https://doi.org/10.33778/kcsa.2021.21.2.037

탈중앙화 신원증명을 이용한 출입통제 시스템의 설계 및 구현

이 상 근*, 김 도 형*, 정 순 기**

요 약

탈중앙화 신원증명(DID, Decentralized Identifier) 기술은 블록체인 기술을 이용하여 개인의 신원증명을 중앙시스템을 통하지 않고 개인이 소유한 정보를 통해 자신의 신원을 증명하는 기술이다. 본 논문에서는 탈중앙화 신원증명 기술을 이용한 출입통제 시스템을 제시하고자 한다. 탈중앙화 신원증명 기술을 이용한 출입통제 시스템(이하 DID 출입통제 시스템)은 사용자 자신의 스마트폰(모바일 사원증)에 저장되어 있는 본인의 정보를 통해 DID 블록체인 서버로부터 신원을 증명하고 증명된 신원이 출입통제 시스템에 등록된 사용자임을 확인되었을 때 출입을 할 수 있도록 구현된 시스템이다. 이를 통해 개인의 신원을 증명하기 위한 정보를 출입통제 시스템에 저장할 필요 없이 스마트폰(모바일 사원증)과 DID 블록체인 서버와의 신원증명 확인만으로 출입통제를 관리할 수 있다.

Design and implementation of access control systems using decentralized identifier technology

Sang-Geun Lee*, Do-Hyeong Kim*, Soon-Ki Jung**

ABSTRACT

Decentralized Identifier (DID) technology is a technology that uses blockchain technology to prove an individual's identity through information owned by the individual rather than through a central system. In this paper, we would like to present an access control system using decentralized identifier technology. The access control system using decentralized identifier technology (DID access control system) is a system that allows users to verify their identity from the DID blockchain server through their smartphone (mobile employee ID) and access when they are confirmed to be registered in the access control system. Through this, access control can be managed only by verifying identification with smartphones (mobile employee ID) and DID blockchain servers without having to store information to prove an individual's identity in the access control system.

Key words : Decentralized Identifier(DID), Blockchain, Access Control System

접수일(2021년 05월 29일), 수정일(2021년 06월 20일), 게재확정일(2021년 06월 25일)

* (주)대구은행 정보보호부
** 경북대학교 컴퓨터학부(교신저자)

1. 서 론

최근 블록체인 기술을 기반으로 한 탈중앙화 신원증명 기술이 다양한 분야에서 활용이 이루어 지고 있다. 탈중앙화 신원증명 (DID, Decentralized Identifier) 기술은 자기 주권 신원(SSI, Self-Sovereign Indentity)을 실현하기 위해 자신의 아이디의 주권자가 되어 중앙기관에 아이디를 등록하지 않고 자신에 대한 정보를 스스로 통제할 수 있도록 하는 기술이다.[1] DID 기술을 이용하면 신원증명을 중앙집중형 서비스에 의존하지 않아도 되기 때문에 서버의 해킹 등에 의한 정보유출의 위험에서 안전해 질 수 있다.

DID 기술은 본인의 신원증명을 할 수 있는 다양한 분야에 활용할 수 있다. 각종 공공기관 제공 서비스, 금융서비스, 인터넷 서비스, 각종 증명서 발급 등 본인증명을 통해 활용할 수 있는 모든 서비스 영역에 활용되어 질 수 있다. 금융회사의 경우 금융결제원을 중심으로 비대면 실명확인 및 모바일 신분증에 DID 기술을 이용한 분산 ID 활용을 확대하고 있다.[2]

본 논문에서는 DID 기술을 이용하여 출입통제 시스템을 설계하고 구현한다. 제2장 관련 연구에서는 DID 기술 및 출입통제 시스템에 대해 살펴보고, 제3장에서는 NFC 출입통제시스템에 DID 기술을 접목한 탈중앙화 신원증명(DID) 출입통제 시스템을 설계하고 구현한다. 제4장에서는 본 시스템의 평가 및 기존 시스템과 비교를 하고, 제5장에서는 본 시스템의 효과성을 분석하고 결론을 맺는다.

2. 관련 연구

2.1 신원증명 기술

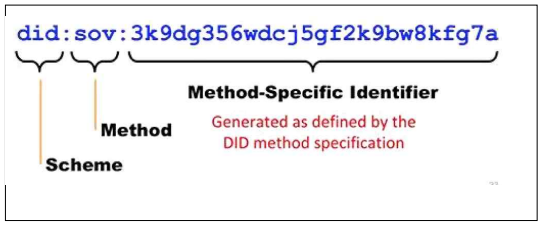
신원증명 기술은 개인의 신상 또는 신원정보를 증명하는 기술이다. 신원을 확인하는 방법에는 오프라인에서 신분증을 확인하는 절차와 같은 방식에서부터 여러 가지 온라인 기술을 사용하여 사용자를 확인하는 방식이 있다. 온라인 기술을 이용하는 대표적인 방식으로 공인인증서가 있다. 최근에는 공인인증서의 여러 가지 불편함을 해결하고자 DID 블록체인, 생체인증 등 새로운 기술을 이용한 신원증명 기술이 개발 및 표준화되고 있다.[12]

