ &VC1*VC3 = Witness \end{aligned} \quad (1)$$

사용자는 검증인에게 V2 인수와 Witness를 전달하면 검증인은 이를 계산하여 올바른 Accumulator 값을 구하여 VC 폐기 여부를 검증한다.

4. 분석

본 장에서는 제안하는 본인 인증 모델에 대하여 보안성과 편의성에 대해 분석한다. 보안성에서는 1세대, 2세대 인증 모델과 공격방식 및 위협에 대해 비교 분석하고, 편의성에서는 실생활 적용 시 실효성에 대해 분석한다.

4.1 보안성

1세대 및 2세대 방식의 인증 시스템은 중앙집중식으로 공격자에게 주요 공격 요인이 된다. 중앙집중식으로 관리자의 실수나 해킹 사고 등에 의해 ID가 유출될 수 있고, 내부자의 악의적인 목적으로 무단 도용될 수 있다. 관리자가 사용자 몰래 무단 도용으로 이벤트 내역, 거래를 조작·변조하여 통제할 수 있다.

공격 방식은 중간자 공격, 재전송 공격, 스니핑, 스파이웨어 등이 있다. 분산원장 기술은 중앙 서버에 정보를 저장하지 않고 분산함으로써 공격 요인이 많아지기 때문에 공격이 비효율적이다. 기존 인증 방식과 비교 분석은 Table 2와 같다.

Table 2. Comparison of previous generation methods with proposed models

Classification	ID/PW	SSO	Proposal
ID leakage	Height	Height	Lowness
Unauthorized use of ID by insider	Height	Height	Lowness
ID transaction history tampering	Height	Height	Lowness
Packet sniffing	Normal	Lowness	Lowness
Man in the middle attack	Normal	Lowness	Lowness
Key safety	Normal	Height	Height
Convenience	Lowness	Normal	Height

DID 시스템은 PKI를 기반한 암호화 시스템으로 DID Auth를 인증할 때 매번 다른 값의 Challenge를 수행함으로써 중간자 공격, 재전송 공격 등으로부터 안전하다.

발행기관은 임의의 난수 값을 생성하여 사용자에게 보내고 사용자는 약속된 암호 알고리즘으로 암호화하

여 Response를 전달한다. 인증 서버는 임의의 난수값과 사용자 정보를 이용해서 결괏값을 비교 후 인증을 수행하여 스니핑과 재사용 공격에 안전하며, 인증 서버는 사용자 토큰과 동기를 유지할 필요가 없다. 특히 VP 소유권 증명 시에는 발행기관과 사용자의 Proof가 각각 포함돼 있어 두 차례 인증한다.

4.2 편의성

제안 모델은 App에 접근 시 생체인증 등을 이용하며, 회원가입 절차 없이 휴대폰의 본인 인증을 기본으로 한다. 한국에서 발급받은 신분증, 증명서는 한국에서만 효력이 있으나, 추후 DID 기반 신원증명을 활용하면 한국에서 발급받은 전자주민증, 전자증명서 등을 해외에서도 활용이 가능하다. 이는 플라스틱 형태의 신분증과 수첩 형태인 여권 등을 대체할 수 있으며 비용 절감 효과가 있다. 오프라인에서는 휴대폰만으로 물건 구매가 가능하다. 편의점과 같은 곳에서 물건 구매 시 모바일 페이로 결제를 하고, 성인 인증을 위한 신분증 제시에는 휴대폰에 VP를 QR코드로 제출함으로써 성인 여부만 제공하여 이름 나이 주소 등의 불필요한 개인정보 노출을 줄인다.

5. 결론

온라인 신분 확인 기술이 발전함에 따라 편리하면서 개인정보 노출을 최소화하고, 보안 위협을 낮출 필요성이 있다. 본 논문에서는 분산원장 기술을 바탕으로 하는 탈중앙화 신원증명 기반 본인 인증 모델을 제시하여 자기주권 신원증명을 실현하였다. 본인 인증 모델은 분산원장 기술과 Wallet App을 기본으로 한다. 신용카드를 휴대폰에서 사용하는 모바일 페이와 같이 신분증 역시 플라스틱 카드를 지갑에 가지고 다니는 것이 아닌 휴대폰에 저장하여 이용한다. 단순히 신분증을 휴대폰으로 옮기는 것이 아닌 분산원장에 DID를 등록한 뒤 휴대폰에서 필요할 때 마다 전자신분증을 꺼내 쓰는 DID 기반 자기주권 신원증명을 실현했다.

사용자의 신원증명서는 휴대폰에서 직접 발급하며, 생체인증 기술 기반으로 App에 접근한다. 발행기관을 통하여 전자주민증을 검증 및 등록하고 발행기관으로부터 발급받은 VC는 사용자가 필요한 정보만을 재가공하여 VP를 생성해 제출할 수 있으며 Proof 항목으로 소유권을 증명한다.

