Hierarchical Sovereignty Management and Access Control based on Self-Sovereign Identity

Kang Woo Cho, Mi Hyeon Jeon, and Sang Uk Shin*
Pukyong National University, Busan, South Korea
{kwcho899, jmh3850, shinsu}@pukyong.ac.kr

Abstract

Self-sovereign identity is a type of decentralized identity technology and has been proposed to solve various problems of the existing public key infrastructure based centralized identity authentication service. In addition, the demand for a secure decentralized access control management (ACM) technique has increased according to the demand for such next-generation identity identification service. Accordingly, although various ACM techniques that can be applied to decentralized services have been proposed, most fall into the introductory stage of research. In this paper, based on the SOVRIN-based restructured verifiable credential concept proposed in our previous study, we provide a hierarchical sovereignty and ACM technique that does not use a smart contract.

Keywords: Blockchain, Self-Sovereign Identity, Access Control

1 Introduction

As various identity authentication services change into a decentralized service type, a change in the access control management (ACM) technique used in existing centralized identity authentication is required. In the case of a centralized ACM, efficient policy management is possible for collectively stored identity data, and it is easy to distribute access rights according to policies trusted by all network participants. However, a decentralized digital identity authentication service records identity data in a distributed ledger [1]. Because it forms a peer-to-peer (P2P) network of mutually trustless relationships, there are a number of limitations to applying the existing ACM technique.

In this paper, we extend the restructured verifiable credential (VC) concept proposed in [2]. Each participant in an identity data transaction uses a different restructured VC for one credential to control access to the identity attribute [3]. Restructured VC can ensure ACM about identity attribute and provide hierarchical sovereignty according to the information-handling authority. The proposed model restructures the original VC such that each participant can read only the information corresponding to their access rights. This restructures the VCs for external sharing. In addition, to prove the correlation between the original and restructured credentials, a proof of transaction is generated as a hash digest of the blind secret, which is a unique parameter of the credential.

In Section 2 of this paper, background on the SSI and related studies on decentralized ACM are described. Section 3 details the SSI-based hierarchical sovereignty management and ACM technique and analyzes the acceptable level within a transaction by calculating the overhead incurred to create a restructured VC in the proposed model. Finally, Section 4 provides some concluding remarks regarding this paper.

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 7, Article No. 19 (December 15, 2021)
DOI:*10.22667/ReBiCTE.2021.12.15.019*

*Corresponding author: Department of IT Convergence and Application Engineering, Pukyong National University, South Korea, Tel: +82-(0)51-629-6249, Web: https://cms.pknu.ac.kr/lacuc/view.do?no=16745

2 Background

2.1 Self-Sovereign Identity

In self-sovereign identity (SSI), actors classified as holders, issuers, and verifiers participate in the digital identity authentication process, and aim to generate SSI attribute information using the concepts of claims and VCs [4, 5]. SSI satisfies requirements such as data self-sovereignty, decentralization, explicit consent of the data subject, and provisioning of minimum information for purposes other than that in line with the national data processing trend established based on the EU's General Data Protection Regulation (GDPR) [6]. SOVRIN, based on Hyperledger Indy [7]; uPort, based on Ethereum[8]; Jolocom[9]; and Shocard [10] have all been proposed.

SOVRIN, a representative study of SSI, has emerged for realizing self-sovereign identity authentication for actors [7]. Unlike other SSI techniques, SOVRIN does not use smart contracts throughout the process. The identity attribute in SOVRIN originates from the claim of the holder, who is the first information subject, and is created as a VC through a digital signature by the issuer to give it a public effect. The VP is configured in a form that enables zero-knowledge proof (ZKP) through the challenge verification process between the holder and the verifier [11]. SOVRIN uses a Camenisch–Lysyanskaya (CL) signature, which is a digital signature technique for applying ZKP during the process [12].

