https://doi.org/10.33778/kcsa.2024.24.2.141

자기주권 신원 보장을 위한 영지식증명 기반의 대학 내 DID 시스템 적용방안 연구★

임 성 식*, 김 서 연**, 김 동 우**, 한 수 진***, 이 기 찬***, 오 수 현****

요 약

최근 개인정보 유출에 대한 사고가 빈번하게 발생함에 따라 개인정보보호에 대한 관심이 높아지고 있다. 또한, 블록체인 기술의 등장과 함께 블록체인을 적용한 자기주권 신원 모델에 대한 관심이 높아지고 있으며, 이를 실현하기 위해 DID에 대한 연구도 꾸준히 이루어지고 있다. 하지만 대학 내 전산시스템은 수많은 개인정보 등의 주요 정보를 저장하고 활용하지만, 중앙화된 정보시스템을 기반으로 운영 및 관리되고 있으며, 이에 따른 개인정보 유출 사고사례도 매년 발생하고 있다. 따라서 본 논문에서는 대학 내 적용 가능한 DID 기반의 전산시스템을 제안하고 이를 구현한다. 또한, 대학 내에서의 대표적인 서비스를 설정하고 구현 시스템에서 수행한다. 제안하는 시스템은 영지식증명을 기반으로 사용자의 자기주권 신원을 보장할 수 있으며, 기존의 중앙화된 시스템에서 벗어나 안전한 대학 내 통합정보시스템을 구성할 수 있다.

Study on the Application of a Decentralized Identity System within University Based on Zero-Knowledge Proof for Self-Sovereign Identity Assurance

Im Sung Sik*, Kim Seo Yeon**, Kim Dong Woo**,
Han Su Jin***, Lee Ki Chan***, Oh Soo Hyun****

ABSTRACT

With the increasing frequency of incidents related to personal information leaks, there is a growing concern about personal information protection. Moreover, with the emergence of blockchain technology, there is a heightened interest in self-sovereign identity models applied through blockchain, with ongoing research on Decentralized Identifiers (DID) to achieve this. However, despite universities storing and utilizing significant information such as personal data, their computer systems are operated and managed based on centralized systems, leading to annual occurrences of personal data breaches. Therefore, this paper proposes and implements a DID-based computing system applicable within universities. Additionally, it establishes and executes prominent services within the university context. The proposed system ensures users' self-sovereign identities through verifiable credentials, enabling the establishment of a secure integrated information system within the university, departing from traditional centralized systems.

Key words : Decentralized Identity(DID), Zero-Knowledge Proof(ZKP), Self Sovereign Identity(SSI)

접수일(2024년 01월 29일), 수정일(1차: 2024년 02월 14일), (2차: 2024년 02월 28일), 게재확정일(2024년 03월 08일)
★ 본 연구는 과학기술정보통신부와 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음

* 호서대학교 정보보호학과 석사과정(주저자)
** 호서대학교 정보보호학과 석사과정(공동저자)
*** 호서대학교 컴퓨터공학부 학부생(공동저자)
**** 호서대학교 컴퓨터공학부 교수(교신저자)

1. 서 론

대학을 포함한 대부분의 교육기관에서는 관련 행정 업무를 수행함에 있어 학생 및 교직원들의 개인정보를 포함한 다양한 정보들을 활용하게 되며, 이러한 과정은 주로 중앙 서버 및 시스템을 통해 이루어지게 된다. 이처럼 중앙화된 종합정보시스템을 기반으로 운영 및 관리되는 교내 전산시스템으로 인해 개인정보 유출에 대한 여러 가지 위험 요소들이 존재한다. 실제로 대학 내 개인정보 유출 사고사례는 매년 발생하고 있으며, 최근에는 4만 6천여 명의 개인정보 유출 사고가 발생하였다[1].

개인정보 유출 사고는 국내뿐만 아니라 해외에서도 빈번하게 발생하고 있으며, 이에 따라 개인정보보호에 대한 관심이 높아지고 각종 사고에 대응하기 위한 많은 연구가 이루어지고 있다. 사토시 나카모토가 논문[2]에서 처음 제안한 비트코인과 블록체인 기술이 주목받기 시작하면서 개인정보보호를 위해 블록체인 기술을 적용한 자기주권 신원(Self Sovereign Identity, SSI) 모델에 대한 관심이 높아지고 있으며, 이러한 자기주권 신원 모델을 실현하기 위한 기술로서 분산 ID(Decentralized Identity, DID)가 주목받고 있다.

이러한 분산 ID는 모바일 운전면허증 서비스를 포함하여 금융권과 공공분야 등 다양한 분야에서 활용되고 있다. 또한, 대학과 같은 교내 환경에 분산 ID 기반의 신원증명 시스템을 적용하여 제증명 발급 및 검증과 같은 서비스의 복잡한 절차를 간소화하고 비용을 절약할 수 있으며, 보안성을 강화할 수 있다. 이러한 이점에도 불구하고, 국내 몇몇 대학에서만 일부 시스템에 부분적으로 분산 ID를 적용하고 있다[3].

