JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 5, pp. 127-138, May 2022
https://doi.org/10.9708/jksci.2022.27.05.127

FinDID : A DID service supporting the standard service scheme for the financial sector

Young-Eun Lee*, Hye-Won Kim*, Myung-Joon Lee**

*Student, Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan, Ulsan, Korea
*Student, Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan, Ulsan, Korea
**Professor, School of IT Convergence, University of Ulsan, Ulsan, Korea

[Abstract]

In this paper, we present FinDID (Financial Decentralized IDentity), a blockchain-based DID(Decentralized IDentity) service that can flexibly control personal information or credentials through a systematic verification method while complying with the standard service scheme of decentralized identity for the financial sector. DID is an identity management system used in a decentralized environment without a specific certification authority, and as a technology that allows users to control their own information, it can realize self-sovereignty over users' own personal information. Through FinDID, users receive credentials that authenticate their various personal information from the issuer, select only the claims required by the target financial service using their personal electronic wallet, create presentations from credentials. Then they submit it to the financial service, leading to their qualification from the service. FinDID consists of electronic wallet, credential issuer, credential storage, DID service including DID management contract and credential management contract, and financial services using this service scheme. The DID service manages each user's DID and supports all verification processes of the associated identity management scheme.

▸ **Key words**: DID, Blockchain Service, Electronic Wallet, Financial Service, Identity Management

[요 약]

본 논문에서는 금융권 DID(Decentralized Identity) 서비스 체계의 표준 방식을 준수하는 가운데 체계적인 검증 방식을 통하여 개인 정보나 자격 증명을 유연하게 제어할 수 있는 블록체인 기반의 DID 서비스인 FinDID(Financial Decentralized IDentity)를 제시한다. DID는 특정 인증기관 없이 탈중앙화 환경에서 활용하는 신원 관리 체계이며, 사용자가 자신의 정보를 제어할 수 있는 기술로서 사용자 자신의 개인정보에 대한 자기 주권화를 실현할 수 있다. FinDID을 통하여 사용자는 자신의 여러 개인정보를 인증하는 크리덴셜을 발급자에게 발급받아 개인 전자지갑을 이용해 타겟 금융 서비스가 필수적으로 요구하는 클레임만을 크리덴셜에서 선택하여 프레젠테이션을 생성하고, 이를 금융 서비스에게 제출하여 자신의 서비스 이용자격을 부여받는다. FinDID는 전자지갑, 크리덴셜 발급자, 크리덴셜 저장소 그리고 DID 관리 컨트랙트 및 크리덴셜 관리 컨트랙트를 포함하는 DID 서비스 및 이러한 서비스 체계를 이용하는 금융서비스로 구성된다. DID 서비스는 각 사용자의 DID를 관리하고 관련된 신원 관리체계의 모든 검증과정을 지원한다.

▸ **주제어**: DID, 블록체인 서비스, 전자지갑, 금융 서비스, 신원관리

• First Author: Young-Eun Lee, Corresponding Author: Myung-Joon Lee
*Young-Eun Lee (lyoung828@cicweb.ulsan.ac.kr), Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan
*Hye-Won Kim (alsldjcjstk@cicweb.ulsan.ac.kr), Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan
**Myung-Joon Lee (mjlee@ulsan.ac.kr), School of IT Convergence, University of Ulsan
• Received: 2022. 05. 02, Revised: 2022. 05. 23, Accepted: 2022. 05. 23.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

최근 많은 서비스가 신원확인, 각종 증명서 및 중요 개인정보 제출 등에 DID(Decentralized Identity)를[1-2] 활용하고 있다.[3-8] DID는 특정 인증기관 없이 탈중앙화 환경에서 활용하는 신원정보 체계로서 사용자가 자신의 정보를 제어할 수 있으며, 자신의 개인정보에 대한 자기 주권화를 실현할 수 있다. 이에 따라 금융정보화추진협의회에서는 금융회사 DID 서비스 운용 및 공유체계 표준 v1.0을 제정하여[9], 금융권에서 DID 서비스를 도입하여 이용하고자 할 때 참조할 수 있는 DID 서비스 모델, 고려사항 및 공유체계를 제시하였다. 표준에서 제시하는 DID 체계를 구성하는 주요 개념들에는 클레임, 크리덴셜, 프레젠테이션 등이 존재한다.

클레임은 디지털 환경에서 개인의 신원 및 자격 정보를 표현할 수 있는 각 단위 데이터를 의미한다. 크리덴셜은 개별 주체에 대한 한 개 이상의 클레임으로 구성된 집합으로 디지털 환경에서의 자격 증명서를 나타낸다. 클레임을 조합하여 개별 주체에 대한 신원이나 자격을 검증할 수 있는 증명서의 역할을 할 수 있다. 프레젠테이션은 크리덴셜로부터 유도 가능한 클레임의 최소 집합체이다. 프레젠테이션은 무분별한 개인정보 데이터의 유출을 막고자 특정 상황에 맞게 증명 과정에 필요한 최소한의 클레임만을 크리덴셜에서 선택하여 구성한 새로운 형식으로 만들어지며, 개별 주체가 이를 금융 서비스에 제출해 자신의 서비스 이용자격을 검증받을 수 있다.

현재로서는 표준에서 제시하는 형태의 기능인 사용자가 전자지갑을 통해 크리덴셜로부터 클레임 추출하고, 추출된 클레임들의 무결성을 검증할 수 있는 프레젠테이션을 생성 가능하도록 하는 기법을 제공하는 서비스는 아직 소개되고 있지 않다. FinDID는 표준 방식을 준수하면서 프레젠테이션에 포함된 개별 클레임에 대한 무결성 보장을 위한 검증과정을 체계적으로 개발하여 프레젠테이션을 통해 사용자의 자격 검증이 확실하게 이루어질 수 있도록 보장하는 DID 서비스를 제공한다.

FinDID는 전자지갑, 크리덴셜 발급자, 크리덴셜 저장소 그리고 DID 관리 컨트랙트 및 크리덴셜 관리 컨트랙트를 포함하는 DID 서비스 및 이러한 서비스 체계를 이용하는 금융서비스로 구성된다. 사용자는 전자지갑을 통해 자신의 DID 정보 및 크리덴셜을 보관하고 프레젠테이션을 생성한다. 여기서 크리덴셜은 크리덴셜 발급자를 통해 발급받으며, 발급된 크리덴셜은 크리덴셜 저장소에서 관리된다. 금융 서비스는 생성된 프레젠테이션을 전달받고 프리젠테이션 검증과 함께 이에 포함된 개별 클레임의 검증을 통하여 사용자의 서비스 이용자격을 확인한다. 또한, DID 서비스는 각 사용자의 DID와 크리덴셜 발급내역을 클레이튼[10] 블록체인의 스마트 컨트랙트로 개발된 DID 관리 컨트랙트와 크리덴셜 관리 컨트랙트에서 관리하고, 관련된 신원 관리체계의 모든 검증과정을 지원한다. 이처럼 FinDID의 각 컴포넌트들이 상호작용하며 체계적인 DID 서비스를 제공하여 개인 신원정보 관리와 증명 과정의 신뢰성을 보장한다.

실제 응용 서비스들이 FinDID를 이용해 동작하는 과정의 이해를 돕고, 각 과정이 신뢰성 있게 진행되는지 증명하기 위해 실험적인 크리덴셜 발급자 및 금융 서비스를 개발하였다. 크리덴셜 발급자는 카드 회사를 모형으로 구현하였으며, 카드사는 사용자에게 카드사 가입 시에 증명된 사용자의 모든 정보를 크리덴셜로 발급한다. 금융 서비스는 온라인 쇼핑몰을 모형으로 구현하였으며, 사용자가 온라인 쇼핑몰 서비스 이용을 위해 카드 정보를 등록해야 하고, 사용자는 필수적인 정보만 크리덴셜로부터 추출하여 전자지갑을 통해 생성한 프레젠테이션을 생성하고, 쇼핑몰 서비스는 사용자의 이용자격을 전달받아 검증한다.