2.2 Related Works

SSIBAC is an ACM technique focusing on user data privacy and sovereignty in the SSI model for authentication and credential issuance [13]. It is used to store the context-based permission VC at the policy retrieval point (PRP) for users to access data, and aims to port the access control policy used in the existing centralized ACM to the blockchain-based SSI solution. SSIBAC applies access control when a holder obtains a *schema*. Therefore, the verifier returns *schema* to the holder including the access control policy VC for PRR. Subsequently, the verifier creates a challenge, including the access control policy in the *schema*, and the holder must be able to respond to it. The holder sends the challenge response for the identity and ACM policies of the owned VC to the verifier, which can grant access by verifying it.

Jolocom proposed a hierarchical deterministic (HD) key-based identity-management system [9]. As with SSI open-source projects such as SOVRIN, this aims to satisfy the requirements of guaranteeing self-sovereignty for data subjects, explicit consent, and minimum information provisioning. Jolocom uses HD keys generated from a known seed and is directly controlled by the user. Because of its hierarchically deterministic nature, it is possible to generate multiple hierarchically derived keys and share the same seed. Each derivative key of the HD key creates a sub-ID defined as personas, and then combines the original HD key with the DID. Thereafter, an individual persona is identified based on the derived key and seed, and IPFS hash mapping is applied on each persona for the ACM. As a result, access control is achieved through Ethereum's smart contracts under the IPFS structure.

3 Hierarchical Sovereign Management and Access Control

3.1 Restructured Verifiable Credential

In [2], the concept of a restructured VC was suggested. It was considered to provide minimum information for purposes other than statistics, academics, and research to others who are not participants in the general SOVRIN SSI creation and verification process, and it is possible to create a restructured VC with limited information in comparison to the original VC. The verification results of the original VC are information that cannot be verified by a transaction party who shares the challenge value, owing to the characteristics