향후 연구에서 실제 구현을 위한 플랫폼 간에 호환성 문제 해결 및 신원증명을 기반한 표준화 작업에 대한 연구가 필요하다. 특히 지갑에 넣어 다니는 플라스틱 신분증을 분실하는 것은 사용자의 개인정보를 분실하는 것과 같으며, 휴대폰에 App에 저장된 개인키 분실은 개인정보를 분실하는 것이다. 따라서, 휴대폰에 저장된 개인키 관리에 관한 연구가 필요하다.

REFERENCES

[1] J. Fang, C. Yan & C. Yan. (2009). Centralized Identity Authentication Research Based on Management Application Platform. *First International Conference on Information Science and Engineering,* 2292-2295.

[2] D. Choi, S. Jin & H. Yoon. (2007). Trust Management for User-Centric Identity Management on the Internet. *IEEE International Symposium on Consumer Electronics,* 1-4.

[3] W. Li & C. J. Mitchell. (2020). User Access Privacy in OAuth 2.0 and OpenID Connect. *IEEE EuroS&PW.*
DOI : 10.1109/eurospw51379.2020.00095

[4] Y. Kortesniemi, D. Lagutin, T. Elo & N. Fotiou (2019). Improving the Privacy of IoT with Decentralised Identifiers (DIDs). *Journal of Computer Networks and Communications, 1-10.*
DOI : 10.1155/2019/8706760

[5] M. H. Rhie, K. H. Kim, D. Y. Hwang & K. H. Kim. (2021). Vulnerability Analysis of DID Document's Updating Process in the Decentralized Identifier Systems. *2021 International Conference on Information Networking (ICOIN),* 517-520.
DOI : 10.1109/icoin50884.2021.9334011

[6] Sovrin Protocol and Token White Paper. (2018). *Sovrin.* (Online). https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[7] What is self-sovereign identity. (2018). *Sovrin.* (Online). https://sovrin.org/faq/what-is-self-sovereign-identity

[8] GDPR. (2018). *General Data Protection Regulation.* (Online). https://gdpr.eu/tag/gdpr/

[9] M. Chisholm. (2018). *California Consumer Privacy Act of 2018 vs. GDPR.* (Online). https://www.firstsanfranciscopartners.com/blog/california-consumer-privacy-act-of-2018-vs-gdpr

[10] L. Determann. (2018). California Privacy Law : Practical Guide and Commentary U.U. Federal and California Law. *International Association of Privacy Professionals (IAPP).* (Online). https://iapp.org/media/pdf/publications/IAPP-California-Privacy-Law-2018-SAMPLE.pdf

[11] L. Determann. (2018). Analysis: *The California Consumer Privacy Act of 2018.* (Online). https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/

[12] J. K. Lee. (2020). Hyperledger Fabric Configuration and Channel Development Case Study for Google Cloud-based Distributed Ledger Processing. *Korean Association Of Computers And Accounting, 18(1),* 19-39.

[13] W. Y. Hwang & H. K. Kim. (2020). A Study on Implementation of BlockChain Voting System using Hyperledger Fabric. *Korea Information Electron Communication Technology, 13(4),* 298-305.

[14] Decentralized identity Foundation. (2019). *DIF.* (Online). https://identity.foundation

[15] W3C DID WG. (2019). *W3C.* (Online). https://www.w3.org/2019/did-wg

[16] C. Brunner, U. Gallersdorfer, F. Knirsch, D. Engel & F. Matthes. (2020). DID and VC: Untangling Decentralized Identifiers and Verifiable Credntials for the Web of Trust. *International Conference on Blockchain Technology and Applications (ICBTA 2020),* 61-66.
DOI : 10.1145/3446983.3446992

[17] S. R. Cho, Y. S. Cho & S. H. Kim. (2016). Introduction to FIDO 2.0 Universal Certification Technology. *Korea Institute Of Information Security And Cryptology, 26(2),* 14-19.

김 호 윤(Ho-Yoon Kim) [정회원]

· 2021년 2월 : 동명대학교 정보보호학과 (공학사)
· 2021년 3월 ~ 현재 : 동명대학교 컴퓨터미디어공학과 석사과정
· 관심 분야 : Blockchain, DID, 암호 프로토콜, IoT
· E-Mail : miask376@gmail.com

한 군 희(Kun-Hee Han) [종신회원]

· 2001년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수
· 관심분야 : 멀티미디어, 유비쿼터스, DB보안, 암호 프로토콜/알고리즘
· E-Mail : hankh@bu.ac.kr

신 승 수(Seung-Soo Shin) [정회원]

· 2001년 2월 : 충북대학교 수학과 (이학박사)
· 2004년 8월 : 충북대학교 컴퓨터공학과(공학박사)
· 2005년 3월 ~ 현재 : 동명대학교 소프트웨어융합보안학과 교수
· 관심 분야 : 암호 프로토콜, 네트워크 보안, 헬스 케어, IoT, Blockchain
· E-Mail : shinss@tu.ac.kr