본 논문의 구성은 다음과 같다. 1장 및 2장에서는 서론과 배경지식을 다룬다. 3장에서는 FinDID의 시스템 및 데이터 구조를 제안하고, 4장에서는 FinDID의 주요 프로세스에 관하여 기술한다. 5장에서는 FinDID의 구현 결과에 관하여 기술하며. 마지막으로 6장에서는 본 논문의 결론에 관하여 서술한다.

II. Background Knowledge

1. DID

DID는 특정 인증기관 없이 탈중앙화 환경에서 활용하는 신원정보 체계로서 사용자가 자신의 정보를 제어할 수 있으며, 자신의 개인정보에 대한 자기 주권화를 실현할 수 있는 기술이다. 금융정보화추진협의회 표준화사업에서는 분산ID(DID) 관련 표준화를 진행하는 W3C에서 공표한 2021년3월 Decentralized Identifiers v1.0을[1] 참조하여 금융회사가 공동으로 이용할 분산ID 서비스 및 신원관리 프레임워크에 대한 표준을 제정하였다. 제정된 표준에선 금융회사가 적용할 수 있는 분산ID 서비스의 모델 시스템 및 데이터 구성과 금융회사 간 공유체계 등을 표준화하여 정의했다. 표준 분산ID 서비스 모델의 구성요소로 금융회사는 분산ID를 이용해 사용자에게 디지털 신원증명을 발급하거나 이용하는 서비스 제공자 역할을 수행하고, 블

록체인 기반 분산ID 저장소와 전자지갑과 같은 인프라를 제공한다.

표준에서 제시하는 분산ID 서비스를 통해 금융소비자의 신원을 증명하는데 사용되는 정보개념은 분산ID 식별자, 크리덴셜, 프레젠테이션을 포함한다. 분산ID 식별자(DID)는 중앙화된 등록 기관이 아닌 블록체인이 관리하는 식별자로 개개인이 자신의 개인정보를 제어할 수 있으며 서명을 통해 자신의 신원을 인증할 수 있다. 크리덴셜은 금융소비자가 제출한 정보를 토대로 발급해주는 일종의 디지털 신원정보이다. 프레젠테이션은 금융소비자가 금융서비스를 이용하기 위해 금융회사에 제출하는 자신의 자격증명이다.

현재 많은 서비스가 신원확인, 각종 증명서 및 중요 개인 정보 제출 등에 DID를 활용하고 있지만, 아직까지 표준에서 제시하는 개념과 검증기법을 준수하는 서비스는 소개되고 있지 않다. 이에 따라 FinDID는 표준 방식을 준수하면서 프레젠테이션에 포함된 개별 클레임에 대한 무결성 보장을 위한 검증과정을 체계적으로 개발하여 프레젠테이션을 통해 사용자의 자격 검증이 확실하게 이루어질 수 있도록 보장하는 DID 서비스를 제공한다.

2. Klaytn and Smart contract

클레이튼은 하이브리드 형태의 블록체인으로 탈중앙화 데이터 통제 및 제어가 용이한 분산된 거버넌스의 개방형 블록체인(Public Blockchain)과 낮은 지연성과 높은 확장성의 폐쇄형 블록체인(Private Blockchain)의 장점을 융합한 블록체인이다. 2세대 블록체인인 이더리움의[11] UI-UX 약점을 보완하여 사용자 친화적 경험 및 직관적인 개발 환경을 제공하여 대중적인 서비스로 운영 가능한 블록체인 플랫폼이다. 클레이튼은 카카오(Kakao), 엘지전자(LG Electronics), 넷마블(Netmarble) 등 수백 개의 국내 대기업들이 포함된 거버넌스 카운슬(Governance council)을 이루어 대중 친화적인 서비스 개발을 적극적으로 주도하고 있다. 또한, 처리 속도면에 있어서 이더리움의 초당 처리가능한 트랜잭션 수(TPS, Transactions per second)가 평균 13인 반면에 클레이튼 메인넷의 TPS는 4,000으로 높은 처리량과 즉각적인 완결성을 보여준다. 클레이튼은 기술 스택의 인터페이스와 실행 방식을 이더리움과 호환시켜 이더리움과 상호적인 연동으로 클레이튼 생태계의 확장성을 높였으며, 이더리움 가상 머신(EVM)에서 작동하는 스마트 컨트랙트를 위하여 개발된 정적타입의 프로그래밍 언어인 솔리디티를 사용하여 스마트 컨트랙트를 개발한다. 스마트 컨트랙트란 블록체인 상에서 특정 계약 조건에 따라 자동으로 계약 내용이 실행되도록 하는 스마트 계약 기능으로 무결성 및 조작 방지에 대한 보장이 가능하다.

III. Architecture of FinDID

본 장에서는 FinDID의 주요 데이터 및 컴포넌트 구조에 관하여 기술한다. 크리덴셜과 프레젠테이션의 구조와 이에 포함되는 데이터 간의 관계가 설명되며, FinDID를 이루는 개별 컴포넌트들의 역할과 각 컴포넌트들 간의 상호작용하는 방식 또한 설명된다.

1. Data Structure

1.1 Credential

크리덴셜은 사용자에 대한 한 개 이상의 클레임으로 구성된 집합으로 디지털 환경에서 자격 증명서를 나타낸다. 크리덴셜은 단위 신원정보인 클레임을 조합하여 사용자에 대한 신원을 검증할 수 있는 증명서의 역할을 할 수 있다. 여기서 크리덴셜은 검증정보가 포함되어있는 검증 가능한 크리덴셜(VC, Verifiable Credential)의 의미로 사용된다.

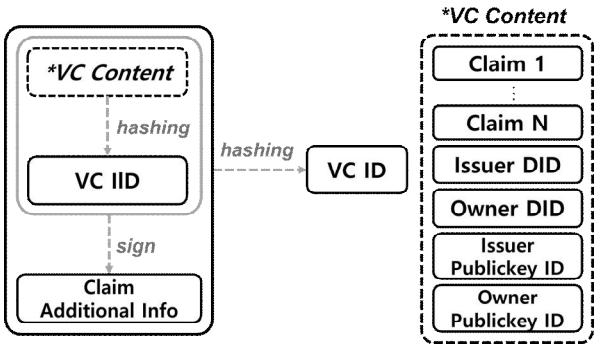

Fig. 1. Structure of Credential

FinDID에서 크리덴셜은 크리덴셜 발급자로부터 발급받을 수 있으며, 발급된 크리덴셜은 크리덴셜 저장소에 보관된다. 크리덴셜의 구조는 그림 1과 같이 클레임을 포함하는 크리덴셜 내용과 이를 해싱한 값인 크리덴셜 IID 그리고 개별 클레임과 크리덴셜 IID를 크리덴셜 발급자 개인키로 서명한 값인 클레임 부가정보, 이 모든 값을 해싱한 크리덴셜의 식별자 역할을 하는 크리덴셜 ID로 구성되어 있다. 크리덴셜 내용 항목에는 클레임 집합과 함께 크리덴셜 발급자와 사용자의 DID 및 공개키 ID가 포함되어있다.