2.2 DID(Decentralized Identifier) 기술

DID란 원격에 있는 상대방을 식별하기 위해 사용되는 Indentifier를 블록체인에 기록하여 중앙화된 인증기관 없이도 식별 가능하게 하는 규약이다. DID는 DID의 주체와 관련된 URL로써, DID Document를 통해, 해당 주체와 신뢰할 수 있는 상호작용을 할 수 있다.[3]

2.2.1 DID 구성

DID는 URI 체계로 3가지 부분으로 구성 되어 있다. (그림 1)과 같이 “Scheme:Method:Specific-Identifier”로 되어 있으며, Scheme는 DID 체계를 의미하여 Method에 따라 서로 다른 방식의 네트워크에 기록이 된다. Specific-Identifier를 통해 유일한 식별 특징을 가지고 있다. [1]



(그림 1) DID(Decentralized Identifier) 형식[4]

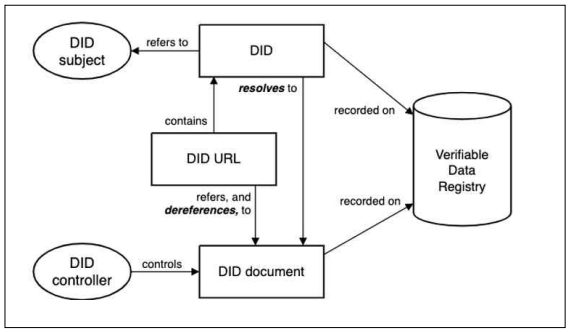
각 Method에 따라 DID Document를 관리하는 Registry가 운영되고 있으며, 많이 사용되는 상위 몇 가지는 <표 1>과 같다.[3]

<표 1> DID Method[3]

Method	Network	Authors
did:brcr:	Bitcoin	Cristoper Allen, Ryan Grant, Kim Hamilton Duffy
did:erc725:	Ethereum	ERC-725 Alliance
did:sov:	Sovrin	Sovrin Foundation
did:ethr:	Ethereum	uPort
did:v1:	Veres One	Digital Bazzar

2.2.2 DID Architecture

DID는 (그림 2)와 같이 DID document, DID controller, DID method, DID resolver, DID subject 등으로 구성되어 있다.[1]



(그림 2) DID Architecture 구성요소[5]

Verifiable Data Registry는 DID의 공개키를 포함함 DID의 정보를 가지고 있는 DID Document를 저장하는 분산 원장이다. DID Document는 DID subject에 대한 정보들의 모음으로 subject가 자신을 인증하는데 사용할 수 있는 공개키와 같은 데이터를 포함하고 있다.[1] DID Document는 주로 JSON-LD(JavaScript Object Notation for Linked Data)로 작성되며 (그림 3)과 같은 형태이다.

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "service": [{
    // used to retrieve Verifiable Credentials associated with the DID
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

(그림 3) DID Document 예시[5]

각 항목은 다음과 같이 정의될 수 있다.[1][3]

(1) context : 동일한 DID 문서에서 작동하는 두 개의 소프트웨어 시스템이 서로 이해할 수 있는 용어와 프로토콜을 사용하도록 하기 위해 지정하는 항목

(2) id : 유일하게 식별되는 DID 자체를 나타내며, DID Document들은 반드시 id 속성을 포함

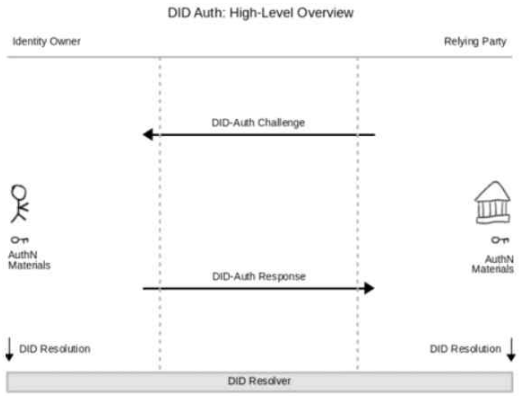
(3) authentication : DID Subject가 Document에 나와 있는 DID임을 인증할 수 있는 방식을 나타내는 항목

(4) controller : holder라고 부르기도 하며, DID Document를 제어할 수 있는 Subject 및 Group

(5) publicKey : 공개키는 사용자 간 인증을 하거나 service endpoint와의 안전한 통신을 위해 필요한 전자서명, 암호화 등의 여러 목적에 사용되는 공개키들의 목록

(6) service : DID Subject와 상호작용할 수 있는 서비스로 service endpoint 항목을 통해 DID Subject가 제공하는 서비스를 검색 및 사용할 수 있도록 해주며 예시로는 DID 관리, 파일 저장, 검색 같은 서비스가 있음

