논문 22-47-04-11 The Journal of Korean Institute of Communications and Information Sciences '22-04 Vol.47 No.04
https://doi.org/10.7840/kics.2022.47.4.656

자기주권신원에 기반한 검증 가능한 자격증명의 안전한 위임 기법

임 승 주◆, 김 기 형°

Safe Transfer Method of Verifiable Credentials Based on Self-Sovereign Identity

Seungjoo Lim◆, Ki-Hyung Kim°

요 약

디지털 신원 모델에서 자기주권성(Self-Sovereignty) 보장의 중요성이 점차 중요해지면서 자기주권신원(Self-Sovereign Identity)이 급부상하고 있다. 자기주권신원을 실현하고자 W3C(World Wide Web Consortium)가 표준화중인 검증 가능한 자격증명(Verifiable Credentials, VC)이 대표적이다. 그러나 검증 가능한 자격증명의 표준은 인증(Authentication)에 대해서만 명시하고 있을 뿐, 인가(Authorization)에 대해서는 명시하고 있지 않다. 검증 가능한 자격증명에 기반한 인가 프레임워크의 적절한 구현에 대한 필요성만 명시되어 있을 뿐, 보안 요구사항이나 자세한 구조에 대한 명세가 부재하기 때문에 자기주권성이 침해될 우려가 있다. 특히 검증 가능한 자격증명의 표준에서 타인에게 자격증명을 전송하는 경우에 대한 명세가 부족해 이 경우의 자기주권성이 보장되기 어렵다. 따라서 본 논문에서는 자기주권성을 지키면서 타인에게 안전하게 자격증명을 전송하는 기법을 제안한다.

Key Words : Self-Sovereign Identity, Blockchain, Network Security, Identification, Authorization

ABSTRACT

Self-Sovereign Identity(SSI) is rapidly emerging as the importance of self-sovereignty guarantee becomes increasingly important in the digital identity model. World Wide Web Consortium(W3C) is standardizing the Verifiable Credential(VC) to realize SSI. While the standards for VC focus on the authentication, the authorization is relatively not yet dealted with, only mentioning the need for the appropriate implementation of an authorization framework based on VC and a risk of infringement of self-sovereignty because there is no specification of security requirements or detailed structures. In particular, it is difficult to guarantee self-sovereignty in this case due to the lack of specifications for transmitting credentials to others in the VC standard. This paper proposes a method for safely transmitting credentials to others while protecting self-sovereignty.

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업과 2021년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원과 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원의 연구결과로 수행되었음. (IITP-2021-2021-0-01835, P0008703, 2021년 산업혁신인재성장지원사업, 2021R1F1A1045861, 2021-0-00590, 대규모 노드에서 블록단위의 효율적인 거래 확정을 위한 최종성 보장 기술개발)
◆ First Author : Ajou University Department of Computer Engineering, dlaking@ajou.ac.kr, 학생회원
° Corresponding Author : Ajou University Department of Cyber Security, kkim86@ajou.ac.kr, 종신회원
논문번호 : 202112-336-B-RN, Received December 19, 2021; Revised February 14, 2022; Accepted February 21, 2022

Ⅰ. 서 론

전자기기의 사용은 점차 보편화되어 개인용 컴퓨터나 스마트폰 같은 단말기와 인터넷은 일상생활에서 빼놓을 수 없는 존재로 자리매김하고 있다. 위와 같은 일상의 디지털화는 온라인뱅킹, 서류발급, 신원인증 등 기존의 대면 서비스를 전산화하여 비대면 서비스로 전환하는 등 일상에 큰 변화를 야기했다. 서비스를 안전하게 제공하기 위해서 다양한 암호화 기법들과 정보보호기법들이 대거 등장하였고, 신원증명의 경우 구글이나 페이스북, 애플 같은 신뢰할 수 있는 제3자의 보증에 의존하는 디지털 신원 모델이 등장하여 널리 사용되고 있다.