1.2 Presentation

프레젠테이션은 크리덴셜로부터 유도 가능한 클레임의 최소 집합체이다. 무분별한 개인정보 데이터의 유출을 막고자 특정 상황에 맞게 증명 과정에 반드시 필요한 최소한의 클레임만으로 구성한 새로운 형식을 만들어 사용자가 서비스 이용자격 인증을 위해 금융 서비스에 제출한다. 여기서 프레젠테이션은 크리덴셜의 경우처럼 위변조 여부를 검증할 수 있으며 검증 가능한 프레젠테이션(VP, Verifiable Presentation)의 의미로 사용된다.

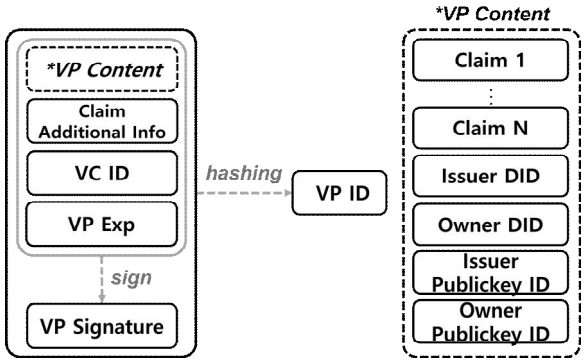

Fig. 2. Structure of Presentation

FinDID에서 프레젠테이션은 사용자가 전자지갑을 통해 크리덴셜에서 필요한 클레임만을 추출하여 생성할 수 있다. 프레젠테이션은 그림 2와 같이 프레젠테이션 내용, 선택된 클레임들의 부가정보, 크리덴셜 ID 그리고 위 정보들을 사용자 개인 키로 서명한 프레젠테이션 서명 값, 마지막으로 위 정보들을 모두 해싱한 프레젠테이션의 식별자 역할을 하는 프레젠테이션 ID 값으로 구성된다. 프레젠테이션 내용 항목에는 크리덴셜로부터 사용자가 선택한 클레임들과 크리덴셜 발급자와 사용자의 DID 및 공개키 ID가 포함되어있다.

2. Component Structure

2.1 DID Registry

DID 저장소는 DID 생성부터 저장, 조회, 폐기 그리고 해당 DID로 발급된 크리덴셜 내역을 관리하는 모든 DID 관련 프로세스를 담당하며, 이 모든 프로세스는 DID 서비스에 의해 통제된다. FinDID에서는 DID 저장소를 DID 관리 컨트랙트와 크리덴셜 관리 컨트랙트로 나누어 구현하여 좀 더 유연한 정보 관리가 가능하다. 그림 3은 DID 관리 컨트랙트에서 관리되는 데이터 및 내부 구조를 나타낸다.

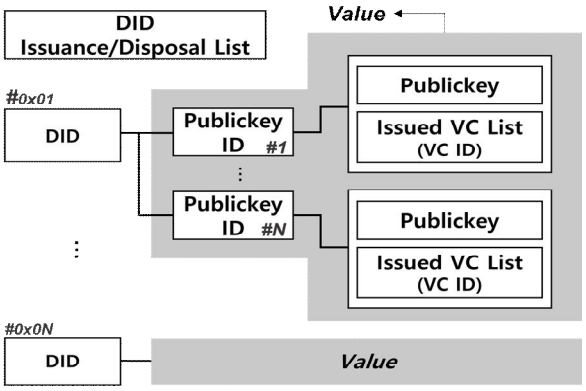

Fig. 3. Structure of DID Management Contract

DID 관리 컨트랙트는 발급된 DID와 DID 주체의 공개키 및 발급된 크리덴셜 목록과 상태 등을 저장하고 관리하는 블록체인 컨트랙트이다. 생성된 전체 사용자의 DID 식별자 목록, DID의 발급과 폐기상태에 대한 정보, 그리고 DID 식별자의 공개키 ID마다 사용자의 공개키와 발급된 모든 크리덴셜의 식별 값인 크리덴셜 ID를 맵핑하고 이를 저장하여 관리한다.

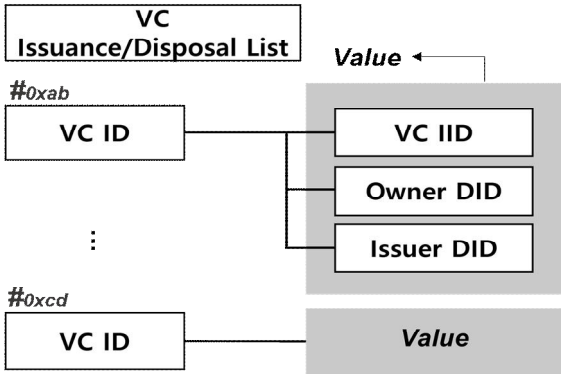

Fig. 4. Structure of Credential Management Contract

그림 4는 크리덴셜 관리 컨트랙트에서 관리되는 데이터 및 내부 구조를 나타낸다. 크리덴셜 관리 컨트랙트는 DID 서비스를 사용하는 인증된 사용자들이 발급받은 모든 크리덴셜 정보가 저장되어있는 컨트랙트이다. 크리덴셜 관리 컨트랙트를 구성하는 데이터에는 전체 크리덴셜에 대한 발급과 폐기목록, 크리덴셜 식별자 값 및 소유자와 발급자 DID를 담고 있다.

2.2 DID Service

DID 서비스는 DID 관리 컨트랙트와 크리덴셜 관리 컨트랙트로 구성된 DID 저장소와 연결되어 이를 총괄하며, 각 사용자의 DID와 크리덴셜의 정보 및 발급 내역을 DID

저장소의 각 컨트랙트를 통해 관리하고 DID 신원 관리체계의 모든 검증과정을 지원한다. DID 생성 및 조회, 검증 그리고 폐기까지 DID에 관련된 모든 프로세스는 DID 서비스를 거쳐서 이루어짐으로 유연하고 신뢰성 있는 DID 서비스를 제공한다.

2.3 Electronic Wallet

전자지갑은 DID 서비스를 이용하기 위하여 필요한 정보인 DID 식별자, 사용자 공개키와 개인 키를 저장한다. 기존의 블록체인 기반의 전자지갑과는 차별적으로 FinDID의 전자지갑은 크리덴셜을 저장하여 관리하고 크리덴셜을 클레임을 추출해 프레젠테이션을 생성하는 기능과 저장하여 관리하는 기능을 제공해주며, DID 서비스를 이용하는 사용자마다 개인적으로 가지고 있다.

2.4 Credential Storage

크리덴셜 저장소는 발급된 물리적인 크리덴셜과 접근권한 제어를 위해 크리덴셜 발급자 목록을 저장하여 관리한다. 개별적인 서버를 가진 별도의 카산드라 데이터베이스[12] 기반의 스토리지로 구성된다. 크리덴셜 ID를 식별자로 크리덴셜을 저장하며, 크리덴셜 발급자로 인증된 기관만이 크리덴셜 스토리지에 크리덴셜을 등록할 권한을 가진다. 또한, 크리덴셜 전체를 조회하는 권한은 크리덴셜 발급자와 크리덴셜 소유자만이 가능한 반면에, 크리덴셜 IID는 누구나 조회가 가능하도록 구성되어있다. 이러한 권한 제어를 위해 크리덴셜 저장소는 크리덴셜 발급자 목록과 크리덴셜 속 DID 정보를 이용해 검증을 진행한다.

2.5 Credential Issuer

크리덴셜 발급자는 사용자에게 크리덴셜을 발급하는 응용 서비스이며, DID를 통한 사용자 신원인증을 통해 신원인증이 완료된 사용자에게 크리덴셜을 발급한다. 또한, 발급 후에는 크리덴셜 저장소에게 크리덴셜을 전달하여 크리덴셜을 안전하게 보관하도록 하며, DID 서비스에게 크리덴셜 발급 내역을 전달한다. DID 서비스는 이를 크리덴셜 관리 컨트랙트에서 관리되도록 하여 크리덴셜 발급 내역의 무결성을 보장한다.