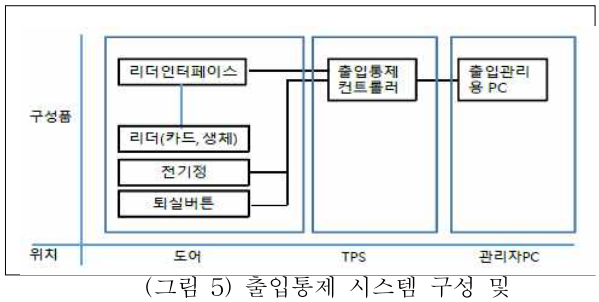
DID 구현은 DID Resolver를 통해 이루어 진다. DID Resolver는 DID 값을 입력으로 받아 해당하는 DID Document를 결과로 반환하는 소프트웨어 및 하드웨어로 DID document 정보를 가져올 때 DID Method에 정의된 4가지 operation인 Create, Read, Update, Deactivate 중 Read를 이용한다. (그림 4)는 DID Reslover를 이용해 DID Document에서 상대방의 공개키 정보를 획득하고 Challenge-Response를 통해 서로의 DID를 인증하는 과정을 보여준다.[1]



(그림 4) DID 인증[6]

2.3 출입통제 시스템

출입통제 시스템은 주요 시설물 보호, 기밀 유출 방지, 도난 예방 등을 위한 목적으로 사전에 등록된 사용자만이 해당 장소 및 시간에 허용할 수 있도록 하는 기술이다. 일반적인 출입통제 시스템은 (그림 5)와 같이 출입문, 리더기, 컨트롤러(리더기에 포함되기도 함), 출입관리용 PC(서버)가 종합적으로 연결되어 구성된다.[7]



(그림 5) 출입통제 시스템 구성 및 다이어그램[7]

2.3.1 출입통제 시스템의 인증수단

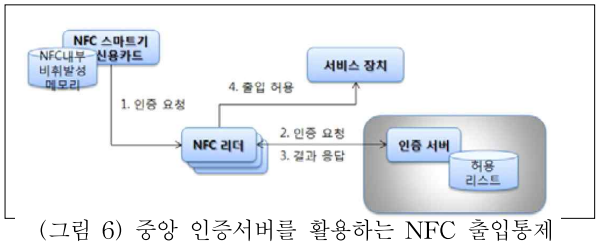
출입통제 시스템의 인증수단에는 소지기반의 인증와 생체기반의 인증이 있다. 소지기반의 인증에는 RF카드, 모바일 앱 인식이 있으며, 생체기반의 인증에는 지문인식, 홍체인식, 망막인식, 장문인식, 얼굴인식, 정맥인식 등이 있다.

2.3.2 모바일 앱 기반의 출입통제 시스템

모바일 앱 기반의 출입통제 시스템은 기존의 RF 카드의 기능을 스마트폰 앱으로 구현시킨 인증 방식으로 RF 카드와 같이 무선 주파수를 활용하여 통신하며, 통신 수단은 범용 기준인 NFC를 주로 이용한다.

NFC(Near Field Communication)는 비접촉식 근거리 무선 통신기술로 두 대의 NFC 칩 단말기 간 10cm 이내의 거리에서 데이터를 양방향으로 통신할 수 있는 기술이다.[7] NFC 기술은 하나의 장치에서 RF카드 리더와 태그 기능을 동시에 지원하며 NFC Card Emulation Mode를 활용하여 APP을 개발하면 NFC에서 표준규격을 활용한 카드 데이터값을 전송 및 수신할 수 있다. 이를 활용하여 NFC 리더에서는 카드 데이터값에 대한 Read/Write가 가능하며 입력된 정보를 출입 권한에 매핑하여 출입제어에 사용할 수 있다.[8]

NFC를 활용한 출입통제 시스템의 개념적 구성내용은 (그림 6)과 같다.[9]



(그림 6) 중앙 인증서버를 활용하는 NFC 출입통제 모델[9]

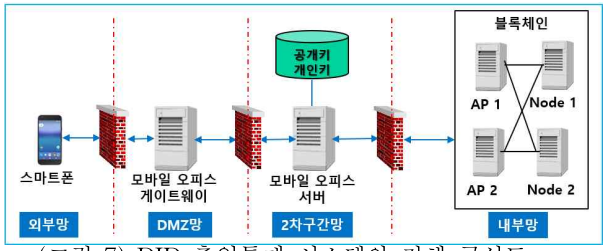
NFC는 카드 모드로 스마트기기 또는 OS에서 요청이 있을 시 해당 통신을 지원하는 수동모드로 동작하며 NFC 리더에 근접했을 때 인증요청을 하며 NFC 리더는 통신을 통해 얻은 인증데이터를 서버에 다시 인증을 한다. 서버는 데이터 값 검증 후 결과를 응답하며 NFC 리더기에서 출입을 허용하는 절차를 가진다.[9]

3. DID 출입통제 시스템의 설계 및 구현

시스템의 설계 및 구현은 기 운영 중인 RF 기반 출입통제 시스템에 NFC 및 탈중앙화 신원증명(Decentralized Identifier) 기술을 접목하여 적용하였다.