그러나 기존의 디지털 신원 모델은 이를 보증해주는 기관에 지나치게 의존적이기 때문에 신원주체의 자기주권성이 보장되기 어렵다는 문제점이 꾸준히 제기되고 있다. 이를 해결하고자 분산원장기술을 활용하여 자기주권신원(Self-Sovereign Identity)[1]을 실현하려는 시도가 이루어지고 있다. 대표적으로 DID(Decentralized Identifier)[2]와 VC(Verifiable Credentials)[3]와 같은 기술이 존재하며, 이는 W3C에 의해서 표준화가 진행 중에 있으며, 이에 기반한 서비스도 다양하게 개발되고 있어 국내에서도 이에 대한 대응 및 관련 논의가 필요하다.[4]

VC 표준은 인증(Authentication)절차에 대해서만 명시하고 있을 뿐, 인가(Authorization)절차에 대해서는 따로 명시하고 있지 않다. 인증은 특정 시스템으로의 접근을 허용하기 전에 신원을 검증하는 것을 말하며, 인가는 인증된 사용자에게 어떤 수준의 권한과 서비스를 허용하는 것을 말한다. 그러나 VC 표준에는 VC를 활용한 인가 프레임워크가 어떻게 동작해야하는지, 어떤 동작이 존재할 수 있는지에 대해서는 설계자의 자율에 맡기고 있다. 명시의 부재로 인해서 VC 기반의 인가 프레임워크가 설계자의 자율로 개발될 경우 자기주권성이 침해될 우려가 있으며, 특히 신원주체가 자신의 자격증명(Credential)을 타인에게 전달·위임하는 경우 자기주권성이 보장되지 않는다. 본 논문에서는 신원주체의 자기주권성을 보호하고 자기주권신원 기반의 인가 프레임워크의 안전한 설계를 위해서 자격증명의 안전한 전송 기법을 제안한다.

Ⅱ. 본 론

2.1 자기주권신원

자기주권신원은 현재까지도 대중적으로 사용되고 있는 암호화 프로토콜인 TLS(Transport Layer Security)표준의 공동저자이자 암호학을 사용하여 중앙화된 구조에 저항하는 집단인 Cypherpunk의 일원인 Christopher Allen이 2016년에 자신의 블로그를 통해 제안한 개념으로,[1] 디지털 신원 모델의 탈중앙화 필요성을 제시한 중요한 주제로서 평가되고 있다. 기존의 디지털 신원 모델은 서비스 제공자나 중앙기관 등의 제3자 의존도가 매우 높아 중앙화되어 있기 때문에 공격자들의 주요 표적이 되거나 대규모의 개인정보 유출이 일어날 수 있으며, 신원주체의 권한이 중앙기관에 의해서 침해될 수 있어 완전히 보장되지 않는다는 단점이 존재한다. 따라서 Christopher Allen은 “You Can’t Spell Identity without an I”[1]라는 문장을 들며 신원주체의 존재 없이는 신원인증을 언급할 수 없다고 지적하며 자기주권신원의 필요성을 주장하였다.

자기주권신원의 명백한 정의는 아직 합의가 이루어지지 않아 Christopher Allen은 자기주권성 보장을 위한 10가지 요구사항을 표 1과 같이 주장하고 있다. 표 1에 따르면, 신원주체는 자신의 신원정보를 반드시 통제·접근할 수 있어야하고, 이를 위한 시스템은 반드

표 1. 자기주권신원의 10가지 원칙
Table 1. 10 Principles of Self-Sovereign Identity

원칙	설명
Existence (실존성)	신원주체는 반드시 실체를 가진 독립적인 존재여야 한다.
Control (통제권)	신원주체는 반드시 자신의 신원을 통제할 수 있어야 한다.
Access (접근성)	신원주체는 반드시 자신 소유의 데이터에 접근할 수 있어야 한다.
Transparency (투명성)	자기주권신원을 구성하는 시스템과 알고리즘은 반드시 투명하게 공개되어 있어야 한다.
Persistence (지속성)	신원은 반드시 반영구적으로 사용될 수 있어야 한다.
Portability (이동성)	신원과 관련된 정보나 서비스들은 반드시 전송가능(Transportable)한 것이어야 한다.
Interoperability (호환성)	신원은 가능한 한 시스템이나 서비스에 구애받지 않고 폭넓게 사용할 수 있어야 한다.
Consent (동의)	신원주체는 자신의 신원이 활용되는 것에 반드시 동의해야한다.
Minimalization (최소화)	신원정보의 노출은 반드시 최소화되어야 한다.
Protection (보호)	신원주체의 권한은 반드시 보호되어야 한다.