2.6 Financial Service

금융 서비스는 사용자에게 프레젠테이션을 전달받아 사용자의 서비스 이용자격을 검증한 후 관련된 기능을 하는 응용 서비스이다. 금융 서비스는 사용자 신원과 프레젠테이션에 포함된 클레임의 유효성을 검증하기 위하여 필요한 정보를 DID 서비스에게 요청하여 이를 바탕으로 필요한 검증절차를 수행한 후, 검증이 완료된 사용자에게만 서비스 이용을 허용한다.

IV. Process of FinDID

본 장에서는 FinDID의 진행 과정에 관하여 기술한다. 주요 과정으로는 크게 2개의 절로 DID Registration 과정과 DID Authorization 과정으로 나눈다. **DID Registration** 과정은 사용자로부터 DID 발급 요청에 따라, DID 관리 컨트랙트에 기록된 발급 내역으로 사용자에게 발급된 DID가 있는지 조회하고 신규 사용자에겐 DID를 발급 및 기록하는 과정과 기존 사용자에겐 이전에 발급받은 DID를 전달하는 과정으로 나뉘어 설명한다. **DID Authorization** 과정은 DID를 이용하여 사용자에 대한 신원을 체계적으로 검증하는 과정으로 크리덴셜 생성과 프레젠테이션 검증 단계로 나눌 수 있다. 또한, 각 과정에서 일어날 수 있는 예외 상황에서 대처하는 과정을 함께 설명한다.

FinDID의 각 과정에서 일어나는 모든 신원확인을 위한 검증은 DID 검증을 기반으로 진행된다. DID 검증을 위해선 필요한 검증정보들이 있으며, 본 장에서는 이를 *DID 검증정보*로 설명한다. DID 검증정보에는 신원확인이 필요한 주체의 DID, 해당 주체의 공개키 ID, 해당 주체의 개인 키로 서명한 서명 값 그리고 이 서명을 위해 사용된 데이터가 포함된다. 서명에 사용된 데이터는 DID 검증 목적에 따라서 달라질 수 있다.

1. DID Registration

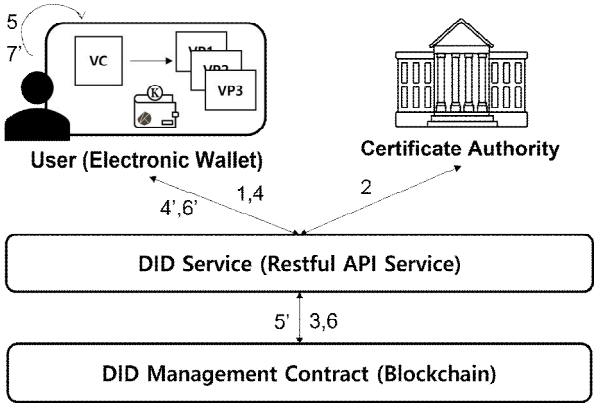

Fig. 5. DID Registration Process

[step1-3 in fig. 5] 사용자로부터 사용자 신원정보와 함께 DID 발급 요청을 받으면, DID 서비스는 전달받은 사

용자 신원정보로 공인기관을 통해 사용자의 신원 인증을 진행한다. 신원이 확인되면, DID 서비스는 DID 관리 컨트랙트에 해당 사용자가 이전에 DID를 발급받은 내역이 있는지 조회한다. 조회를 통해 중복되는 DID가 없으면 **DID 생성과정**인 step4-6을 진행하며, 중복되는 DID가 있으면 **DID 조회과정**인 step4'-7'을 진행한다.

[step4-6 in fig. 5] DID 서비스는 사용자로부터 받은 사용자 신원정보를 이용해 DID 식별자와 사용자 공개키 ID를 생성하여, 사용자에게 발급한다. 사용자는 발급받은 DID를 사용자 전자지갑에 저장한다. DID 서비스는 DID 관리 컨트랙트에 생성한 사용자 DID 식별 값에 사용자 공개키 ID와 사용자의 공개키와 함께 발급 상태를 맵핑하여 저장 및 관리한다.

[step4'-7' in fig. 5] DID 서비스는 사용자에게 공개키 ID, 공개키 그리고 사용자의 개인 키로 공개키 ID를 서명한 값을 요청한다. 사용자로부터 전달받은 공개키 ID와 서명 값으로 DID 서비스는 DID 관리 컨트랙트에서 조회된 DID에 대해 공개키 ID와 서명 값을 이용해 DID 검증을 진행할 수 있다. DID 서비스는 DID 검증이 완료되면, 해당 DID를 사용자에게 전달하고 사용자는 전달받은 사용자의 DID를 전자지갑에 저장한다.

2. DID Authorization

2.1 Issue Credential

그림 6은 DID 검증을 통한 크리덴셜 발급 프로세스를 설명한다.

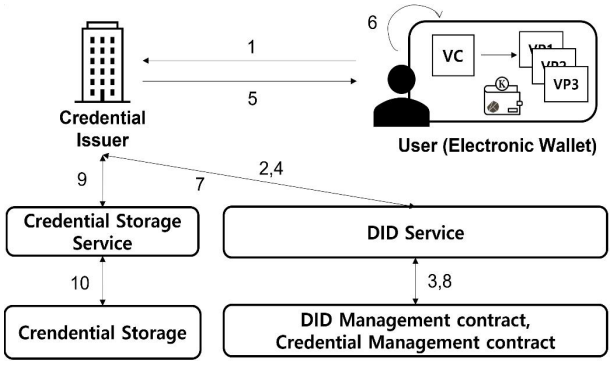

Fig. 6. Issue Credential Process

[step1-5 in fig. 6] 사용자는 DID 검증정보를 이용하여 크리덴셜 발급자에게 신원확인 크리덴셜 발급을 요청한다. 요청을 받은 크리덴셜 발급자는 DID 서비스에게 사용자의 DID를 이용한 신원 인증을 요청한다. 요청을 받은 DID 서비스는 사용자의 정보에 해당하는 공개키를 DID 관리 컨트랙트에서 조회하여 사용자의 신원 인증을 진행한다. 유효한 신원으로 확인되면 DID 서비스는 발급자에게 신원 인증이 완료됨을 알리고, 발급자는 사용자에게 크리덴셜을 발급한다.

[step6-8 in fig. 6] 사용자는 크리덴셜 발급자에게 발급받은 크리덴셜을 전자지갑에 저장한다. 크리덴셜 발급자는 크리덴셜 발급 내역을 DID 서비스에게 전달한다. DID 서비스는 전달받은 크리덴셜 발급 내역을 크리덴셜 컨트랙트에 기록한다.

[step9-10 in fig. 6] 발급 내역뿐만 아니라 크리덴셜 발급자는 물리적으로 크리덴셜을 저장하기 위해 크리덴셜 저장소 서비스에게 발급한 크리덴셜의 저장을 요청한다. 크리덴셜 저장소 관리 서비스는 요청한 크리덴셜 발급자의 크리덴셜 저장소 접근 권한을 확인한 후, 유효한 권한을 가진 발급자로 확인되면 요청한 크리덴셜을 크리덴셜 저장소에 기록한다.

그림 7은 그림 6에서 설명한 크리덴셜 발급 프로세스에서 사용자A의 DID와 공개키 ID가 해커에 의해 탈취 당했을 경우 이를 대처하는 과정에 대해 설명한다.