3.1 시스템의 설계

본 시스템은 DID 기반 블록체인 시스템으로 설계를 하였으며 전체 구성도는 (그림 7)과 같다.



(그림 7) DID 출입통제 시스템의 전체 구성도

주요 구축 내용은 <표 2>와 같다.

<표 2> 시스템 주요 구축 내용

구 분	주요내용
공통 인프라 구축	· Private 블록체인 네트워크 구성 · 노드, 블록, 트랜잭션 관리를 위한 대시보드 구현 · 향후 확장을 위한 기반 마련
DID 인증 기반 구축 (모바일 사원증)	· 모바일오피스에 DID인증 모듈 탑재 · DID인증을 통한 신원정보(모바일사원증) 생성 · 신원정보(모바일사원증) 전자지갑 저장

DID 기반의 Private 블록체인 시스템을 구축하고 이를 통해 출입통제 시스템 뿐만 아니라 향후 타 영역으로의 확장을 위한 기반을 마련하였다. 스마트폰을 출입통제 시스템과 연동하기 위해 기 운영 중인 모바일오피스 앱에 DID 인증 모듈을 탑재하고 NFC 기능을 적용한 모바일 사원증을 개발하였다. DID 모바일 사원증은 모바일오피스 전자지갑에 안전하게 저장되며 출입시 인증에 이용될 수 있다.

3.2 시스템의 구현

시스템의 구현은 금융회사 D사 데이터센터를 대상으로 진행하였다. D사 데이터센터에는 약 200여명의 임직원이 상주하고 있다.

3.2.1 DID 블록체인 시스템의 구성

DID 블록체인 시스템의 구성정보는 <표 3> 과 같다.

<표 3> DID 블록체인 시스템의 구성정보

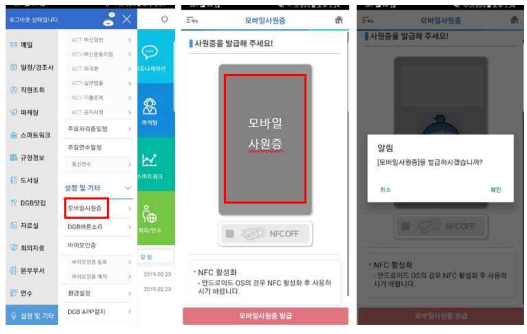
업무명	OS정보	도메인 정보
모바일오피스 게이트웨이 1	AIX 7200	office.xxx.co.kr
모바일오피스 게이트웨이 2	AIX 7200	office.xxx.co.kr
모바일오피스 AP1	AIX 7200	-
모바일오피스 AP2	AIX 7200	-
블록체인 API 1	RedHat 8.3	did.xxx.co.kr
블록체인 API 2	RedHat 8.3	did.xxx.co.kr
블록체인 AP 1	RedHat 8.3	bic1.xxx.co.kr
블록체인 AP 2	RedHat 8.3	bic2.xxx.co.kr

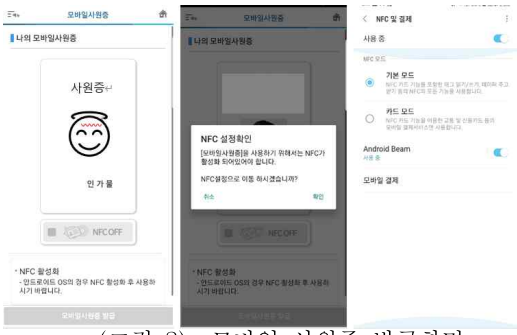
모바일오피스 시스템은 기존에 운영하던 시스템을 이용하였으며, DID 블록체인 시스템을 위해 블록체인 API 서버 2대, 블록체인 노드 서버 2대를 L4 스위치를 이용하여 Active-Active 이중화로 구성하였다. 블록체인 서버는 RedHat 8.3 리눅스 운영체제에 프라이빗 블록체인 기술인 하이퍼레저 패브릭(Hyperledger Fabric)으로 구성하였다.

하이퍼레저(Hyperledger)는 2015년12월 리눅스 재단에 의해 시작된 블록체인 오픈소스 프로젝트로 여러 기업이 참여하여 기술을 공동 개발하고 있다. 하이퍼레저의 목표는 여러 산업에 걸쳐 응용 가능한 블록체인 기술을 만드는 것이다. 하이퍼레저는 하이퍼레저 캘리퍼(Caliper)와 같은 도구와 하이퍼레저 우르사(Ursa)와 같은 라이브러리, 하이퍼레저 패브릭(Fabric), 쏘투스(Sawtooth), 인디(Indy)를 포함한 다양한 분산 원장 프레임워크를 제공한다.[11] 본 시스템은 하이퍼레저 중 가장 많이 이용되는 하이퍼레저 패브릭을 적용하였다.