따라서 본 논문에서는 중앙화된 교내 전산시스템의 문제를 해결하기 위해 영지식증명(Zero Knowledge Proof, ZKP)이 적용된 자기주권 신원을 보장하는 대학 내 분산 ID 시스템을 제안한다. 본 논문의 구성으로 2장에서는 DID 표준 및 활용사례와 영지식증명에 대해 정리한다. 3장에서는 영지식증명 기반의 대학 내 DID 시스템을 제안하고 구현 및 활용방안을 제시한다. 4장에서는 보안 요구사항에 따른 제안하는 시스템의 안전성을 분석하고 기존 DID 시스템과 비교하며, 마지막으로 5장에서는 결론을 기술한다.

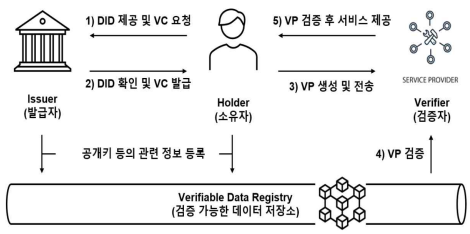
2. 관련연구

2.1 DID

2.1.1 DID 표준

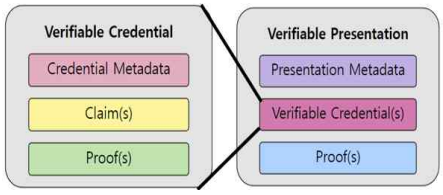
DID는 기존의 중앙화된 신원인증 문제점을 개선하기 위해 블록체인 기술을 이용하여 탈중앙화된 환경에서의 신원인증이 가능하게 한다. 웹 표준화 단체인 World Wide Web Consortium(W3C)에서는 DID에 대한 표준(Decentralized Identifiers, DIDs)[4]과 검증 가능한 자격증명(Verifiable Credentials, VC)에 대한 표준[5]을 제정하고 있으며, Decentralized Identity Foundation(DIF)에서는 DID를 이용한 인증 방법인 DID Auth에 대한 표준화를 진행하고 있다. 국내에서는 금융보안원에서 '분산ID를 활용한 신원관리 프레임워크'[6,7]를 개발하였고, 이는 2020년 12월 한국정보통신기술협회(TTA) 표준으로 채택되었다.

W3C의 DIDs 표준과 Verifiable Credentials Data Model 표준에서는 DID 구성 모델을 (그림 1)과 같이 제시하고 있다.



(그림 1) DID 구성 모델

Issuer(발급자)는 사용자의 신원정보를 인증하고 발급하는 주체로, 제출된 Claim(정보)을 사용하여 사용자의 신원정보인 VC를 발급한다. Holder(소유자)는 Issuer로부터 VC를 발급받고 소유하고 있는 주체이며, 해당 VC를 기반으로 검증 가능한 프레젠테이션(Verifiable Presentation, VP)을 생성하고 필요시 Verifier(검증자)에 제출한다. Verifier는 Holder가 제출한 VP를 검증하게 되며, Verifiable Data Registry (검증 가능한 데이터 저장소)는 데이터베이스, 분산 장부 등의 여러 가지 저장소 형태로 존재하여 검증을 위한 각종 키나 식별자를 저장한다.



(그림 2) VC 및 VP 구조

2.1.2 DID 활용사례

2.1.2.1 COOV

질병관리청에서 개발한 COOV[8]는 세계 최초의 블록체인 기반 코로나19 예방 접종 인증 시스템으로, 블록체인랩스에서 세계 최초로 개발한 가상화폐 없는 퍼블릭 블록체인인 InfraBlockchain을 기반으로 한다. COOV는 백신 접종에 대한 디지털 증명서를 상대방에게 제출할 수 있으며, 상대방의 증명서를 QR 스캔을 통해 검증할 수 있다. 또한, COOV는 코로나19 예방 접종 증명뿐만 아니라 본인 인증을 비롯한 다양한 인증 시스템으로도 활용되고 있다.

2.1.2.2 띠딧

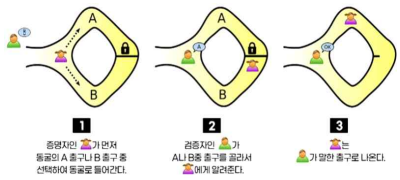
띠딧[9]은 2022년 12월, LG CNS에서 블록체인 DID 기술을 적용한 모바일 구독형 신원인증 서비스이며, 자사 임직원의 모바일 사원증에 띠딧을 적용하여 구현했다. 기업은 별도의 신원인증 앱을 개발할 필요 없이, 띠딧을 활용해 모바일 사원증과 같은 서비스를 운영 및 관리할 수 있다. 또한, 모바일 사원증 외에도 발급 기관의 상황에 따라 제증명 발급 서비스가 가능하며, 출입 단말기 태깅 및 편의시설 단말과의 연계도 가능하다.

