A Subject-Centric Credential Management Method based on the Verifiable Credentials

Seungjoo Lim
Dept. of Computer Engineering
Ajou University
Suwon, Republic of Korea
dlaking@ajou.ac.kr

Min-Hyung Rhie
Dept. of Knowledge Information Engineering
Ajou University
Suwon, Republic of Korea
quotia72@ajou.ac.kr

DongYeop Hwang
Dept. of Computer Engineering
Ajou University
Suwon, Republic of Korea
bc8c@naver.com

Ki-Hyung Kim
Dept. of Cyber Security
Ajou University
Suwon, Republic of Korea
kkim86@ajou.ac.kr

2021 International Conference on Information Networking (ICOIN) | 978-1-7281-9101-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICOIN50884.2021.9333857

***Abstract*—In this paper, a subject-centric structure is proposed that improves the holder-centric structural problems of verifiable credentials developed for self-sovereign identities. Holder-Centric structured verifiable credentials represent a structure in which a holder can control the credentials even if it is not a subject. This structure allows the holder to attempt authentication or transfer credentials without the subject's permission. The subject may lose some control over the credential, thus losing the meaning of self-sovereign identity. We propose a subject-centric structure that allows the subject to control over the transferred verifiable credentials.**

***Index Terms*—Self-Sovereign Identity, Verifiable Credentials, Decentralized Identifiers, Blockchains, Authentication Method**

I. Introduction

Research on self-sovereign identity is actively being conducted to ensure the identity control of the subject [1]. One of the representative efforts of the self-sovereign identity is a Verifiable Credential (VC) [2]–[4], which is standardized by World Wide Web Consortium (W3C). The VC supports the decentralized identities, so the identity can be verified without having additional communication and allowing the subject to control its own identity.

In the VC, the holder of issued credentials can be different from the subject of the credential. The issuer can issue credentials to the subject, and the subject can delegate credentials by transferring the credentials to another holder. For example, someone gets a prescription on behalf of a patient who cannot move, or a parent uses the child's credentials.

A problem arises if the holder of the credentials different from the subject, that the holder can use or transfer the credentials without the subject's permission. This is because the signature of the holder is used instead of the subject's one when presenting the credentials to the verifier. We call the VC is holder-centric, focusing on the holder-centered structure in which the holder can use the credentials without the permission of the subject.

In this paper, we propose a subject-centric structure of VC that solves the holder-centric problem by allowing the subject to control the transferred credentials. By allowing subjects to control their credentials through the subject-centric structure, the VC becomes closer to the self-sovereign identity.

In the remainder of this paper, Section II first explains related works and W3C's VC for background information. In Section III, the problem of the holder-centric structure is explained, and we propose a subject-centric structure of VC. Section IV concludes the proposal of this paper and proposes future research.

II. Preliminaries

A. W3C Verifiable Credentials

The W3C is standardizing a new digital credential scheme called verifiable credentials (VC) [2]–[4]. The VC realizes decentralization by combining with technologies such as the decentralized identifiers [5] and the blockchain. [6] The development of an authentication platform using VC is very active and is recognized as an essential technology for achieving self-sovereign identity [7].

Fig. 1. Core Data Model in W3C's VC

Figure 1 shows three main types of data models in VC: claims, verifiable credentials, and verifiable presentations. The claim means an attribute that describes a subject endorsed by the issuer. The verifiable credential is a collection of claims endorsed by the issuer and contains metadata and the issuer's signature called proof. The verifiable presentation includes the collection of verifiable credentials the holder wants to present,

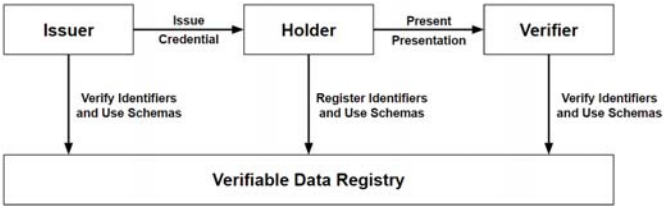

Fig. 2. Basic Concept of W3C's VC

along with the metadata and the holder's signature called proof. All credentials and presentations contain a signature called a proof that can be verified through the issuer and holder's public keys.

Figure 2 shows the basic concept of VC. When a subject requests an issuer to issue a credential, the issuer reviews it and issues a credential that guarantees the subject. The subjects can keep issued credentials and select only the required credentials and present them to the verifier when authentication is required. Holders and verifiers can validate credentials and presentations through public keys and schemes stored in a verifiable data registry.