3.2.2 모바일 사원증의 발급

모바일 사원증의 발급은 기 운영 중인 모바일오피스 시스템을 이용하였다. 모바일 사원증 발급 절차는 (그림 8)과 같다. 모바일오피스는 NFC 기능을 활성화하고 모바일오피스의 직원정보와 사번정보를 기본값으로 하여 모바일 사원증을 발급하고 전자지갑에 저장한다.





(그림 8) 모바일 사원증 발급화면

3.2.4 개인키 및 공개키의 생성

모바일 사원증의 안전한 전달을 위해 사용한 암호화 기술은 타원 곡선형 공개키 암호화 알고리즘인 “Ed25519”를 사용하였다. Ed25519는 TLS 1.3이 나오면서 등장한 새로운 디지털 서명 알고리즘인 EdDSA(Edwards-curve Digital Signature Algorithm)의 하나이다. Ed25519는 Edwards25519 Curve를 사용하는 EdDSA이다. Hash는 SHA-512(SHA-2)를 사용한다. [10]

이를 통해 공개키 및 개인키를 (그림 9)와 같이 생성한다. 생성된 키를 이용해 신원정보를 암호화하여 활용한다.

```
POST https://dgb-did-test.daios.net/v1/xlm/key
```

```
{
    "responseStatus": 200,
    "responseMessage": "S0000",
    "data": {
        "publicKey": "GAAKOR2HLJLR6Y5GNANQ3FYTNQ5USJNWP7NMQKC54GTDDPMFPRM5BIF7", // 공개키
        "secretKey": "SBF2N6YMRHZWNP4XL6WKOH4GRWZ7WI7PIEQDH5LYQUTMRDG2T72G5GPF" // 개인키
    }
}
```

(그림 9) Ed25519 암호화 알고리즘을 이용한 공개키, 개인키 생성

3.2.5 DID 표준 명세

출입 인증을 위해 스마트폰 모바일오피스 앱에서 DID 블록체인 서버에 요청하는 DID 표준명세 정보는 (그림 10)과 같다. 포함된 내용은 공개키와 모바일오피스의 직원정보이다. 직원정보에는 소속사, 사번, 이름, 부서명, 직급 등이 들어간다.

```
POST {{internal-api}}/v1/did/credential
POST http://dgb-did-internal.daios.net:9443/v1/did/credential // 외부 테스트망
POST http://didt.daegubank.co.kr:9443/v1/did/credential // 내부 테스트망


{
    "stellar": { // Stellar 정보
        "network": "TESTNET",
        "publicKey": "GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ",
        "memo": "DID 발급"
    },
    "credentialStatus": "active", // 현재 active 값 고정
    "credentialSubject": {
        "group": "DGB", // 고정
        "affiliate": "데이터시스템즈", // 계열사
        "id": "1234567", // 행번
        "name": "홍길동", // 이름
        "department": "금융개발부", // 부서

        "position": "사원", // 직급
        "gateway": "INNOVATION_LOBBY01" // 출입문 고유코드
    }
}
```

항목	설명
stellar	스텔라 공개키 관련 정보
credentialStatus	크리덴셜 상태정보
credentialSubject	크리덴셜 상세정보

(그림 10) 요청시 DID 전문정보

요청을 받은 DID 블록체인 서버는 (그림 11)과 같은 응답 전문을 회신한다. 응답 전문에는 인증방법, 인증상태, 증명방법 등의 정보가 포함되어 있다.

```
{
    "responseStatus": 200,
    "responseMessage": "S0000",
    "data": {
        "verifiableCredential": {
            "@context": [
                "https://www.w3.org/ns/did/v1",
                "https://daib.io/credential1s/dgb/v1"
            ],
            "id": "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ", // 외부에 조회할 DID 공개키
            "type": [
                "VerifiableCredential",
                "DGBCredential"
            ],
            "issuer": "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ",
            "verificationMethod": [
                {
                    "id": "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ",
                    "type": "Ed25519VerificationKey2018",
                    "controller": "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ",
                    "daibAddress": "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ",
                    "ipfsTxId": "QmcHmFhDyFGUApKqE18zJFwtUFMJakjWhMZYoF5bw7Q3Hh"
                }
            ],
            "authentication": [
                {
                    "id": "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ",
                    "type": "Ed25519VerificationKey2018",
                    "controller": "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ",
                    "publicKey": "GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ"
                }
            ],
            "service": [
                {
                    "id": "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ",
                    "type": "VerifiableCredentialService",
                    "serviceEndpoint": "https://dgb-did.daios.net/v1/vc"
                }
            ],
            "credentialSubject": {
                "group": "DGB",
                "affiliate": "데이터시스템즈",
                "id": "1234567",
                "name": "홍길동",
                "department": "금융개발부",
                "position": "사원",
                "gateway": "INNOVATION_LOBBY01"
            },
            "credentialStatus": {
                "id": "http://localhost:9443/v1/did/DGB/1234567",
                "type": "credentialStatus-dgb-did"
            },
            "assertionMethod": [
                "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ"
            ],
            "capabilityDelegation": [
                "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ"
            ],
            "capabilityInvocation": [
                "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ"
            ],
            "validFrom": "2020-11-25T00:49:53Z",
            "validUntil": "",
            "proof": {
                "type": "Ed25519VerificationKey2018",
                "proofPurpose": "assertionMethod",
                "verificationMethod": "did:daib:GBS2OHWMCNO4F7AX6FTTBB3O2BVWURIUFXTGCYWJU4IDNGHI7GU76UMJ",
                "created": "2020-11-25T00:49:53Z"
            }
        }
    }
}
```