2.1.2.3 Initial

SKT에서 블록체인 DID 기술을 기반으로 출시한 Initial[10]은 사용자가 본인의 단말기에 다양한 증명서를 발급 및 저장, 제출하는 서비스이다. 신원 증명 발급, 증명서 보관함, 공공부문 전자증명서 발급 등의 기능을 제공하며, 최근에는 고려대학교에 KU Mobile ID로 모바일 신분증 및 제증명 서비스 등을 제공하고 있다. 또한, 디지털 혁신공유대학 교육과정을 지원하는 대학 중 일부에 해당 서비스를 지원하고 있으며 향후 혁신공유대학 사업단 전체로 확장 예정이다.

2.2 Zero Knowledge Proof

영지식증명(ZKP)은 특정 비밀정보를 공개하지 않으면서 정보를 알고 있음과 정보의 유효성을 증명할 수 있는 기술이며, 크게 대화형 영지식증명과 비대화형 영지식증명으로 분류된다. 주로 (그림 3)과 같이 'The Ali Baba Cave'라는 예시로 설명되는 대화형 영지식증명은 정보의 유효성 증명의 결과 확률을 높이기 위해 다수의 메시지 교환을 수행한다. 이는 시스템 결과의 안전성을 높이지만, 다수의 메시지 교환으로 인해 효율성이 떨어지는 한계가 있다.



(그림 3) 'The Ali Baba Cave'

비대화형 영지식증명에서는 반복적인 메시지 교환 과정 없이 한 번의 메시지 교환을 통해 증명이 이루어진다. 대표적인 비대화형 영지식증명 기술에는 zk-SNARKs, zk-STARKs와 함께 CL-Signature, BBS+ Signature 등이 있다.

DID 시스템에서는 정보 주체의 주권을 보장하기 위해 영지식증명을 통한 선택적 증명 및 범위 증명이 가능하게 한다. W3C 표준에 명시된 CL-Signature는 RSA 암호체계를 기반으로 하지만, BBS+ Signature는 타원곡선 암호체계를 기반으로 한다. BBS+ Signature는 <표 1>[11]과 같이 연산 수행 속도와 키 길이 등의 요소에서 더 효율적인 성능을 보여준다.

<표 1> CL-Signature과 BBS+ Signature 비교

	CL Signature	BBS+ Signature
키 생성 속도	8800 ms	2.69 ms
서명 생성 속도	93 ms	1.43 ms
proof 생성/검증 속도	24 ms	10.22 ms
개인 키 크기	256 B	48 B
서명 크기	672 B	193 B

3. 제안하는 영지식증명 기반 대학 내 DID 시스템

3.1 시스템 구성

본 장에서는 (그림 4)와 같이 응용 환경을 대학 내로 구성한 자기 주권 신원이 보장된 분산 ID 시스템을 구성하고, 동작 가능한 시나리오를 고려하여 설계 및 구현한다. 학교는 Issuer로서 Holder의 신원을 확인하고, 각종 증명서 및 모바일 신분증을 발급한다. Holder는 발급받은 증명서 및 신분증을 교내·외의 Verifier에 제출하여 자신의 정보에 대한 유효성을 검증받고, 필요한 서비스를 제공받는다. 또한, 영지식증명 기술을 적용하여 Holder의 선택적 증명 및 범위 증명 등을 가능하게 함으로써 사용자의 데이터 주권을 보장한다.

제안하는 영지식증명 기반 대학 내 DID 시스템은 Hyperledger Foundation의 Hyperledger Indy[12], Aries[13] 프로젝트를 활용하여 구현한다. Indy 프로젝트에서는 개체를 Trustee, Steward, Node, Endorser, User 총 다섯 가지로 <표 2>와 같이 정의한다.

<표 2> Hyperledger Indy의 그룹별 역할

그룹	역할
Trustee	최상위 권한을 가지는 최초의 구성원
Steward	노드 운영 권한(Node 권한 부여, 분산 원장 초기화 등)을 가진 그룹
Endorser	원장에 트랜잭션 작성이 가능한 그룹
Node	분산 원장 네트워크의 유지를 위해 합의 알고리즘을 동작하는 개체
User	읽는 권한을 가진 일반 사용자

Trustee는 개인 또는 그룹일 수 있으며, 제안하는 시스템에서는 시스템 관리자가 해당 역할을 맡아 초기 구성을 진행한다. 또한, Steward와 함께 분산 원장 네트워크 관리를 수행할 수 있다.