시 공개되어 있으며 상호호환성과 신원주체의 권한을 보장해야 한다.

2.2 Verifiable Credential

Verifiable Credential(VC)은 자기주권신원을 실현하고자 2018년 Rebooting Web of Trust(RWOT) 워크샵에서 Nate Otto에 의해서 제안되어[5] W3C에서 표준화에 착수한[3] 신원증명 기술이다. VC는 분산원장을 활용하여 중앙기관의 개입을 가능한 한 배제하여 신원주체가 직접 자신의 신원을 관리할 수 있게 한다.

VC의 구조는 그림 1와 같다. 발급자(Issuer)는 기존의 제3자나 중앙기관을 의미하여, 사용자(Holder)에게 자격증명(Credential)을 발급하는 역할을 한다. 검증자(Verifier)는 사용자의 신원을 인증하는 주체로, 사용자가 제시한 자격증명을 검증함으로써 신원인증을 진행한다. 사용자에게 발급된 자격증명의 검증에는 검증 가능한 데이터 저장소(Verifiable Data Registry)에 저장된 값만을 이용하기 때문에 발급자의 추가 개입이 필요하지 않다. 제출된 자료의 검증에 발급자가 개입하지 않기 때문에, 신원정보의 보유·관리·통제를 신원주체가 직접 수행하므로 VC는 자기주권성을 일부 보장한다.

자격증명의 구조는 그림 2와 같다. 자격증명은 크게 Metadata, Claim, Proof의 세 부분으로 나누어진다. Metadata에는 자격증명을 발급한 발급자에 대한 정보나 자격증명의 유효기간 등이 명시되어 있다. Claim에는 발급자가 작성한 신원주체에 대한 정보(이름, 나이, 최종학력 등)가 명시되어 있으며, Claim에 기재된 내용은 자격증명에 존재하는 Proof에 의해서 보장된다. 이때 Proof에는 RSA[6]나 ECDSA[7] 등 다양한 비대칭 암호화 알고리즘이 사용될 수 있으며, 검증에 필요한 데이터는 모두 검증 가능한 데이터 저장소를 통해 얻을 수 있다.

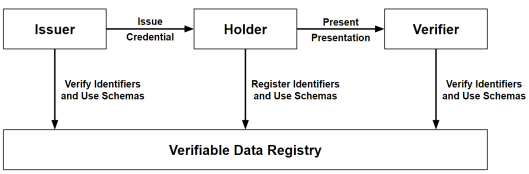

그림 1. 검증 가능한 자격증명의 구조
Fig. 1. The structure of the Verifiable Credential

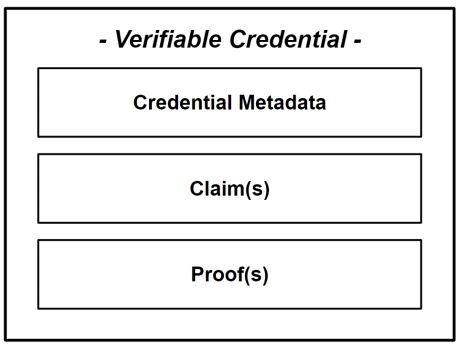

그림 2. 자격증명의 데이터 모델
Fig 2. Data model of Credential

사용자는 발급자에게서 발급받은 자격증명을 활용해서 인증을 진행하는데, 이때 검증자는 인증에 필요한 요소를 사용자에게 요청한다. 사용자는 보유중인 자격증명을 활용하여 이에 적절한 요소들을 기록한 검증 가능한 프레젠테이션(Verifiable Presentation)을 생성하여 검증자에게 제출한다. 검증 가능한 프레젠테이션의 예시는 그림 3과 같다. 프레젠테이션에는 사용자가 보유중인 자격증명이 일부 포함될 수 있으며, 해당 프레젠테이션이 사용자가 직접 생성한 것임을 증명하기 위한 프레젠테이션 Proof가 존재한다. VC의 동작 구조는 다음과 같다 :