항목	설명	비고
responseStatus	응답상태코드	
responseMessage	응답메시지	
data:id	VC ID	DID 공개키
data:issuer	발급자	
data:verificationMethod	인증방법	
data:authentication	인증	
data:service	서비스 설명	
data:credentialSubject	개인정보(인증대상정보)	사원정보
data:credentialStatus	인증상태	
data:assertionMethod	인증주장방법	
data:capabilityDelegation	권한위임방법	
data:capabilityInvocation	권한실행방법	
data:proof	증명방법	

(그림 11) 응답시 DID 전문정보

3.3 DID 출입통제 시스템의 업무 흐름도

구현한 DID 출입통제 시스템의 동작 방식은 발급, 개폐, 폐기 총 3개의 프로세스로 구성이 되어 있다.

3.3.1 모바일 사원증 발급(신청) 프로세스

모바일 사원증 발급(신청) 프로세스는 (그림12)와 같다.

(그림 12) 모바일 사원증 발급(신청) 프로세스

① 모바일오피스 접속 후 모바일 사원증 발급 버튼을 클릭하여 모바일오피스 G/W로 발급 요청(SSL 구간 암호화)

② 모바일오피스 G/W는 모바일오피스 서버로 해당 요청 전달(SSL 구간 암호화)

③ 모바일오피스 서버에서 공개키 암호화 알고리즘을 이용하여 개인키, 공개키 생성

④ 모바일오피스 서버에서 공개키 및 사원정보를 블록체인 API 서버로 전송(블록체인 API 서버에서 DID 증명서 생성)

⑤ 블록체인 API 서버에서 블록체인 노드로 공개키 및 사원정보 전송

- 블록체인 노드에 공개키 및 사원정보 저장
- 블록체인 노드에 발급요청 거래로그 저장

⑥ 생성된 DID 증명서를 모바일오피스 서버로 전송

⑦ 모바일오피스 서버에서 UUID를 생성하여 전달받은 DID증명서 ID 및 사원정보를 DB에 <표 4>와 같이 저장

<표 4> DB 저장정보

회사 코드	사번	성명	영문 성명	개인키	공개키	VCID	UUID	생성 일시

※ VCID(Verifiable Credential Identifier) : DID증명서 ID

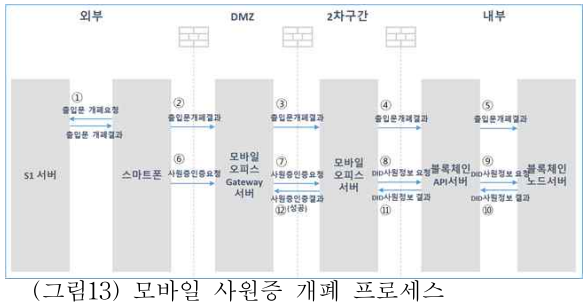
※ UUID(Universally Unique Identifier : 범용 고유 식별자)

⑧ 모바일오피스 서버에서 생성된 UUID, 사번, 발급회차 정보를 암호화하여 모바일오피스 G/W로 전송

⑨ 모바일오피스 G/W는 전달받은 정보를 스마트폰으로 전송

3.3.2 모바일 사원증 개폐 프로세스

모바일 사원증 개폐 프로세스는 (그림13)과 같다.



(그림13) 모바일 사원증 개폐 프로세스

① NFC가 활성화된 스마트폰을 출입단말에 태그했을 때 S1(출입통제 시스템)의 SDK를 통해 모바일 사원증의 카드번호(사번) 및 발급회차 정보를 암호화하여 출입단말에 전송