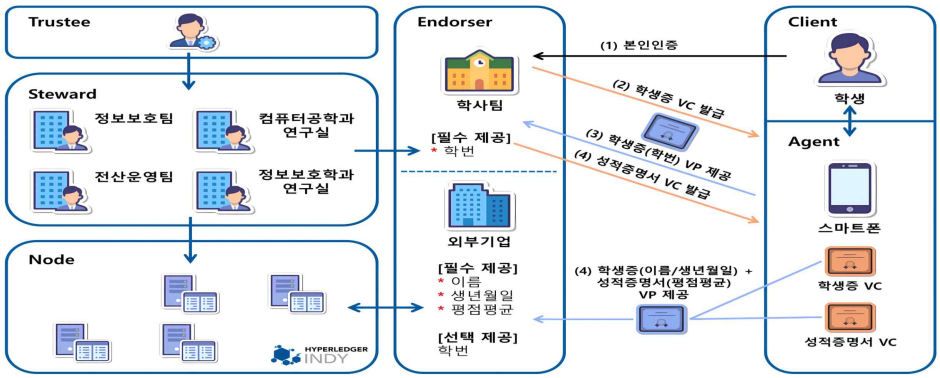
Steward는 Node를 직접 운용하거나 다른 개체에 의해 운용되는 Node에 권한을 부여하여 분산 원장 네트워크를 유지할 수 있다. 제안하는 시스템에서 Steward는 Node를 직접 운용하는 개체로 가정하였으며, 이에 따라 Node의 이상 발생 시 이를 대처할 수 있는 네트워크 기반 지식이 있는 컴퓨터 관련 연구실, 전산팀 등의 그룹이나 개인으로 구성하였다.

Node는 합의 알고리즘을 통해 분산 원장 내의 데이터를 합의하여 무결성을 보장한다. 또한, DID 식별자를 기반으로 학생의 신원정보나 성적 등 생성된 VC의 정보를 검증할 수 있는 데이터를 유지한다.

Endorser는 User와 상호작용을 통해 VC를 발급하거나 전달받은 VP를 검증하는 개체이며, 제안하는 시스템에서는 교내 학사팀과 외부 기업으로 구성하였다.

User는 Endorser와 상호작용을 통해 해당 시스템 내에서 서비스를 이용하는 개체이다. 제안하는 시스템에서는 학생으로 가정되며, 스마트폰 애플리케이션을 통해 Endorser와 상호작용을 수행한다.

Hyperledger Aries는 DID Auth에 기반한 VC 발급, VP 검증 등의 프로세스를 API를 통해 제공하고, DID Comm에 기반하여 신뢰할 수 있는 P2P 통신을 지원하는 프로젝트이다. 제안하는 시스템에서는 Aries를 통해 신원 증명 등의 프로세스를 구현하며, 테스트용 사용자 인터페이스 등 다양한 도구를 제공한다.



(그림 4) 제안하는 영지식증명 기반 대학 내 DID 시스템

3.2 구현 시스템 및 구성 요소별 기능

제안하는 시스템의 구현 과정에서 Trustee는 분산 원장의 초기 구성을 위해 indy-node 및 indy-sdk 라이브러리를 활용하여 웹 서버를 구축한다. 해당 웹 서버는 Python의 Flask 모듈을 사용해 구동되며 CSS 및 HTML을 통해 사용자 인터페이스를 제공한다.

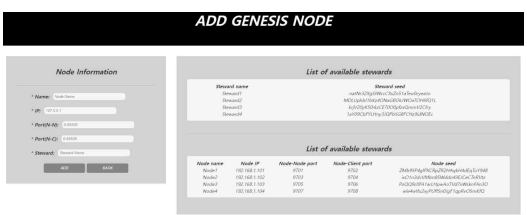
Steward는 bcgov의 von-network[14]를 활용하여 구현되며, Indy 네트워크 내의 모든 참여자가 분산 원장의 내용을 탐색할 수 있도록 Ledger Browser를 구현하고 운영한다. 해당 Ledger Browser를 활용하기 위해서는 분산 원장이 유지되고 있어야 한다. 이를 위해 Node는 indy-node 라이브러리를 통해 구현하며, 제안하는 시스템에서는 네 개의 노드가 상호 작용하여 해당 분산 원장을 유지하고 운영한다.

Endorser는 Hyperledger Aries 프로젝트에서 제공하는 'Hyperledger Aries Cloud Agent - Python' 및 'aries-acapy-plugin-toolbox', 'aries-toolbox'를 활용하여 VC를 발급하거나 VP를 검증하는 Endorser 개체를 구현한다. User는 오픈소스 디지털 지갑 애플리케이션인 'Trinsic Wallet'을 통해 서비스를 이용한다.

3.2.1 Trustee

Trustee는 Indy 네트워크를 구동하기 위해 Pool Transaction과 Domain Transaction에 대한 Genesis 파일을 생성해야 한다. 또한 Trustee는 해당 파일을 구성하고 네트워크에 참가할 개체에 배포해야 한다.

웹 인터페이스를 통해 각 Genesis 파일을 구성하기 위해서는 Steward 역할을 부여해야 한다. Steward를 추가하면 각 Steward는 서명 및 검증을 위한 Key 값의 재료인 Seed 값을 부여받는다. Steward 생성이 완료되었으면, 생성된 Steward는 각 Node에 (그림 5)와 같이 권한을 부여한다.