1) 사용자는 발급자에게 자격증명의 발급을 요청
2) 발급자는 1)의 요청을 검토하여 사용자에게 적절한 내용을 기재한 자격증명을 발급
3) 사용자는 2)에서 발급받은 자격증명을 저장
4) 사용자는 검증자에게 인증을 요청
5) 검증자는 4)의 요청에 따라 인증에 필요한 요소를 결정하여 사용자에게 요청
6) 사용자는 5)의 요청에 따라 보유중인 자격증명을 활용하여 프레젠테이션을 생성해 검증자에게 제출
7) 검증자는 5)에서 요청한 내용과 6)에서 제출받은 내용을 대조하여 검증 가능한 데이터 저장소를 이용해 인증을 진행

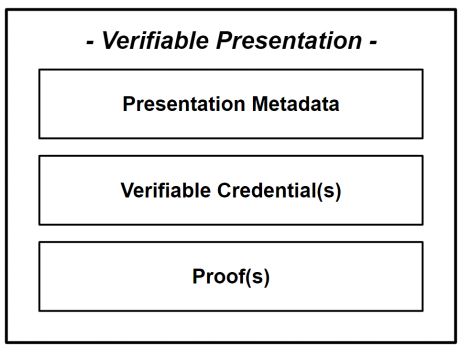

그림 3. 검증 가능한 프레젠테이션의 데이터 모델
Fig 3. Data model of Verifiable Presentation

2.3 자격증명의 위임 문제

VC 표준에서는 자격증명을 타인에게 위임하는 행위를 그림 4와 같이 단순히 명시하고만 있을 뿐, 자세한 과정을 명시하고 있지 않기 때문에 타인에게 자격증명을 위임할 경우 자기주권성이 침해될 우려가 존재한다. VC에 기반한 인가 프레임워크가 추후 설계·개발될 경우, 자기주권성을 보장하면서도 타인에게 권한을 위임하는 경우가 존재할 수 있는데, VC 표준에서는 이러한 경우에서의 자기주권성에 대해서는 고려하지 않아 추후에 문제가 될 여지가 있다.

단순히 VC 표준에 따라 사용자가 발급받은 자격증명을 그대로 타인에게 전송할 경우 그림 5와 같은 자기주권성 침해 문제가 발생한다. 사용자는 자격증명을 넘겨받은 타인이 해당 자격증명을 활용하여 검증자에게 제시하는 것을 통제·감시할 수 없고, 다른 제3자에게 또다시 자격증명을 재위임하지 못하도록 강제할 수 없다. 따라서 사용자는 타인에게 넘겨준 자격증명에 대해서 통제하는 것이 불가능해져, 표 1의 원칙 중 통제권(Control), 접근성(Access), 동의(Consent)를 더 이상 보장할 수 없게 된다.

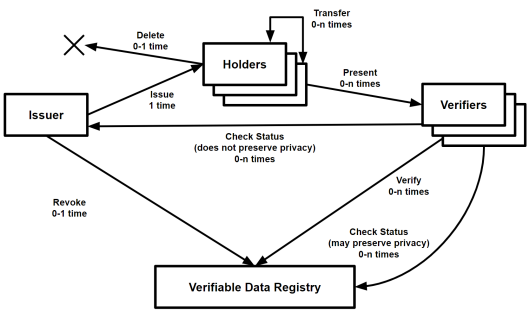

그림 4. 자격증명의 생명주기
Fig 4. Life cycle of a Verifiable Credential

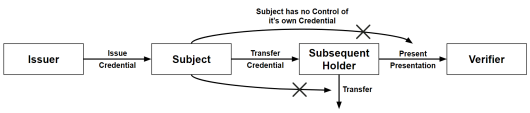

그림 5. 위임된 자격증명의 자기주권성 침해
Fig 5. Infringement of Self-sovereignty of the delegated Credential