- 출입통제 시스템에는 사번 및 발급회차 정보만 저장되어 있으며 이를 통해 개폐여부 결정

② 출입문 개폐결과(성공/실패 여부)를 모바일오피스 G/W로 전송

③ 출입문 개폐결과(성공/실패 여부)를 모바일오

피스 서버로 전송
④ 출입문 개폐결과(성공/실패 여부)를 블록체인 API 서버로 전송
⑤ 출입문 개폐결과(성공/실패 여부)를 블록체인 노드 서버로 전송
- 블록체인에 거래로그(성공/실패 여부) 저장
⑥ 스마트폰에서 모바일오피스 G/W로 사원증 인증 요청
⑦ 모바일오피스 G/W에서 모바일오피스 서버로 사원증 인증 요청
⑧ 모바일오피스 서버에서 블록체인 API 서버로 DID 사원정보 인증요청
- 공개키와 DID 구조체를 조립하여 블록체인 API 서버로 전송하면 일치 여부 회신. UUID 및 사번 일치 여부 확인
⑨ 블록체인 API 서버는 공개키와 DID 구조체를 블록체인 노드로 전송
- DID 사원정보 검증 및 검증결과를 블록체인 노드에 기록
⑩ 블록체인 노드 서버에서 DID 사원정보 검증결과를 API 서버로 전송
⑪ 블록체인 API 서버는 모바일오피스 서버로 DID 사원정보 검증결과 전송
⑫ 모바일오피스 서버는 DID 사원정보 검증결과를 모바일오피스 G/W로 전송
- UUID, DID 구조체 일치 여부(DID ID, 공개키, 사번 일치) 검증

3.3.3 모바일 사원증 폐기 프로세스

모바일 사원증 폐기 프로세스는 (그림14)와 같다.

(그림14) 모바일 사원증 폐기 프로세스

①~⑪ 개폐 프로세스와 동일
⑫ UUID 또는 DID 구조체 불일치시 모바일오피스 서버는 모바일오피스 G/W로 스마트폰의 UUID, 카드번호(사번), 카드 발급회차 정보 삭제 지시
⑬ 모바일오피스 G/W는 스마트폰의 상기 정보 삭제 메시지 전달
⑭ 스마트폰에서 사원증 관련 정보 삭제

4. 평가 및 기존 시스템과의 비교

본 논문에서는 출입통제 시스템의 신원증명을 위해 DID 기술을 이용하였다. 기존 NFC 기반의 출입통제 시스템이 사용자 인증정보를 내부 DB에 저장하고 이를 신원증명으로 이용하고 있는 반면 본 논문에서 제시한 DID 출입통제 시스템은 개인이 보유한 스마트폰의 사용자 정보를 이용하여 사용자 자격을 증명하고, 정당하게 자격 증명이 된 사용자만 출입을 허용한다. 본 절에서는 제안한 DID 출입통제 시스템을 정보보호의 3대 요소인 가용성, 기밀성, 무결성 기준으로 평가하고, DID 기반 NFC 출입통제 시스템이 기존 일반적인 NFC 기반 출입통제 시스템과 기술적인 비교를 통해 제안한 시스템의 강화된 차이점을 비교한다.

4.1 가용성

DID Document 정보를 저장하는 Verifiable Data Registry는 블록체인의 저장소로써 분산된 노드 간 네트워크를 형성하여 하나의 노드에 장애가 발생해도 다른 노드가 중단되지 않고 기능을 유지할 수 있다. 본 시스템은 이중화 노드로 구성되어 가용성을 가진다.

4.2 기밀성

본 논문에서 제안하는 시스템은 스마트폰과 모바일오피스 서버와 통신시에는 SSL 암호화를 이용하고 블록체인 서버로 정보전달 및 저장시에는 공개키 기반의 암호화를 이용하고 있다. 이중으로 암호화하여 당사자 외에는 정보를 확인할 수 없도록 기밀성을 가진다.

4.3 무결성

Verifiable Data Registry에는 DID Document가 저장된다. DID Document는 반드시 id 속성을 가지고 있으며, 이 id 속성은 유일하게 식별되는 DID 자체를 나타낸다. 또한 Verifiable Data Registry가 분산원장으로 처리되므로 정보의 위변조가 불가능하다.

4.4 기존 방식과의 비교

제안한 방식과 기존 방식을 비교하면 <표 4>와 같다.

<표 4> 제안방식과 기존 방식의 비교

구 분	DID 출입통제 시스템	NFC 출입통제 시스템
신원증명	스마트폰에 저장된 사용자 정보를 이용해 신원증명	출입통제 시스템 DB에 저장된 사용자 정보 및 인증정보를 통해 신원증명
시스템 구성	출입통제 시스템과 별도로 DID 블록체인 서버가 구성이 되며, 신원증명은 DID 블록체인서버가 담당	출입통제 시스템이 내부망에 위치함
사용자 정보의 보호	저장되는 사용자 정보는 공개키 암호화로 암호화하고 블록체인으로 분산 저장됨	사용자 정보가 DB로 저장이 되어있어 보호를 위해서는 별도 DB 암호화 솔루션이 필요
출입통제 시스템에 저장되는 개인정보	출입통제 시스템에는 인증을 위한 최소정보(카드정보)만 저장	NFC 정보와 사용자의 신원증명에 필요한 모든 정보가 출입통제 시스템 DB에 저장됨
출입자의 통제	출입통제 시스템의 카드번호 업데이트를 통해 관리	출입통제 시스템의 사용자 정보 업데이트를 통해 관리