(그림 5) Node 생성 페이지

각 Node는 식별되는 Node IP, Node-Node 사이에서 사용할 Port 번호, Node-Client 사이에서 사용할 Port 번호를 지정해야 한다. 이후 Steward와 같이 각 Node 별 Seed 값이 생성되며, 각 Node는 해당 Seed 값으로 DID와 Key를 생성한 후 해당 Key로 상호 통신을 수행한다.

Node 권한 부여가 마무리되면, Trustee는 해당 정보를 가지고 Genesis 파일을 구성 및 생성하며, 생성된 파일을 배포한다. 구현한 시스템에서는 WebDAV 서버를 구현하여 각 개체에 해당 파일을 배포한다.

3.2.2 Steward

Steward는 분산 원장 네트워크 참여자에게 원장의 탐색을 지원하기 위해 웹 애플리케이션을 적용하고 운용해야 한다. 구현한 시스템에서는 von-network를 활용하여 (그림 6)과 같은 Ledger Browser를 구축하였다. Ledger Browser를 통해 네트워크 참가자는 누구나 분산 원장에서 유지되고 있는 데이터를 확인할 수 있으며, Endorser의 경우 해당 웹에서 자신의 디지털 지갑에 대한 Seed를 등록함으로써 네트워크에 참여할 권한을 부여받을 수 있다.

(그림 6) Ledger Browser

3.2.3 Node

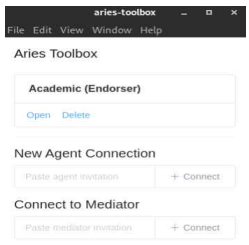
Node는 Steward로부터 역할을 부여받고 대응되는 Seed를 통해 자신의 DID와 Key 값을 생성한다. 이후 Node는 Trustee로부터 Transactions Genesis 파일들을 배포 받는다. 각 Node는 해당 파일을 기반으로 Indy 네트워크에서 합의 알고리즘을 통해 원장을 유지한다.

구동 중인 Node는 Pool Transactions Genesis 파일에 존재하는 다른 Node와 주기적으로 통신하면서

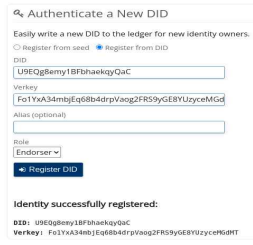
Transaction이 발생하면 Node 간 합의를 통해 해당 데이터를 원장에 기록하는 역할을 한다.

3.2.4 Endorser

Endorser는 Trustee, Steward의 허가를 통해 원장에 Transaction 작성이 가능하며, Aries Toolbox를 통해 User와 통신하면서 VC를 발급한다. Aries Toolbox는 시스템 관리자를 위한 도구로써 (그림 7)과 같이 다른 Endorser, User와의 통신을 위한 사용자 인터페이스를 제공한다. 먼저 학사팀(Endorser)은 (그림 8)과 같이 자신의 DID와 Verkey를 원장에 등록하여 Endorser 권한을 얻는다. 이후 Invitations를 생성하여 자신이 연결할 학생에게 QR코드 초대장을 제공하고, 이를 통해 연결이 확립되면 연결된 학생들을 관리할 수 있게 된다. 해당 과정을 완료한 학사팀은 Endorser로서의 서비스 준비를 마치게 된다.



(그림 7) Aries Toolbox



(그림 8) 원장에 등록한 학사팀 DID

3.2.5 User

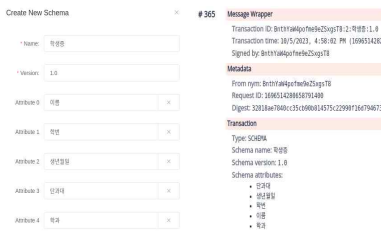
제안하는 시스템에서 학생 그룹에 해당하는 User는 Endorser에게 VC를 발급받고, 이후 해당 VC를 통해 VP를 생성하여 검증받고자 하는 곳에 제출하는 방식으로 동작한다. User는 Endorser와의 통신을 위해 오픈소스 디지털 지갑 애플리케이션인 'Trinsic Wallet'을 사용한다. 'Trinsic Wallet'은 DID 네트워크상의 User를 위한 디지털 지갑이며, User의 디지털 자격 증명을 수신, 저장 및 검증받을 수 있다.

User(학생)는 초기에 학사팀(Endorser)과 동일한 원장의 Genesis 파일을 애플리케이션에 등록한 뒤 초대장을 통해 학사팀과의 연결을 확립한다. 또한, 해당 애플리케이션을 통해 자신과 연결된 Connections를 관리할 수 있다. 제안하는 시스템에서는 학생이 학사팀에게 학생증, 성적증명서 등의 각종 교내 증명서를 발급받고, 외부 기업에게 해당 VC에 대한 VP를 만들어 구직 신청 시 검증받는 과정을 수행한다.