2.4 자격증명의 안전한 전송 기법

본 논문에서는 신원주체의 자기주권성을 보장하기 위해 타인에게 안전하게 자격증명을 전송하는 기법을 제안한다. 제안방식은 그림 6과 같이 동작한다. 사용자는 발급자로부터 자격증명을 발급받고, 이를 타인에게 위임할 수 있다. 타인에게 위임할 때, 사용자는 그

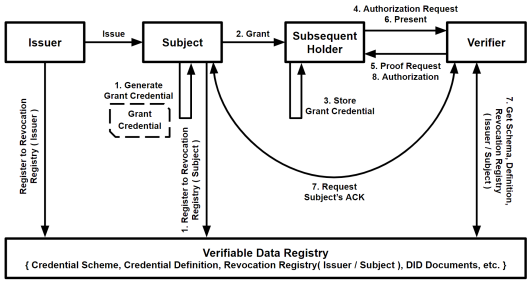

그림 6. 자격증명의 안전한 전송 기법
Fig 6. Safe Transfer Method of Verifiable Credential

림 7과 같은 위임 자격증명(Grant Credential)을 생성함으로써 자기주권성을 보장한다. 제안방식의 기본적인 동작과정은 다음과 같다(단, 사용자에게 자격증명을 발급하는 초기 과정은 생략한다) :

1) 사용자는 타인에게 권한을 부여하기 위해 허용 권한이나 유효기간 등, 사용범위를 나타내는 위임 자격증명을 작성
2) 사용자는 권한을 부여할 대상에게 위임 자격증명을 발급(전송)
3) 사용자에게 권한을 부여받는 대상은 2)에서 발급한 위임 자격증명을 저장
4) 사용자에게 권한을 부여받는 대상은 검증자에게 인증을 요청
5) 검증자는 4)의 요청에 따라 인증에 필요한 요소를 결정하여 요청
6) 사용자에게 권한을 부여받는 대상은 5)의 요청에 따라 보유중인 위임 자격증명을 활용하여 프레젠테이션을 생성해 검증자에게 제출
7) 검증자는 5)에서 요청한 내용과 6)에서 제출받은 내용을 대조하여 검증 가능한 데이터 저장소

- Grant Credential -

Holder : Subsequent Holder를 명시
Permission : 신원주체가 부여한 권한 명시
ACK : ACK의 값이 존재할 경우, 검증자는 반드시 신원주체의 승인(Acknowledgement)을 받아야 함
Revocation Registry Entry : Grant Credential의 Revocation 여부를 확인할 수 있는 Registry를 가리킴
Issuance Date : valid from ~
Expiration Date : valid until ~
Claim(s) : from Verifiable Credentials
Proof(s) : from Verifiable Credentials +
Subject's Signature

그림 7. 위임 자격증명의 데이터 모델
Fig 7. Data model of Grant Credential

를 이용해 검증을 진행하며, 필요한 경우 위임 자격증명의 동의(ACK)를 신원주체에게 요청함
8) 검증자는 7)의 검증 결과가 정상일 경우, 위임 자격증명에 따라 적절한 권한을 부여(인가)함

위임 자격증명의 구조는 그림 7과 같다. 위임 자격증명은 Holder, Permission, ACK, Revocation Registry Entry, Issuance Date, Expiration Date, Proof를 포함하고 있으며, 별도의 제3자를 개입시키지 않고도 검증이 가능해 사용자의 자기주권성을 개선시킬 수 있다.