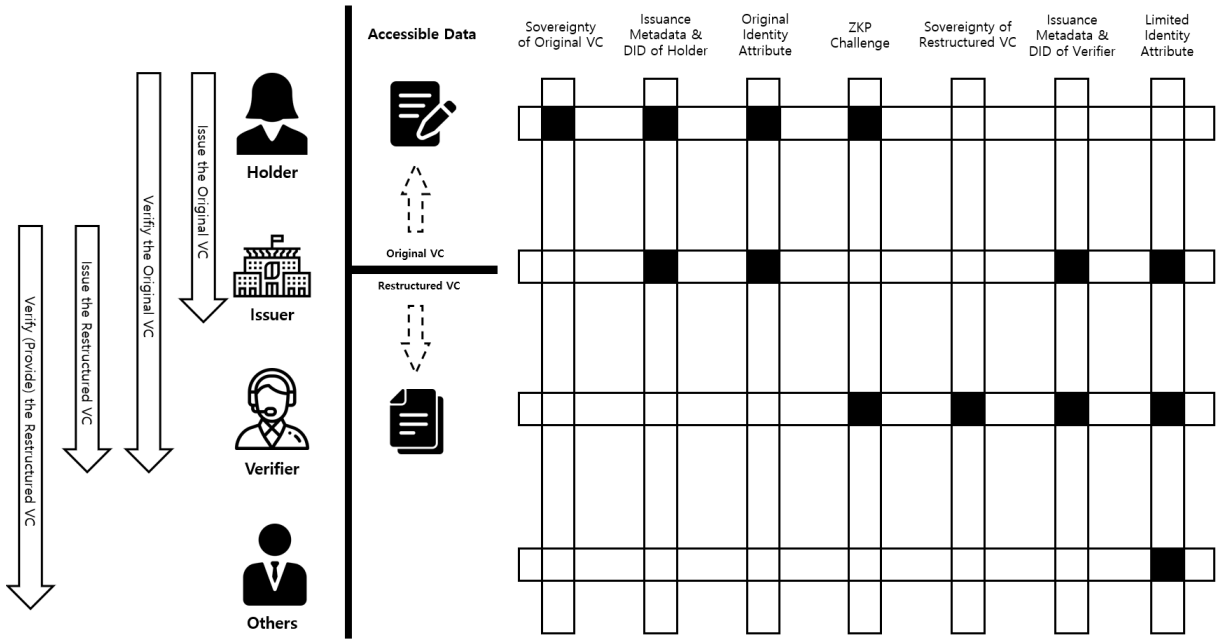

Figure 1: Hierarchical Sovereignty Management Overview

of ZKP. Therefore, strong sniffing protection is provided. However, result of the ZKP can be viewed as closed data that cannot be safely provided to outsiders. Therefore, the proposed model creates a separate VC copy using the ZKP verification result of the original VC as the qualification claim, and then defines it as the restructured VC.

Although the restructured VC includes the ZKP results of the original VC, it is resistant to guessing attacks because it does not include the holder's DID, ZKP challenge, or issuance metadata such as blind secrets. In addition, the holder's DID is replaced with the verifier's DID such that it can be independently used for verification, and a restructuring process is performed to create a new blinded secret and issuance metadata based on the changed DID. When providing the restructured VC to others, to prove the correlation without leaking the identity attribute of the original VC, it includes the hash digest $H(Bs)$ of the original VC's unique identification information-blinded secret as proof of transaction. Because $H(Bs)$ is passed to the verifier during the verification process of the original VC between the holder and verifier, the verifier includes $H(Bs)$ in the restructured VC creation. Therefore, the original VC can be proven as the party that conducted the transaction.

3.2 Hierarchical Sovereign Management

This subsection describes hierarchical sovereignty and ACM using the concept of a restructured VC described above. The proposed model classifies the credentials used in the SSI identity data transaction process into the original and restructured VC. During this process, the original VC is an existing VC issued through a reasonable procedure by an honest issuer and contains sensitive information such as the holder's original identity attribute data, identifiers such as the DID, and issuance metadata. Because verifiers who only conduct a simple verification of the identity attribute data, or others we conduct a verification for other purposes, should not have access to these original VCs, with the proposed model, based on the original VCs, verifiers and others can freely use separately issued restructured VCs. We classified the factors that can be included in both the original and restructured VCs according to a hierarchical ACM. Factors that can be included in the original VC include self-sovereignty and issuance

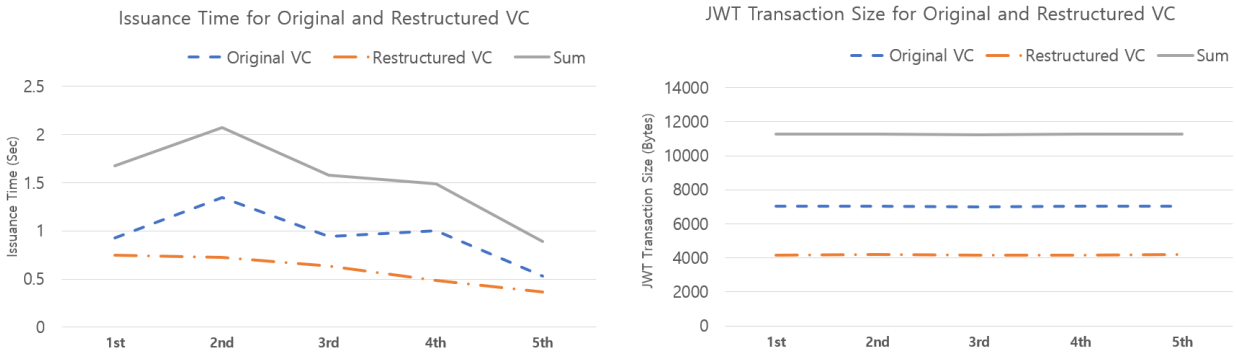

Figure 2: Overhead Analysis of Proposed Model

metadata of the original VC, the holder's DID, the original identity attribute, and the ZKP challenge for verification. In addition, factors that can be included in a restructured VC include self-sovereignty and issuance metadata of the restructured VC, the verifier's DID, and limited identity attributes that can be provided to the least privileged others.