제안한 DID 출입통제 시스템은 기존 NFC 출입통제시스템에 비해 사용자 신원증명을 중앙집중화된 정보가 아닌 스마트폰에 분산 저장된 정보를 이용하고, 사용자 정보가 출입통제 시스템 DB에 저장되는 것이 아닌 블록체인 서버에 암호화 되어 저장이 되며, 출입통제 시스템 DB에는 최소한의 정보만 관리하게 함으로써 중앙서버의 해킹에 안전하게 하고, 직원들 본인의 정보를 본인이 소유한 스마트폰을 통해 관리하고 신원증명을 하게 함으로써 개인정보를 보다 안전하게 관리할 수 있다.

5. 결 론

본 논문에서는 DID 기술을 출입통제 시스템에 접목하여 신원증명을 기존의 중앙서버를 통한 방식이 아닌 개인 소유에 기반한 탈중앙화 방식의 신원증명 방식으로 활용이 가능함을 보여 주었다.

DID 출입통제 시스템을 통해 신원 증명을 개인이 소유한 스마트폰에 저장된 개인정보를 이용함으로써 본인의 개인정보를 중앙서버에 저장할 필요가 없이 본인의 주도하에 관리할 수 있게 되었다.

DID 기술을 이용하면 신원증명을 개인이 주체가 되어 관리할 수 있기 때문에 중앙 집중형 서비스에 의존하지 않아 서버 해킹 등을 통한 개인정보유출의 위험에서 자유로워 질 수 있다.

DID 기술은 출입통제 시스템 뿐만 아니라 신원증명이 필요한 다양한 분야에 응용되어 질 수 있다.

향후 연구과제로 본 논문의 DID 출입통제 시스템 기술을 확장하여 PC 로그인 신원증명, 시스템 접속시 신원증명, 복합기 사용시 신원증명, 전자결재 등 기업의 다양한 영역에 활용할 수 있을 것이다.

참고문헌

[1] 최정용, “DID 기반 탈중앙화 키 관리 시스템에서 복구용 DID를 사용한 키 복구 방법”, 아주대학교 대학원, 2021.

[2] 금융결제원, “분산ID[모바일신분증] 서비스설명자료”, 2019.

[3] 김영현, “블록체인을 활용한 디지털 신원증 명 적용방안 연구”, 국민대학교 소프트웨어융합대학원, 2019.

[4] Alex Andrade-Walz, “What are Decentralized Identifiers (DIDs)?”, https://www.evernym.com/blog/ what-are-decentralized-identifiersdids/

[5] Drummond Reed, et al., “Decentralized Indentifiers

(DIDs) v1.0 - Core architecture, data model, data model, and representations", https://www.w3.org/TR/did-core/

[6] Markus Sabadello et al., "Introduction to DID Auth", Rebooting the Web of Trust VI design workshop, 2018.

[7] 금융감독원, "2018-2019년 출동 보안 서비스 회사 매출", pp. 38, 2020.02.

[8] 류성관, 박요한, 김창균, 박영호 "출입통제 시스템의 취약성 분석 및 대응방안", 한국통신학회 학술대회논문집, pp. 800-801, 2016.

[9] 이민구, 김동완, 손진수 "NFC를 활용한 능동형 인증방법", 한국통신학회논문지, 제37권, 제2호, pp. 140-156, 2012.

[10] AEP코리아네트 "ECDSA와 EdDSA", https://blog.naver .com/aepkoreanet/222088849086.

[11] 하이퍼레저 프로젝트, "What is Hyperledger?", https://www.hyperledger.org

[12] 김지영, "블록체인기반 모바일 신원증명 서비스의 수용의도에 영향을 미치는 요인에 관한 연구", 숭실대학교 대학원, 2020.

[13] 김민수, 이동휘, 김귀남, "이중 출입통제 시스템을 이용한 내부 시설 보안성 확보 방안", 융합보안논문지, 제12권, 제4호, pp.123-129, 2012.09.

〔저자소개〕

이 상 근 (Sang-Geun Lee)

1993년 2월 경일대학교 컴퓨터공학 학사
2010년 2월 경북대학교 경영정보전공 경영학 석사
현재 경북대학교 정보보안전공 박사과정
현재 DGB대구은행 정보보호부 정보보호 최고책임자

email : sang@dgbfn.com

김 도 형 (Do-Hyeong Kim)

2001년 2월 한국방송통신대학교 미디어영상학 학사
2003년 2월 경기대학교 정보보안전공 공학석사
2008년 8월 경기대학교 정보보호학 이학박사
현재 DGB대구은행 정보보호부 차장

email : pccop@daum.net

정 순 기 (Soon-Ki Jung)

1990년 경북대학교 공학사
1992년 KAIST 이학석사
1997년 KAIST 공학박사
1998년~현재 경북대학교 컴퓨터학부 교수

email : skjung@knu.ac.kr