In the VC, authentication is possible with only issued credentials without a centralized procedure. Each credential and presentation is signed using an encryption algorithm such as RSA [8] to ensure integrity. The public key required to decrypt the signature can be obtained from a verifiable data registry like a blockchain. By verifying that each signature is decryptable with the public key recorded in the verifiable data registry, the verifier can verify that it was signed using the private key without requiring further communication with the issuer or holder.

B. Related Works

In the preceding literature [1], the Sovrin foundation shows that the transition to self-sovereign identity is inevitable in the future. Self-sovereign identity means that an individual has full control over its information, and the integrity and privacy of that information are guaranteed.

The W3C is standardizing a technology called verifiable credential (VC) to realize self-sovereign identity [2]–[4]. VC is a tamper-evident, machine-readable trustworthy means for an issuer to assert claims about a subject.

The W3C is also standardizing decentralized identifiers (DIDs) apart from verifiable credentials [5]. For decentralization of the highly centralized PKI system, DIDs use a distributed ledger such as a blockchain. [9] Using DIDs, entities can leverage verifiable credentials that can be verified with public keys controlled though the DID.

III. Proposed Subject-Centric VC

A. Holder-Centric Problem of VCs

The VC uses the holder's private key when making proof of verifiable presentations. This is not a problem at all when the holder is the subject of all the credentials that make up the presentation. If one or more of the credentials refer to a different subject than the holder, the subject may lose control of transferred credentials.

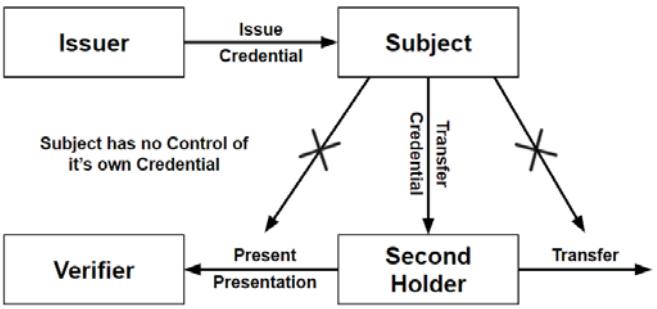

Fig. 3. Structure of Holder-Centric Problem

Figure 3 shows that the subject has no effect on the presentation containing the transferred credential and loses control of it. In VC, the second holder can make a valid presentation regardless of whether the subject trusts the verifier or not, and the second holder can transfer it to any entity without the subject's approval. This issue causes the subject to lose control over the transferred credentials, making the VC holder-centric, which can no longer be called self-sovereign identity.

The W3C has considered the transferred credentials but did not suggest a way to avoid unauthorized transfer or authentication attempts. They only define a few cases in which credentials are transferred. [2] Therefore the holder-centric problem can be considered valid and should be resolved.

B. Proposed Subject-Centric Structure

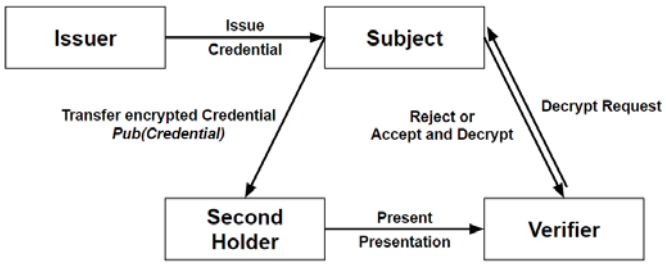

Fig. 4. Subject-Centric Structure

To address the holder-centric problem of the W3C's VC, we propose a subject-centric structure. Figure 4 shows the subject-centric structure where the subject has almost complete control over the transferred credentials. If a credential transfer is required, the subject encrypts the credential with the subject's public key before the transfer, so the contents of the credential cannot be viewed without the subject's private key.

The second holder and verifier cannot decrypt the credentials without the subject's permission, so the second holder creates the presentation without decryption. And the verifier checks that the presentation has the proof from of the second holder and each credential has the proof from of the issuer, and requests the subject to decrypt the encrypted credentials. When requesting decryption, the verifier includes information