[Figure 1] shows hierarchical sovereignty management using the proposed model in the SSI transaction. First, a holder who can own and manage the original VC acts as the only entity that can exercise sovereignty (right to erasure and correction) over the original VC. In addition, it acquires access to various sensitive information, such as the holder's original identity attribute information, ZKP challenge, and issuance metadata, such as a blinded secret. That is, the holder in the proposed model can obtain all access rights to the original VC and ensure the highest level of self-sovereignty; thus, it satisfies the main requirements of SSI. The issuer is an entity with appropriate issuance authority for the VC within the network, and acquires the right to access issuance metadata. It can access information such as issuance metadata and the identity attributes of the original VC. In addition, the issuance metadata and restricted identity attributes of the restructured VC can be accessed. The verifier cannot access any original VC information other than the ZKP challenge because it only conducts ZKP verification of the original VC. However, the verifier can issue a restructured VC based on the original VC verification result with the holder, and because the verifier is the subject of information, the verifier's DID is recorded. Therefore, the aim is to obtain access rights such as self-sovereignty, issuance metadata, and DID for the restructured VC and finally issue limited identity attributes (ZKP challenge results) that can be shared with others. An other is an entity that does not directly participate in the identity transaction and must be an entity that can access the least amount of information within the network for use other than personal information without the consent of the data subject.

3.3 Analysis

In this subsection, we describe the overhead measurement for a restructured VC that additionally occurs to achieve hierarchical self-sovereign access management according to the authority in our proposed model, and analyze it from the perspective of SOVRIN SSI transactions within the Hyperledger Aries. For the overhead measurement, five samples of original and restructured VCs are created, and the issuance time and Json Web Token (JWT) size of each transaction are measured. We use the Hyperledger Aries open source and BCovrin Ledger based on the Ubuntu 16.0.4 LTS 64bit virtual environment to configure the SSI transaction service environment in a network similar to a real one.

[Figure 2] shows the results of measuring the time required for issuance and the JWT size of the original and restructured VCs. The issuance time was flexibly changed according to the network delay at the time of generating each sample VC, and the issuance time of the original VC was measured to

be 0.95 s on average; in addition, the issuance time for the reconstructed VC was measured to be 0.6 s on average. Therefore, the average of the sum of the issuance times of the original and the restructured VCs is 1.54 s, which incurs an issuance time overhead of approximately 63% of the issuance time of the original VCs. The JWT size of each VC sample did not show a significant difference independent of the network delay, and the JWT size of the original VC was measured as 7052 Bytes on average. Moreover, the restructured VCs were measured as 4209 Bytes on average. That is, the JWT size of the restructured VC is approximately 59.6% in comparison to the original VC, which can be expected to gradually approximate the average issuance time overhead (≈63%) as the number of sample VCs increases.

4 Conclusion

This paper discussed the ACM in a decentralized identity authentication service, which is currently in the introductory stage of research. First, we presented a problem in which the ACM used in the existing centralized identity authentication service cannot be applied to the decentralized identity authentication service. Accordingly, we analyzed the ACM techniques in a previously proposed decentralized identity authentication service. In addition, as an extension of our existing study on data de-identification in a decentralized identity authentication service, we used the restructured VC concept to grant hierarchical sovereign access to identity attribute data contained in credentials. The applicability to the actual digital identity authentication service industry was reviewed by generating a sampled restructured VC in the same environment as SOVRIN's SSI transaction service, deriving the overhead, and analyzing the acceptability within the transaction.