Holder는 사용자가 위임 자격증명을 발급한 대상을 명시한다. 검증자는 위임 자격증명을 제시받았을 때, 이를 제시한 객체가 위임 자격증명에 명시된 Holder와 일치하는지 검증한다. 때문에 위임 자격증명을 보유하고 있더라도 사용자가 명시한 Holder 외에는 이를 사용할 수 없다.

Permission은 사용자가 위임 자격증명을 발급한 대상에게 부여한 권한을 나타낸다. 검증자는 Permission에 명시된 권한만 인가함으로써 사용자가 위임 자격증명의 활용범위를 직접 제한할 수 있다. 예를 들어 사용자는 Permission에 해당 위임 자격증명을 특정 검증자에게만 제시할 수 있다고 직접 명시하거나 읽기, 쓰기 등의 권한을 명시하여 인가될 권한의 범위를 조절할 수 있다.

ACK는 권한을 부여받은 타인이 검증자에게 위임 자격증명이 포함된 프레젠테이션을 제시였을 때, 검증에 사용자의 승인(Acknowledgement)이 필요한지를 나타낸다. 이때 ACK에는 URL형태의 값을 가지므로, 검증자가 사용자에게 승인을 요청할 수 있는 경로를 나타낸다. 검증자는 ACK값이 명시되어 있지 않을 경우 사용자의 승인을 받는 절차를 건너뛰고, ACK값이 명시되어 있을 경우 ACK에 명시된 URL을 통해서 사용자의 승인을 받는다. 이때 사용자는 검증자가 ACK에 명시된 URL을 통해 전송한 승인요청을 직접 검토하여 해당 위임 자격증명의 사용을 승인하거나 거부할 수 있다. 사용자의 승인/거부 응답에는 사용자의 전자서명이 첨부되어 검증자는 검증 가능한 데이터 저장소를 이용해 해당 응답을 검증할 수 있다. ACK값을 명시함으로써 사용자는 위임 자격증명이 검증자에게 제시되는 모든 시도를 감시·제어할 수 있다.

Revocation Registry Entry는 사용자에 의해서 직접 관리되는 위임 자격증명의 폐기목록에 접근할 수 있는 경로를 나타낸다. 위임 자격증명은 사용자가 직접 발급하여 관리하기 때문에 인증기관이 관리하는 인증서 폐기목록과는 달리 사용자가 폐기목록을 직접 관리할 수 있으며, 사용자 임의로 자유롭게 위임 자격증명을 폐기할 수 있다.

Issuance Date와 Expiration Date는 위임 자격증명의 유효기간을 나타낸다. 이는 사용자가 위임 자격증명을 발급할 때 의도한 사용기한으로, 발급 이후에 문제가 생기거나 목적을 달성한 경우 Revocation Registry에 의해서 폐기될 수 있다. 때문에 검증자는 위임 자격증명의 유효성을 검증하기 위해서 Issuance Date와 Expiration Date를 우선 검증하고, Revocation Registry를 조회하여 유효성을 마저 검증한다.

Proof는 사용자가 자신의 개인키를 사용한 전자서명을 포함하여 위임 자격증명의 무결성을 보장하고, 사용자가 해당 위임 자격증명을 직접 생성했다는 사실을 보장한다. Proof에 사용자가 직접 서명한 값이 존재하기 때문에 위임 자격증명은 사용자의 개인키를 가지고 있지 않은 타인이 위조할 수 없다. 검증자는 Proof를 통해서 위임 자격증명에 명시된 내용이 모두 사용자가 직접 생성했다는 사실을 확신할 수 있다.

위임 자격증명의 검증 과정은 다음과 같다 :

1) 제시된 위임 자격증명의 Proof 중, 사용자의 서명을 검증하여 위임 자격증명의 무결성 검증
2) 위임 자격증명에 명시된 Holder와 위임 자격증명을 제시한 객체를 검증
3) Issuance Date, Expiration Date를 검증하여 위임 자격증명의 유효성 검증
4) Revocation Registry Entry를 통해 제시된 위임 자격증명의 폐기 여부 검증
5) 위임 자격증명에 ACK가 명시된 경우, 위임 자격증명을 발급한 사용자에게 승인을 요청
6) 위임 자격증명에 명시된 Permission에 따라 위임 자격증명을 제출한 객체를 인증·인가