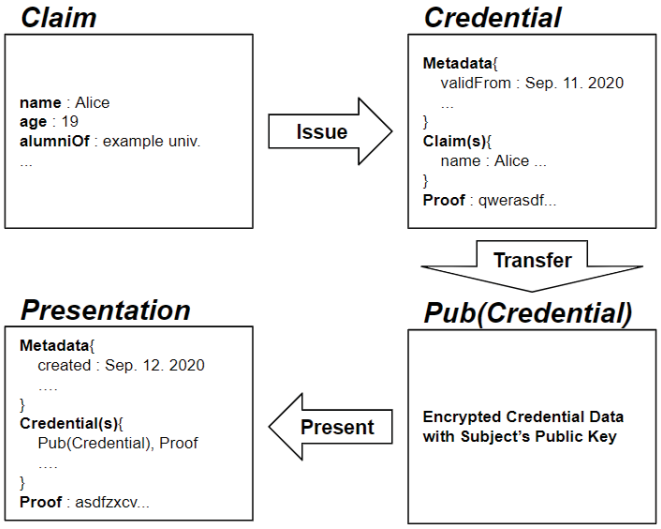

Fig. 5. Transferring Data Model

about the holder who presented this credential, so if the verifier or the second holder is cannot be trusted, the subject can reject the request. As shown in Figure 5, the transferred credentials are encrypted with the subject's public key and the second holder creates the presentation in this state.

The subject of a credential is not always a human but can be a pet, building, company, organization, or property. If a none human being is the subject of a credential, self-control over the credential is nonsense. If humans are not the subject of a credential, there is an agent who issued the credentials such as the owner of the pet, the building, the board of directors, etc. Unless there is a way to ascertain the none humans free will, the above agent is considered to be on behalf of the subject.

The W3C's VC document specifies a subjectless credential, called a bearer credential. [2] Bearer credential does not indicate a specific subject, it indicates that the holder has rights, such as concert tickets or theme park tickets. Bearer credential makes the holder a legitimate owner because the subject does not exist. So, in this case, the transfer of credentials is considered the same as the transfer of ownership and is not handled separately.

C. Limitation

Selectively disclosure is not fully compatible with the subject-centric structure. The second holder cannot extract the claim it is trying to present from the encrypted credential. But it is natural to not expose the information to other holders other than the subject. Therefore, we are limited to the subjects as the only entity that can selectively disclosure in a true subject-centric structure.

Encrypted credentials are transferable and cannot be prevented from being transferred. The subject-centric structure only protects information and prevents unauthorized authentication attempts. Therefore this subject-centric structure cannot track whether or not credentials are being sent. However, as long as the private key is not leaked, encrypted credentials can be considered secure, and any attempts to authenticate using these encrypted credentials are under control and no longer cause the same privacy issues as before.

The subject-centric structure does not allow the second holder to re-transfer. The subject cannot know to whom the second holder transferred the credential, only the second holder designated by the subject can use the credential in the subject-centric structure.

IV. Conclusion and Future Works

In this paper, we explored the holder-centric problem of W3C's verifiable credentials, which is being standardized for secure digital credentials, and proposed a subject-centric structure that improved it. The addition of the process of encrypting and decrypting credentials has complicated the authentication process but is considered acceptable for true self-sovereign identity. Although this proposal is effective against unauthorized authentication attempts of credentials, it is not yet applicable to cases where multiple subjects are specified in a single credential. Therefore, in the case of multi-credential including multiple subjects, a follow-up study will be conducted.

Acknowledgment

This research was supported by "Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2018R1D1A1B07048697)", "Korea Institute for Advancement of Technology(KIAT) grant funded by the Korea Government(MOTIE) (P0008703, The Competency Development Program for Industry Specialist)", and "the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2020-2018-0-01396) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation)".

References

[1] Tobin, Andrew, and Drummond Reed. "The inevitable rise of self-sovereign identity." The Sovrin Foundation, 29 Sep 2016
[2] Manu sporny et al., "Verifiable Credentials Data Model 1.0", W3C Rec, Nov 2019, [online] Available: https://www.w3.org/TR/vc-data-model/
[3] Nate Otto et al., "Verifiable Credentials Use Cases", W3C Working Group Note, Sep 2019,[online] Available: https://www.w3.org/TR/vc-use-cases/
[4] David Chadwick et al., "Verifiable Credentials Implementation Guidelines 1.0", W3C Working Group Note, Sep 2019, [online] Available: https://www.w3.org/TR/vc-imp-guide/
[5] Drummond Reed et al., "Decentralized Identifiers (DIDs) v1.0", W3C Working Draft, Nov 202, [online] Available: https://www.w3.org/TR/did-core/
[6] Clemens Brunner et al., "DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust", Proceedings of Preprint. ACM, 2020
[7] Manu Sporny, "Verifiable Credentials Data Model Implementation Report 1.0", W3C Editor's Draft, Jan 2020, [online] Available: https://w3c.github.io/vc-test-suite/implementations/
[8] R.L. Rivest et al., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Comm. ACM 21, 1978
[9] M. Eisenstadt et al., "COVID-19 Antibody Test/Vaccination Certification: There's an App for That", IEEE Open Journal of Engineering in Medicine and Biology 2020, doi: 10.1109/OJEMB.2020.2999214.