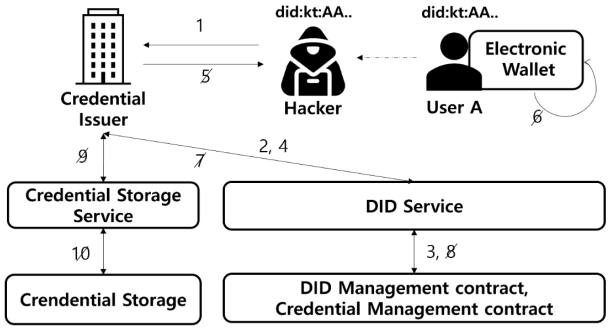

Fig. 7. An Exception to Issue Credential Process

[step1 in fig. 7] 해커는 탈취한 사용자A의 DID와 공개키 ID를 사용하여 DID 검증정보를 생성한 후 DID 검증정보를 통해 크리덴셜 발급자에게 크리덴셜 발급을 요청한다. **[step2 in fig. 7]** 크리덴셜 발급자는 전달받은 DID 검증정보를 통해 DID 서비스에게 요청한 사용자(해커)의 신원인증을 요청한다. **[step3 in fig. 7]** DID 서비스는 DID 검증정보에 포함된 DID와 공개키 ID를 통해 DID 관리 컨트랙트에서 해당하는 DID 문서를 추출한다. **[step4 in fig. 7]** 그러나 해커가 생성한 DID 검증정보에 포함된 서명 값이 올바르지 않기 때문에 신원인증은 실패되며, 신원인증 완료 시 실행되어야 할 모든 과정은 무효화 된다.

이처럼 단지 DID와 공개키 ID와 같은 DID 검증의 핵심 정보가 탈취당해서 해커에 의해 사용되는 예외 상황이 발생하더라도 FinDID에서의 DID 검증은 여러 단계를 거쳐 안전하게 이루어지기 때문에 대처할 수 있다.

2.2 Presentation Verification

DID 검증 및 프레젠테이션 검증과정을 설명한다. 사용자는 금융 서비스에게 프레젠테이션을 통해 서비스 이용 요청을 한다. 금융 서비스는 프레젠테이션의 신뢰성과 유효성을 검증하기 위해 프레젠테이션 서명 값 검증, 위변조 검증, 유효기간 검증, 클레임 검증의 4단계를 거쳐 체계적인 검증을 수행한다. 프레젠테이션 속 클레임 검증은 프레젠테이션 속 개별 클레임의 검증을 말하며, 클레임의 출처인 크리덴셜이 유효하며, 각 클레임들이 하나의 크리덴셜로부터 유도된 것이 맞는지를 검증하는 절차이다.

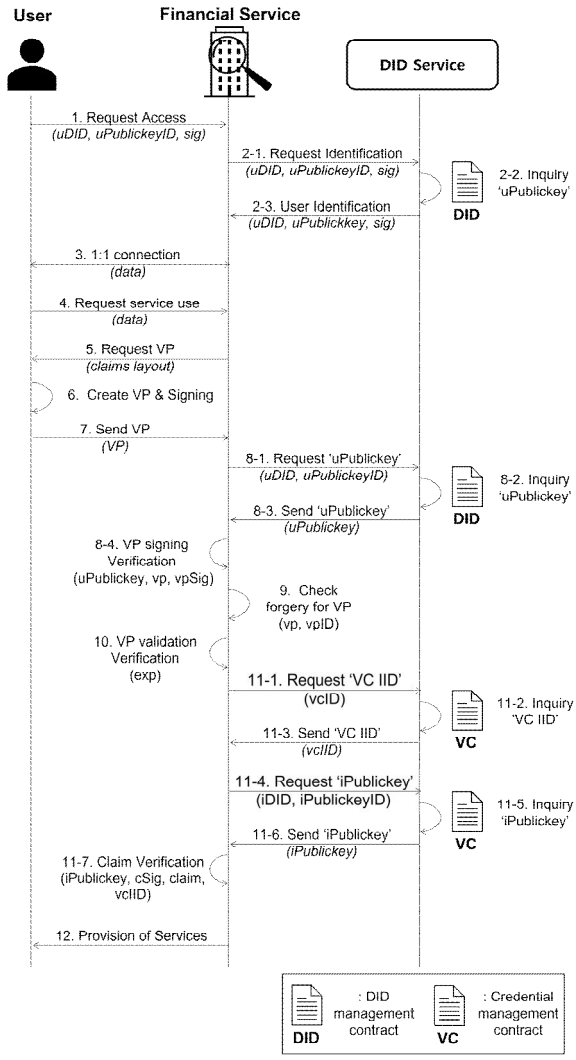

Fig. 8. Verification Presentation Process

[step1-3 in fig. 8] 사용자는 금융 서비스에게 사용자의 DID, 공개키 ID, 사용자의 DID에 개인 키로 서명한 서명 값이 담긴 DID 검증정보를 전달하며 접속을 요청한다. 금융 서비스는 DID 서비스에게 사용자에게 전달받은 DID, 공개키 ID, 서명 값으로 DID 서비스에게 사용자 신원증명을 요청한다. DID 서비스는 사용자 신원증명 요청에 따라 DID 관리 컨트랙트를 통해 사용자 공개키를 조회하고, 조회된 사용자 공개키를 사용하여 사용자의 신원 인증을 DID 검증 방식으로 진행한다. 검증이 완료되면 금융 서비스는 사용자 신원인증이 이루어짐에 따라 사용자와의 1:1 통신 채널을 수립하여 서비스 사용 요청을 가능하게 한다.

[step4-7 in fig. 8] 사용자는 수립된 통신 채널을 통해 금융 서비스에게 서비스 이용 요청을 한다. 금융 서비스는 서비스 제공에 필요한 클레임을 포함하는 프레젠테이션을 요청한다. 사용자는 전자지갑을 통해 이전에 발급받은 크리덴셜에서 필요한 클레임들을 선택하여 프레젠테이션을 생성하여 금융 서비스에게 전달한다.

Table 1. Pseudo-code for [§fig. 8. step8 -step11]

Presentation Verify Process	
vp.value : Value included in vp. uValue : Value for user. iValue : Value for issuer.	
Step 8. Verify VP signature	
1:	uPublickey = request_to_DIDSvc(vp.uDID, vp.uPublickeyID);
2:	vpSig = vp.signature;
3:	vp = vp_except_sig;
4:	finDID.didAuth(uPublicKey, vp, vpSig); *//True or False*
Step 9. Check forgery for VP	
5:	vpID = vpID_included_in_vp;
6:	gen_vpID = keccak256(vp_except_vpID);
7:	is_equal(vpID, gen_vpID); *//True or False*
Step 10. Verify EXP	
8:	if(currentTime < vp.exp) return True;
Step 11. Verify Claim	
9:	vcIID = request_to_VCStorage(vp.vcID);
10:	iPublickey = request_to_DIDSvc(vp.iDID,vp.iPublickeyID);
11:	cSig = vp.cSig; *//VC_additional_Information*
12:	finDID.didAuth(iPublicKey, cSig, {vp.claim, vcIID}); *//True or False*

[step8 in fig. 8] 금융 서비스는 사용자에게 받은 프레젠테이션의 체계적인 검증을 진행한다. 우선 금융 서비스는 프레젠테이션 속 프레젠테이션 서명 값을 통해 해당 프

레젠테이션이 사용자가 생성한 프레젠테이션이 맞는지 검증을 진행한다. DID 서비스를 통해 DID 관리 컨트랙트에게 사용자의 공개키 ID와 DID를 전달하여 사용자 공개키를 조회한다. 이후 해당 공개키로 프레젠테이션, 프레젠테이션을 서명한 프레젠테이션 서명 값으로 DID 검증 진행하여 프레젠테이션 서명 값을 검증한다.