Ⅲ. 평가 분석

본 논문의 제안방식은 기존 VC 표준과 비교하였을 때 자기주권성이 얼마나 개선되었는지를 표 1의 자기주권신원의 원칙을 사용하여 정성적으로 비교해 평가한다. 평가에 사용되는 원칙은 10가지 중 통제권(Control), 접근성(Access), 이동성(Portability), 동의(Consent), 보호(Protection)의 5가지를 선정하여 진행한다. 제안방식의 평가는 표 2와 같다.

제안방식은 표 2와 같이 기존 VC 표준에 비해서 통제권(Control), 이동성(Portability), 동의(Consent),

표 2. 제안방식 평가
Table 2. Evaluation of Proposed Method

원칙	VC 표준	제안방식
Control (통제권)	타인에게 전송된 경우 보장되지 않음	보장됨
Access (접근성)	보장됨	타인에게 전송된 경우 보장되지 않음
Portability (이동성)	전송과 관련한 기법이 명시되지 않음	전송을 지원함
Consent (동의)	타인에게 전송된 경우 보장되지 않음	보장됨
Protection (보호)	타인에게 전송된 경우 보장되지 않음	Control과 Consent가 보장됨

보호(Protection)에서 개선되었음을 알 수 있다. 하지만 접근성(Access)은 기존방식에 비해서 오히려 보장되기 어려워진다는 Tradeoff가 발생한다.

통제권(Control)의 경우 기존방식에서는 사용자의 소유를 벗어난 자격증명에 대해 통제수단이 존재하지 않는 것에 반해, 제안방식에서는 위임 자격증명의 도입을 통해 이를 극복하고 있다. 사용자는 위임 자격증명의 Permission을 통해서 위임 자격증명의 활용범위를 제한할 수 있으며, 자신이 직접 관리하는 Revocation Registry를 사용해서 언제든지 위임 자격증명의 폐기가 가능하다. 따라서 기존방식에 비해서 사용자의 자격증명에 대한 통제력을 개선하였다.

이동성(Portability)의 경우 기존방식에서는 자격증명의 전송이 가능하다고만 명시할 뿐 사용자의 자기주권성을 고려하지 않는 것에 비해 제안방식에서는 위임 자격증명을 통해 사용자의 자기주권성을 보장한다. 사용자는 타인에게 자격증명을 전송하고자 할 경우, 위임 자격증명의 활용범위를 제한하거나 Revocation Registry를 이용해서 폐기하는 등의 방법으로 자기주권성을 지킬 수 있다.

동의(Consent)의 경우 타인이 사용자의 자격증명을 사용하는 사례를 고려하지 않았기 때문에 기존방식에서는 보장되지 않았으나, 제안방식에서는 위임 자격증명의 ACK를 통해서 이를 보장하고 있다. 기존방식에서는 타인에게 전송된 자격증명은 사용자의 통제를 완벽히 벗어나기 때문에 이를 건네받은 타인의 행동을 감시·승인할 수 없었다. 제안방식에서는 ACK에 사용자의 승인을 요청하기 위한 경로를 명시함으로써 Consent를 보장할 수 있다.

하지만 ACK를 사용해서 사용자의 동의를 구하는 과정에서 사용자가 가용한 상황이 아닐 때 False Failure Rate(FFR)가 발생한다는 문제가 존재한다. 정당한 ACK요청임에도 불구하고 사용자가 가용하지 않은 경우 요청이 거부될 수 있으며, 사용자가 의도한 동작임에도 불구하고 가용성이 침해될 수 있다는 한계점이 존재한다.

보호(Protection)의 경우 사용자의 권한을 희생하지 않고도 상기한 통제권(Control), 이동성(Portability) 그리고 동의(Consent)의 세 가지 속성을 기존방식 대비 개선하고 있다. 또한 별도의 제3자의 개입 없이도 위와 같은 개선을 이룰 수 있어 탈중앙화를 해치지 않아 사용자의 자기주권성이 보장되며 기존방식의 목적 또한 해치지 않는다.