3.3 시스템 동작 시나리오

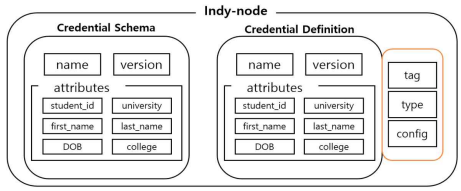
3.3.1 초기 학생증 VC 발급

학사팀은 해당 학생증 VC 발급을 위해 Credential Schema를 (그림 9)와 같이 생성하여 원장에 등록한다.



(그림 9) 학생증 Credential Schema 생성

이후 학사팀은 (그림 10)과 같이 서명 유형, 구성 등의 정보인 tag, type, config 정보를 추가하여 실제 발급에 사용되는 Credential Definition을 생성한다. 이는 동일한 Schema를 통해 다른 용도 및 타 기관에서 VC를 발급할 시에 구분하기 위한 용도로 존재한다.



(그림 10) Credential Definition

학사팀은 교내 데이터베이스 내에 있는 정보를 활용하여 자신의 Connections 목록에 있는 학생에 대해 학생증 Credential Definition 정보를 기입하고, 학생증 VC Offer를 보내게 된다. 학생이 해당 Offer를 수락하면 최종적으로 (그림 11)과 같이 자신의 지갑에 학생증 VC를 저장하게 된다.

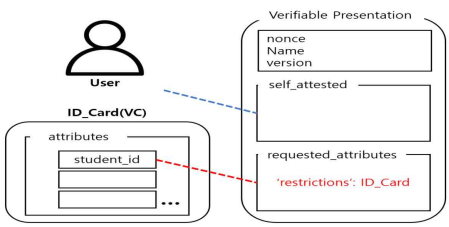
(그림 11) 발급받은 학생증 VC

3.3.2 단일 VC를 통한 VP 생성 및 검증

학생은 각종 교내 증명서를 발급받고자 할 때 초기에 발급받은 학생증 VC를 활용한다. 학사팀은 각종 교내 증명서 발급을 위해 Credential Schema, Credential Definition을 학생증 생성과 같은 과정으로 생성한다.

학생이 학사팀에게 성적증명서 발급을 요청하게 되면, 학사팀은 성적증명서 발급을 위해 학생의 학생증 VC를 검증하는 Proof Request를 생성하여 학생에게 발송한다. Proof Request는 User가 실제 해당하는 VC를 소유하고 있는지, 조건에 맞는 VC인지를 확인하기 위한 절차로, Proof Request를 받은 User는 본인이 소유한 VC를 통해 VP를 생성하여 전송하게 된다.

VP 생성 시 'self_attested'는 본인이 스스로 입력하는 항목이며, 'requested_attributes'에는 Verifier가 지정한 VC에 해당하는 요소들을 입력해야 한다. VP 값에 들어갈 요소 중 학번에 대해 학사팀은 'restrictions' 조건을 설정한다. 해당 조건이 설정된 항목은 정해진 VC에 포함된 값을 통해서만 기입할 수 있다. 해당 Proof Request를 받은 학생은 (그림 12)와 같이 학생증 VC를 활용하여 성적증명서 인증용 VP를 생성한 뒤 검증받는다.



(그림 12) 학생증 VC를 활용한 VP 생성

검증을 마친 학생은 (그림 13)과 같이 학생증 발급 절차와 마찬가지로 성적증명서를 발급받고 자신의 디지털 지갑에 저장하게 된다.

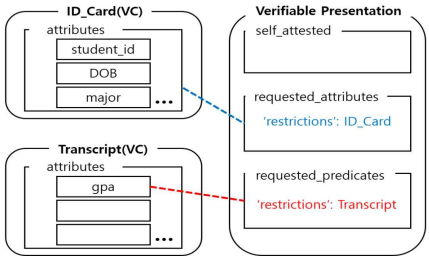
(그림 13) 발급받은 성적증명서 VC

따라서 학생은 초기에 학생증 VC를 발급받은 뒤, 해당 VC를 통해 자신을 검증하여 각종 교내 증명서 VC를 발급받을 수 있다. 이와 같이 DID 시스템을 도입한다면, 개인정보를 서류를 통해 관리하지 않고 자신의 디지털 지갑에서 안전하게 제출, 관리 및 검증할 수 있다.

3.3.3 다중 VC를 통한 VP 생성 및 검증

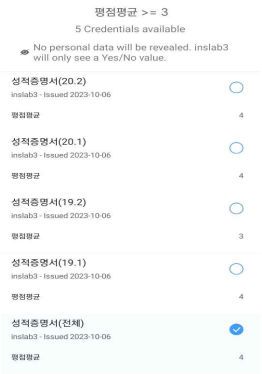
학생은 외부 기업에 구직 신청을 위해 발급받은 학생증 및 성적증명서 VC를 활용할 수 있다. 해당 외부 기업은 지원자의 성적증명서 VC를 통해 신청 자격을 최소 평균 평점 3.0 이상으로 제한하고, 학생증 VC를 통해 학번, 생년월일, 학과 등의 정보를 제공받고자 한다.