[step9 in fig. 8] 금융 서비스는 프레젠테이션 서명 값이 검증 완료됨에 따라 프레젠테이션 내용 위변조 검증을 진행한다. 금융 서비스는 사용자에게 전달받은 프레젠테이션에서 프레젠테이션 ID를 제외한 모든 값을 해싱하여 프레젠테이션 ID를 재생성하고 이를 사용자로부터 전달받은 프레젠테이션 ID와 비교하는 방식으로 프레젠테이션 위변조 여부를 확인한다.

[step10 in fig. 8] 다음 검증으로 프레젠테이션 유효기간을 확인하여 프레젠테이션이 유효한 프레젠테이션이 맞는 지 검증한다.

[step11-12 in fig. 8] 프레젠테이션의 유효성을 확인하면, 프레젠테이션의 클레임 검증을 진행한다. 금융 서비스는 프레젠테이션 속에 포함된 크리덴셜 ID를 크리덴셜 저장소에 전달하여 이에 해당하는 크리덴셜 IID를 요청한다. 금융 서비스가 크리덴셜 저장소로부터 조회된 크리덴셜 IID를 전달받으면 클레임과 크리덴셜 IID를 크리덴셜 발급자의 개인 키로 서명한 값인 선택된 클레임 부가정보를 검증하기 위해 DID 서비스를 통해 DID 관리 컨트랙트에 크리덴셜 발급자의 DID와 공개키 ID를 전달하며 크리덴셜 발급자의 공개키를 요청한다. DID 관리 컨트랙트는 크리덴셜 발급자의 DID와 공개키 ID에 해당하는 발급자 공개키를 DID 서비스를 경유하여 금융 서비스에게 전달한다. 금융 서비스는 전달받은 크리덴셜 발급자 공개키와 크리덴셜 IID, 프레젠테이션 속 클레임, 선택된 클레임들의 부가정보 값을 통해 DID 검증을 진행하여 각 클레임들의 유효성을 검증한다. 금융 서비스는 클레임 검증이 이루어져 프레젠테이션을 통한 모든 검증절차가 완료됨에 따라, 사용자에게 서비스를 제공한다.

그림 9를 통해 그림 8에서 설명한 프레젠테이션 생성 및 검증 프로세스에서 해커가 사용자의 여러 검증정보를 탈취하여 금융 서비스에 접근할 경우 대처하는 과정에 대하여 설명한다. 그림 9는 해커가 탈취한 검증정보와 이를 통해 서비스에 접근하여 서비스를 요청하는 시점, 예외가 처리되어 해커의 요청이 무효화되는 시점을 타임스탬프 형태로 나타낸다.

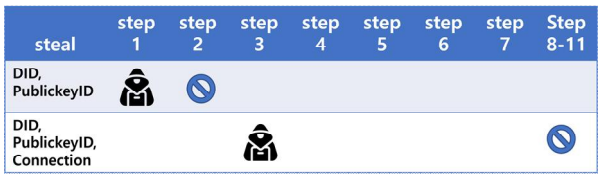

Fig. 9. An Exception to Verification Presentation Process

그림 9에서 첫 번째로 해커가 그림 8의 step 1 과정에서 사용자의 DID와 공개키 ID를 탈취하여 DID 검증정보를 생성해 금융 서비스에 접속을 요청한다. 그러나, DID 검증 시 요구되는 사용자의 개인 키를 통해 서명한 서명 값 검증에 실패하므로 해당 요청과 이후 과정들은 모두 무효화 된다. 그림 9에서 두 번째로 해커가 그림 8의 step 3 과정에서 사용자의 DID와 공개키 ID뿐만 아니라 1:1 통신 채널에 접속할 수 있는 데이터까지 탈취하였다고 가정한다. 또한, 탈취한 정보를 통해 그림 8의 step 4-7까지의 과정은 수행하였다고 가정한다, 그러나 step 8 과정에서 프레젠테이션 서명 값 검증이 요구되는데, 해당 검증과정에서 해커가 생성한 프레젠테이션에 포함된 서명 값이 올바르지 않기 때문에 프레젠테이션 검증은 실패되며, 검증 완료 시 실행되어야 할 모든 과정도 무효화 된다.

V. Implementation Result

이 장은 가상의 시나리오를 토대로 FinDID를 이용해 서비스들의 동작 과정을 사용자 인터페이스를 통해 설명하고, 시나리오를 통해 생성된 크리덴셜과 프레젠테이션의 실제 구조를 보여준다.

1. DID Registration Process

이 절에서는 아래의 가상 시나리오를 토대로 FinDID를 이용해 실험적인 응용 서비스들이 동작하는 과정을 사용자 인터페이스를 통해 설명한다.

사용자는 'BB Shopping Mall'의(§Fig. 16, BB Shopping Mall) 금융 서비스를 이용하기 위해 사용자의 카드 정보를 등록하려고 한다. 이를 위해 'AA Card Company'에서(§Fig. 13, AA Card Company) 등록할 카드에 대한 크리덴셜을 발급받아야 하고, 사용자 전자지갑을 통해 발급받은 크리덴셜에서 필요한 클레임만을 추출하여 프레젠테이션을 생성한다. 이후 생성된 프레젠테이

션을 'BB Shopping Mall'에게 제출하여 카드등록을 완료할 수 있다.

(1) DID 생성 및 조회

그림 10은 사용자가 DID를 발급받기 전 사용자 전자지갑의 메인화면이다.

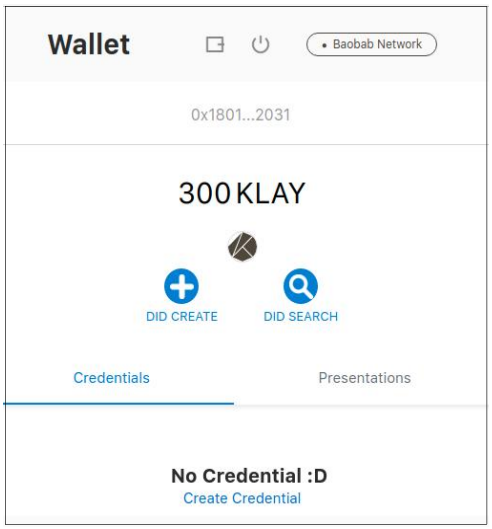

Fig. 10. Electronic Wallet : Credential page

사용자는 DID를 발급받기 위해 그림 10의 DID CREATE 버튼을 클릭한다. 이후 DID 생성 시 필요한 사용자 정보 입력 창이 나타나며, 그림 11과 같이 사용자가 각 정보를 올바르게 입력할 수 있다. 입력이 완료되면, 그림 11의 아래의 Create DID 버튼을 클릭하여 4장 1절의 "DID Registration" 과정 중 DID 생성 과정인 step1-6을 거쳐 DID가 생성되며, 사용자에게 발급된다.

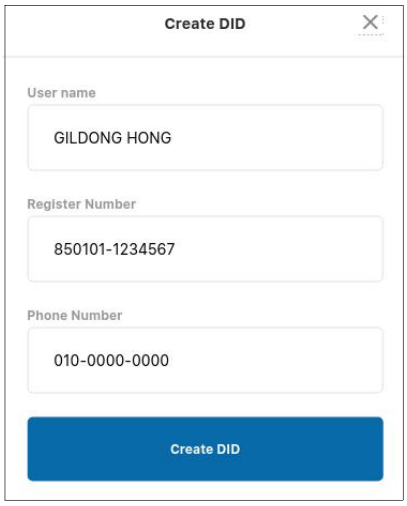

Fig. 11. Electronic Wallet : Create DID

사용자가 DID를 분실하였을 경우, 사용자는 자신의 DID를 조회하기 위해 그림 10의 DID SEARCH 버튼을 클릭한다. 해당 버튼을 클릭하면, 그림 12의 화면이 나타나고, 이 화면에서 사용자의 정보를 입력한 후 Search DID 버튼을 클릭하면 4장 1절의 "DID Registration" 과정 중 DID 조회 과정을 따라 사용자는 안전하게 DID를 조회할 수 있다.