접근성(Access)의 경우 본 제안방식은 타인에게 위임한 자격증명의 활용범위를 제한하고 제어하는 것에 초점을 맞추기 때문에 사용자의 접근을 보장하지 못한다. 기존방식은 타인에게 자격증명을 전송하는 행위에 대해 명시하지 않아 사용자의 접근이 항시 보장되나, 제안방식의 경우 자격증명을 건네받은 타인이 동의하지 않을 경우 사용자의 접근이 제한될 수 있다.

Ⅳ. 결 론

본 논문에서 제안한 검증 가능한 자격증명의 안전한 위임 기법은 타인에게 위임된 자격증명의 경우에도 사용자의 자기주권성을 보장하고 있다. 기존방식에서는 타인에게 자격증명을 전송하는 동작에 대해서는 별도로 명세하지 않아 자기주권성이 침해될 수 있다는 문제점이 존재하였으나, 제안방식을 통해 문제를 해결하고 자기주권신원의 10가지 원칙 중 통제권(Control), 이동성(Portability) 그리고 동의(Consent)를 개선하였다. 하지만 위임 자격증명은 검증자가 이성적(Rational)이라는 가정 하에 작성되어 있어 검증자가 이를 반드시 준수하게끔 강제하는 암호학적, 구조적 수단이 없다. 또한 사용자가 가용한 상황이 아닐 때 FFR이 발생한다는 한계점 또한 존재한다. 따라서 본 제안방식은 위임 자격증명의 내용을 검증자가 반드시 준수하게끔 강제할 암호학적, 구조적 수단과 가용하지 않은 사용자의 ACK를 처리하는 과정에 대한 후속 연구를 통해 개선될 수 있다. 본 제안방식을 통해서 다양한 시나리오에서의 자기주권성에 대한 중요성을 각인하고, 자기주권신원의 보편화와 생태계구축에 기여할 수 있을 것으로 기대한다.

References

[1] C. Allen, *The Path to Self-Sovereign*

Identity(2016), Retrieved Nov. 2021, from http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html, 2016.

[2] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, *Decentralized Identifiers (DIDs) v1.0*(2021), Retrieved Aug. 2021, from https://www.w3.org/TR/did-core/

[3] M. Sporny, G. Noble, D. Longley, D. C. Burnett, B. Zundel, and K. Den Hartog, *Verifiable Credentials Data Model v1.1*(2021), Retrieved Nov. 2021, from https://www.w3.org/TR/vc-data-model/

[4] J.-H. Lee, J.-W. Kim, C.-S. Kim, and J.-H. Yang, "A study on strengthening personal information sovereignty through analysis of domestic service cases and research projects of self-sovereign identity technology," *J. KIIECT*, vol. 13, no. 6, pp. 575-589, Dec. 2020.

[5] O. Nate and H. D. Kim, *Open Badges are Verifiable Credentials*(2018), Retrieved Nov. 2021, from https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/open-badges-are-verifiable-credentials.pdf

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[7] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, pp. 36-63, 2001.

임 승 주 (Seungjoo Lim)

2020년 2월 : 아주대학교 사이버보안학과 졸업

2022년 2월 : 아주대학교 컴퓨터공학과 석사

<관심분야> 탈중앙화, 분산시스템, 네트워크보안, 보안 컴플라이언스

[ORCID:0000-0002-9511-5489]

김 기 형 (Ki-Hyung Kim)

1990년 2월 : 한양대학교 전자통신공학과 졸업

1992년 2월 : KAIST 전자공학과 석사

1996년 8월 : KAIST 전자공학과 박사

1997년 3월~2005년 2월 : 영남대학교 컴퓨터공학과 부교수

2005년 3월~현재 : 아주대학교 사이버보안학과 교수

<관심분야> 블록체인, IoT, 네트워크 보안

[ORCID:0000-0001-6624-3003]