기본적인 검증 구조는 학사팀의 성적증명서 발급 시 검증 과정과 동일하지만, 성적 제한 조건을 위해 해당 Proof Request에는 (그림 14)와 같이 새로운 속성인 'requested_predicates'가 추가된다. 해당 속성을 통해 속성값을 실제로 확인하지 않고, 해당 값이 기준 이상인지 이하인지를 판단할 수 있다.



(그림 14) 학생증 및 성적증명서 VC를 활용한 VP 생성

해당 과정을 통해 본 논문에서 제안하는 DID 시스템이 교내 환경에 제한되는 것이 아니라, 외부 기관 및 단체와 연계 가능하고, 학생이 보유한 다수의 VC를 선택적으로 조합하여 VP를 생성하는 것이 가능함을 보여준다. 또한, (그림 15,16)과 같이 학생은 외부에 자신의 개인정보를 공개하지 않고 해당 속성에 대한 선택적 증명을 수행할 수 있다.



(그림 15) 학생의 평점 검증 과정

(그림 16) 외부 기업의 검증 결과

4. 제안하는 시스템의 안전성 분석

4.1 제안하는 시스템의 보안 요구사항 분석

금융보안원의 '분산ID를 활용한 신원관리 프레임워크 - 제3부 정보보호 요구사항'[15]은 <표 3>과 같이 보안 영역별로 보안 요구사항을 정의한다.

거버넌스 보안 영역에서는 관리 기능 및 악의적 참여자, 상호 연동 상황에 대한 보안 위협을 고려한다. 제안하는 시스템에서는 Trustee가 전체 시스템 관리자로서 보안상·운영상 정책을 수립 및 관리하며 정책에 따라 시스템을 운영한다. 또한, Endorser 및 User는 Steward 및 Trustee로부터 참여자에 대한 인증이 이루어진 후 시스템에 참여할 수 있는 권한이 부여된다.

서비스 보안 영역에서는 참여자 및 전자지갑에 대한 보안 위협과 신원 증명 과정에서의 보안 위협을 고려한다. 제안하는 시스템의 Endorser 및 User와 같은 모든 참여자는 Trustee 및 Steward로부터 참여자 인증이 이루어진 뒤 권한이 부여된다. 또한, 전자지갑으로 사용되는 'Trinsic Wallet'은 W3C의 DID 및 VC 표준과 DIF / Aries의 DIDComm 표준을 기반으로 하며, TLS 및 CurveZMQ(Curve ZeroMQ)를 통해 기밀성 및 무결성을 보장하는 암호화된 통신을 지원한다.

보안 연결 영역에서는 유출 및 위·변조, 취약한 암호 알고리즘, 키 관리, 중간자 공격, 도청, 재전송 공격에 대한 보안 위협을 고려한다. 제안하는 시스템을 구성하는 HyperLedger Indy에서는 ECDH 기반의 키 합의 알고리즘, AES-CBC 및 AES-GCM 기반의 암호 알고리즘과 ECDSA, EdDSA CL-Signature, BBS+ Signature 기반의 서명 알고리즘을 사용한다.

<표 3> 정의된 보안 요구사항에 따른 제안하는 시스템의 안전성 분석

보안 영역	보안 요구사항	만족 여부	비고
거버넌스 보안	보안·운영 정책 수립 및 관리	O	Trustee의 관리 및 정책 수립, 운영
	참여자 관리	O	Steward 및 Trustee의 인증 후 권한 부여
	상호연동 보안	△	타 도메인 및 DID 프레임워크와의 연동 고려 필요
서비스 보안	참여자 인증 및 신원보호	O	Steward 및 Trustee의 인증 후 권한 부여
	전자지갑 보안	O	Trinsic Wallet의 암호화된 통신 지원
	신원 증명 시 보안	△	신원 증명 키 관리 및 저장 방안 고려 필요
보안 연결	기밀성 및 무결성	O	AES-CBC, AES-GCM 기반 암호 알고리즘 사용
	안전한 암호 알고리즘 사용	O	ECDSA, CL-Signature 등의 서명 알고리즘 사용
	통신망 암호화, 재전송 공격 차단	O	TLS 1.3 및 CurveZMQ 기반 암호화된 통신

4.2 기존 인증시스템과의 비교

기존의 신원인증 시스템은 사용자의 신원정보를 중앙 데이터베이스 서버에 저장하며, 신원인증 서비스 이용 시 비밀번호를 통한 사용자 인증을 필요로 한다. 하지만 본 논문에서 제안하는 시스템은 사용자의 신원정보를 서버에 저장하지 않고, 신원정보의 유효성을 검증하기 위한 데이터와 이를 식별하기 위한 분산 ID를 Indy 네트워크에 저장한다. 사용자는 자신의 신원정보를 개인 기기에 안전하게 보관하고 이를 선택적으로 활용하여 필요 서비스를 이용할 수 있다. 검증자는 Indy 네트워크에 저장된 사용자의 분산 ID를 통해 신원 검증 데이터를 식별하고, 해당 데이터를 통해 사용자의 신원을 검증한다. 이러한 시스템은 사용자의 개인정보 유출 위험을 최소화하며, 영지식증명을 통해 사용자가 자신의 데이터를 공개하지 않으면서도 신원을 효과적으로 증명할 수 있게 한다. 또한, 비밀번호 기반의 사용자 인증이 필요하지 않기 때문에 비밀번호 유출로 인한 2차 피해를 방지할 수 있다.