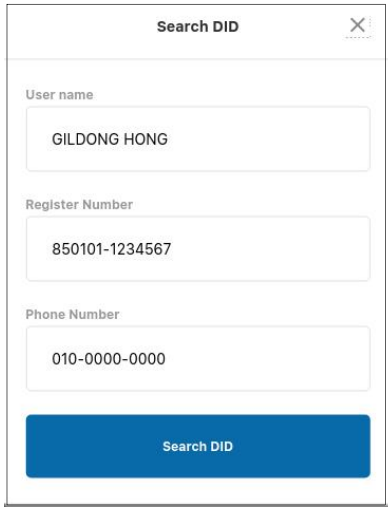

Fig. 12. Electronic Wallet : Search DID

(2) 크리덴셜 발급

DID를 생성한 사용자는 크리덴셜을 크리덴셜 발급자를 통해 발급받아 사용자의 전자지갑에 저장하여 사용할 수 있다. 그림 13은 'AA Card Company'에서 사용자가 크리덴셜을 발급받을 카드를 선택하는 화면이다. 사용자는 'AA Card Company'에서 사용자가 소유한 카드 목록을 확인할 수 있으며, 크리덴셜을 발급받을 카드를 선택할 수 있다.

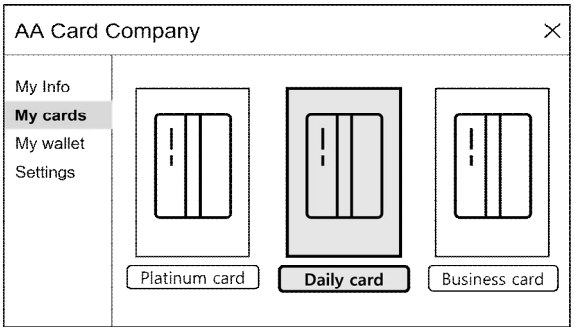

Fig. 13. AA Card Company User Interface : Select card

그림 14는 앞서 선택한 카드에 대한 정보를 보여주는 화면이다. 아래의 Create Credential 버튼을 클릭하면 크리덴셜을 생성하는 4장 2.1절의 'Issue Credential' 과정

을 통해 카드 정보를 담은 크리덴셜이 생성되고 사용자에게 발급된다. 발급된 크리덴셜은 사용자의 전자지갑에 저장되며 그림 15은 크리덴셜이 저장된 전자지갑 화면을 보여준다. 생성된 크리덴셜의 실제 구조는 그림 20의 Credential과 같다.

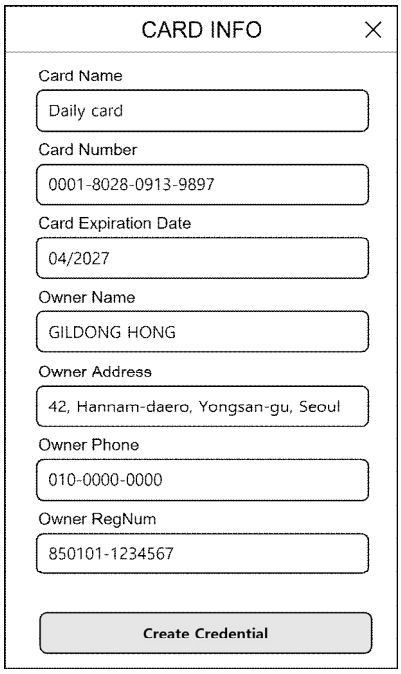

Fig. 14. AA Card Company User Interface : Create Credential

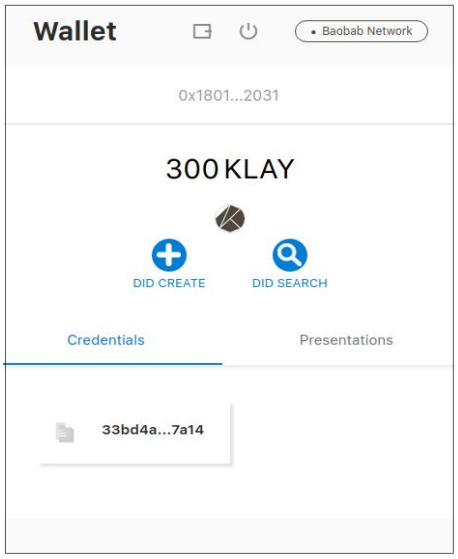

Fig. 15. Electronic Wallet : Credential page

(3) 프레젠테이션 생성 및 검증

크리덴셜을 발급받아 전자지갑에 저장하고 있는 사용자는 발급된 크리덴셜을 통해 프레젠테이션을 생성할 수 있다. 그림 16은 사용자가 'BB Shopping Mall'에 자신의 카드를 등록하기 위해 Add Card 버튼을 클릭하는 화면이다.

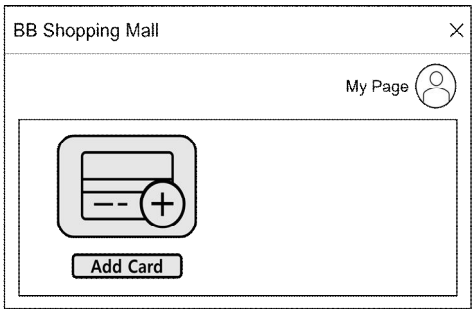

Fig. 16. BB Shopping Mall User Interface : Add Card

그림 17는 카드등록을 위한 검증과정에 필요한 클레임들의 목록을 사용자에게 보여주는 화면이다.

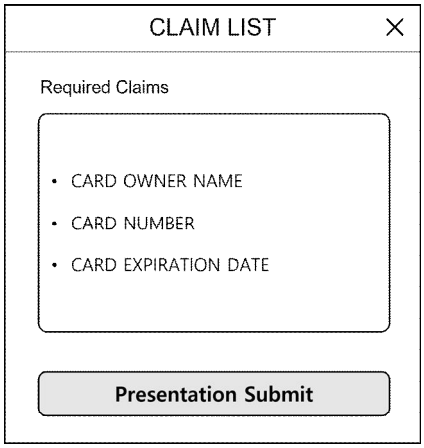

Fig. 17. BB Shopping Mall User Interface : View Required Claim

그림 18은 사용자가 전자지갑을 통해 발급받았던 크리덴셜에서 'BB Shopping Mall'에 제출하기 위하여 필요한 클레임을 선택하여 프레젠테이션을 생성하는 화면이다. 생성된 프레젠테이션의 실제 구조는 그림 20의 Presentation과 같다.

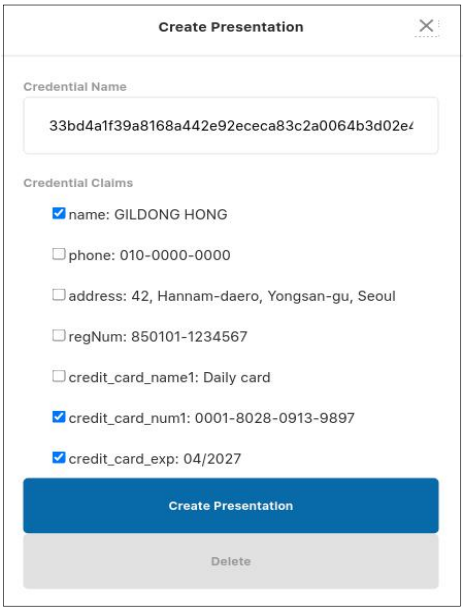

Fig. 18. Electronic Wallet : Create Presentation

사용자는 그림 17의 목록을 토대로 그림 18과 같이 전자지갑을 통해 프레젠테이션을 생성한 후, 그림 17의 하단 프레젠테이션 제출 버튼을 클릭한다. 버튼이 클릭 되면 4장 2.2절의 'Presentation Verification' 과정으로 체계적인 프레젠테이션 검증이 진행된다.