In a digital identity authentication service, sensitive personal data are collected and provided. This requires a stronger privileged ACM compared to other services, and it must be proven that it satisfies international legal standards such as GDPR. This paper discussed the ACM technique in SSI, which is a next-generation digital identity authentication service, and it can be expected that academic discussions on this will continue.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (No. 2019R1I1A3A01060652), and a part of the project titled 'Future fisheries food research center', funded by the Ministry of Oceans and Fisheries, Korea.

References

[1] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel. A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30:80–86, 2018.

[2] K.-W. Cho, M.-H. Jeon, and S. U. Shin. Secure de-identification and data sovereignty management of decentralized ssi using restructured zkp. *Journal of Digital Convergence*, 19(8):205–217, 2021.

[3] World Wide Web Consortium and others. Verifiable credentials data model 1.0: Expressing verifiable information on the web. W3C Recommendation, 2019. `https://www.w3.org/TR/vc-data-model/?#core-data-model`, [Online; Accessed on December 1, 2021].

[4] L. Cocco, R. Tonelli, and M. Marchesi. Blockchain and self sovereign identity to support quality in the food supply chain. *Future Internet*, 13(12):301, 2021.

[5] T. Ehrlich, D. Richter, M. Meisel, and J. Anke. Self-sovereign identity als grundlage für universell einsetzbare digitale identitäten. *HMD Praxis der Wirtschaftsinformatik*, 58(2):247–270, 2021.

[6] G. Kondova and J. Erbguth. Self-sovereign identity on public blockchains and the gdpr. In *Proc. of the 35th Annual ACM Symposium on Applied Computing (SAC'20), Brno, Czech Republic*, pages 342–345. ACM, March 2020.

[7] Sovrin Foundation. Sovrin: A protocol and token for self-sovereign identity and decentralized trust, January 2018. `https://sovrin.org/library/sovrin-protocol-and-token-white-paper/`, [Online; Accessed on December 1, 2021].

[8] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. Uport: A platform for self-sovereign identity, 2017. `https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf`, [Online; Accessed on December 1, 2021].

[9] C. Fei, J. Lohkamp, E. Rusu, K. Szawan, K. Wagner, and N. Wittenberg. Jolocom: Self-sovereign and decentralised identity by design, 2018.

[10] J. Roos. Identity management on the blockchain. *Network*, 105, 2018.

[11] M. Blum, P. Feldman, and S. Micali. Non-interactive zero-knowledge and its applications. In *Proc. of the 20th annual ACM symposium on Theory of computing (STOC'88), Chicago, Illinois, USA*, pages 103–112. ACM, May 1988.

[12] J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. In *Proc. of the 3rd International Conference on Security in Communication Networks (SCN'02), Amalfi Italy*, volume 2576 of *Lecture Notes in Computer Science*, pages 268–289. Springer, September 2002.

[13] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro. SSIBAC: Self-sovereign identity based access control. In *Proc. of the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'20), Guangzhou, China*, pages 1935–1943. IEEE, 2020.

Author Biography

Kang Woo Cho received his B.E. degree in Dept. of Information Communication Engineering from Pukyong National University, Republic of Korea in 2020. He is currently a master course student in Dept. of Information Security from Pukyong National University. His research interests are related with blockchain, identity authentication, and privacy security.

Mi Hyeon Jeon received her B.E. degree in Dept. of IT Convergence and Application Engineering from Pukyong National University, Republic of Korea in 2021. She is currently a master course student in Dept. of Information Security from Pukyong National University. Her research interests are related with blockchain, internet of things(IoT), and Cloud.

Sang Uk Shin received his M.S. and Ph.D. degrees from Pukyong National University, Busan, Korea in 1997 and 2000, respectively. He worked as a senior researcher in Electronics and Tele-communications Research Institute, Daejeon Korea from 2000 to 2003. He is currently a professor in Department of IT Convergence and Application Engineering, Pukyong National University. His research interests include digital forensics, e-Discovery, cryptographic protocol, mobile and wireless network security and multimedia content security.