5. 결 론

중앙화된 교내 전산 및 정보시스템은 개인정보 유출에 대한 여러 위험 요소가 항상 존재하며, 실제로 매년 대학교에서의 개인정보 유출 사고사례가 지속해서 발생하고 있다. 따라서 본 논문에서는 DID 표준을 분석하고, 영지식증명을 적용하여 자기주권 신원을 보장하는 대학 내 DID 시스템을 제안한다.

제안하는 시스템은 대학 내 환경에 맞춰 개체를 구성하고, 구성 개체별 최소 권한 및 기능을 부여한다. 또한, Hyperledger Indy 및 Hyperledger Aries 등을 기반으로 제안하는 시스템을 구현하였으며, 대학 내에서 대표적으로 발생할 수 있는 3가지의 시나리오를 설정하여 구현한 시스템에서 수행하였다. 해당 시스템은 필요한 Credential에 대한 추가 및 수정이 용이하여 향후 대학별로 제공하는 여러 교내 서비스를 환경에 맞춰 추가할 수 있으며, 기존의 중앙화된 시스템에서 벗어나 안전한 대학 내 통합정보시스템 구성 및 운영에 이바지할 것으로 기대된다.

참고문헌

[1] 김영명, “경북대, 4만6,000여명 개인정보 유출 사고 발생... 재학생 2명 소행”, 보안뉴스, 2022.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, www.bitcoin.org, 2008.

[3] 윤원석, “DID기반 대학교 개인정보 보호의 필요성”, 차세대컨버전스정보서비스기술논문지, 제10권, 제1호, pp.33-43, 2021.

[4] Manu Sporny, et al., “Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations”, W3C, https://www.w3.org/TR/did-core/, 2022.

[5] Manu Sporny, et al., “Verifiable Credentials Data Model v1.1”, W3C, https://www.w3.org/TR/vc-data-model/, 2022.

[6] 김지훈, “분산 ID를 활용한 신원관리 프레임워크 - 제 1부 프레임워크 구성 및 모델”, 한국정보통신기술협회, 2020.

[7] 김지훈, “분산 ID를 활용한 신원관리 프레임워크 - 제 2부 신원증명 및 상호연동 방법”, 한국정보통신기술협회, 2020.

[8] 정우진, “COOV Mobile Vaccination Certificate”, 질병관리청, 2021.

[9] 띠딧, “띠딧 브로슈어”, LG CNS, 2023

[10] Initial, “initial 서비스 소개”, SKTl, 2022

[11] A. Guggino, “Privacy-Preserving Credentials for Self-Sovereign Identity with BBS+ Signatures”, POLITECNICO DI TORINO, Master Degree Thesis, 2022.

[12] Tracy Kuhrt, “Hyperledger Indy”, Hyperledger Foundation, https://wiki.hyperledger.org/display/indy, 2023.

[13] David Huseby, “Hyperledger Aries”, Hyperledger Foundation, https://wiki.hyperledger.org/display/ARIES, 2024.

[14] Wade Barnes, “Von-network”, Government of British Columbia, https://github.com/bcgov/von-network, 2023.

[15] 김지훈, “분산 ID를 활용한 신원관리 프레임워크 - 제 3부 정보보호 요구사항”, 한국정보통신기술협회, 2020.

〔저자소개〕

임 성 식 (Sung-sik Im)
2023년 2월 호서대학교 컴퓨터공학부 학사
2023년 3월 ~ 현재 호서대학교 정보보호학과 석사과정
email : sungsik9797@gmail.com

김 서 연 (Seo-yeon Kim)
2023년 2월 호서대학교 컴퓨터공학부 학사
2023년 3월 ~ 현재 호서대학교 정보보호학과 석사과정
email : komtti@naver.com

김 동 우 (Dong-woo Kim)
2023년 2월 호서대학교 컴퓨터공학부 학사
2023년 3월 ~ 현재 호서대학교 정보보호학과 석사과정
email : penetrick0@gmail.com

한 수 진 (Su-jin Han)
2021년 3월 ~ 현재 호서대학교 컴퓨터공학부 학부과정
email : tnwls5875@naver.com

이 기 찬 (Ki-chan Lee)
2019년 3월 ~ 현재 호서대학교 컴퓨터공학부 학부과정
email : ohkatan2@gmail.com

오 수 현 (Soo-hyun Oh)
1998년 2월 성균관대학교 정보공학과 학사
2000년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사(공학석사)
2003년 8월 성균관대학교 전기전자 및 컴퓨터공학과 박사(공학박사)
2004년 3월~현재 호서대학교 컴퓨터공학부 교수
email : shoh@hoseo.edu