그림 19는 프레젠테이션의 검증이 완료된 후 'BB Shopping Mall' 서비스에 사용자의 카드가 등록이 완료됨을 보여주는 화면이다.

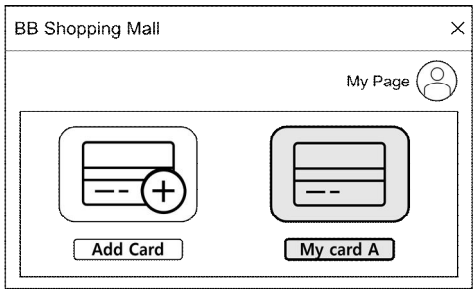

Fig. 19. BB Shopping Mall User Interface : Registration completed

그림 20는 위 과정에서 생성되는 크리덴셜과 프레젠테이션의 실제 구조를 나타낸다. 그림 20에서 claims 항목은 개별 클레임 집합을 나타내며, 이 값들과 크리덴셜 IID(§Fig. 20, ciid)를 크리덴셜 발급자의 개인 키로 서명한 값인 크리덴셜 부가정보는 그림 20의 infos 항목에서 나타난다.

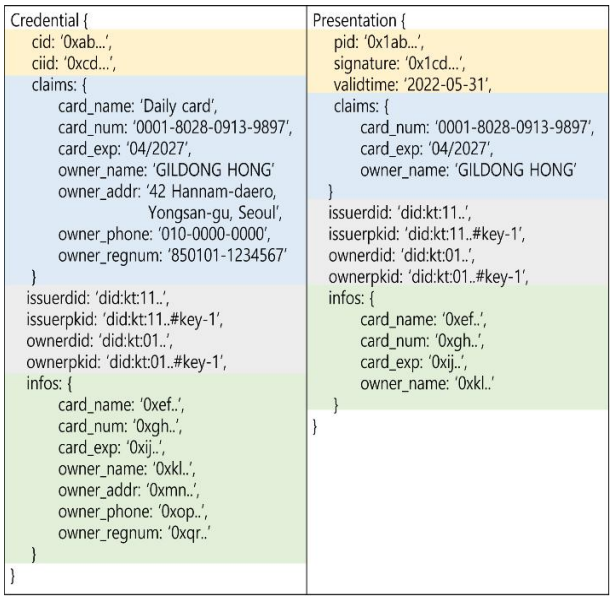

Fig. 20. Result : Credential and Presentation

VI. Conclusions

본 논문에서는 금융권 DID 서비스 체계의 표준 방식을 준수하는 가운데 체계적인 검증 방식을 통하여 개인 정보나 자격증명을 유연하게 제어할 수 있는 블록체인 기반의 DID 서비스인 FinDID에 대하여 기술하였다. 이를 위하여 표준 방식을 준수하면서 프레젠테이션에 포함된 개별 클레임에 대한 무결성을 보장하는 체계적인 검증과정을 개발하였다. FinDID는 이를 바탕으로 프레젠테이션을 통해 사용자의 자격 검증이 확실하게 이루어질 수 있도록 보장하는 DID 서비스를 제공한다. 또한, 실험적인 응용 서비스를 개발하여 실제 응용 서비스들이 FinDID를 이용해 동작하는 과정의 이해를 돕고, 각 과정이 신뢰성 있게 진행되는지 증명하였다. 연구 결과는 표준 방식의 DID를 지원하는 FinDID 서비스를 통해 실생활에서 체계적으로 신원을 검증받을 수 있는 안전한 신원검증체계가 실현될 수 있음을 보여준다. 다만, 본 연구에서는 간단한 검증 동작만을 지원하는 발급자와 검증자 응용 서비스로서 사용자가 실제로 사용하기에는 다소 미흡한 점이 존재한다. 따라서 향후 연구로는 추후 개발된 기법을 적용한 FinDID의 각종 구성요소를 실제적인 금융 서비스에서 활용할 수 있도록 서비스를 발전시킬 계획이다.

ACKNOWLEDGEMENT

This research was partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(No. 2019R1I1A3A01052970)

REFERENCES

[1] Drummond Reed, et al. "Decentralized Identifiers (DID) v1.0", W3C Working Draft, https://www.w3.org/TR/did-core

[2] Clemens Brunner, et al. "DID and VC:Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust", 2020 the 3rd International Conference on Blockchain Technology and Applications, pp. 61-66, New York, USA, Dec 2020. DOI: 10.1145/3446983.3446992

[3] Kim. Hye-Won, et al. “BCON : Blockchain-Based Content Management Service Using DID.” Journal of the Korea Society of Computer and Information, Vol. 26, No. 6, pp. 97-105, Jun 2021. DOI: 10.9708/JKSCI.2021.26.06.097

[4] Lee. Young-Eun, et al. “NextAuction: A DID-Based Robust Auction Service for Digital Contents.” Journal of the Korea Society of Computer and Information, Vol. 27, No. 2, pp. 115-124, Feb 2022. DOI: 10.9708/JKSCI.2022.27.02.115

[5] Kwon. Min-Ho, et al. “InfoDID: A Robust User Information Management Serivce Based on Decentralized Identifiers.” Journal of the Korea Society of Computer and Information, Vol. 26, No. 4, pp. 75-84, Apr 2021. DOI: 10.9708/JKSCI.2021.26.04.075

[6] Coinplug, MYKEEPiN, https://coinplug.com/mykeepin#mykeepin_app

[7] IconLoop, Zzeung, https://www.iconloop.com/services/

[8] RAON OmniOne Enterprise, RAON, https://www.raoncorp.com/ko/main

[9] BANK OF KOREA, Service Employment and Sharing Scheme using Decentralized Identity in The Financial Sector, https://www.bok.or.kr/portal/bbs/B0000239/view.do?nttId=10068344&menuNo=200729&pageIndex=1

[10] Klaytn, Kaikas Docs, https://docs.kaikas.io

[11] D. Mohanty, "Ethereum Use Case," Ethereum for Architects and Developers, pp. 203-243, Oct 2018. DOI: 10.1007/978-1-4842-4075-5_9

[12] Cassandra Apache, https://cassandra.apache.org

Authors

Young-Eun Lee received the B.S degrees in IT convergence from University of Ulsan, Korea, in 2021. She is currently an M.S student in Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan. She is interested in blockchain technology, distributed computing, and Artificial Intelligence technology.

Hye-Won Kim received the B.S degrees in IT convergence from University of Ulsan, Korea, in 2021. She is currently an M.S student in Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan. She is interested in blockchain technology, distributed computing, and Artificial Intelligence technology.

Myung-Joon Lee received the B.S. degree in Mathematics from Seoul National University in 1980, and the M.S. and Ph.D. degrees in Computer Science from KAIST in 1982 and 1991, respectively.

Dr. Lee joined the faculty of the Department of Computer Science at University of Ulsan, Ulsan, Korea, in 1982. He is currently a Professor in the School of IT Convergence, University of Ulsan. He is interested in blockchain technology, distributed computing, and mobile/cloud service.