5ZC-03

An accountable blockchain-based Self-Sovereign Identity Management Platform

XINGXING CHEN　HITOSHI AIDA

Abstract

We propose a transactions auditable self-sovereign identity management solution (**TXA-IMS**) that supports auditing of data exchange between entities as well as give the individual user right to issue a delegate credential which claims that the delegate credential holder can act legally on behalf of the individual issuer. ***Keywords***— **Self-Sovereign Identity**, **Delegation of Authority**, **Auiditable**

1. Introduction

In the most deployed Identity Management(IDM) systems, identity owners never had control of their identity and its associated data[5]. **Self-sovereign identity(SSI)** IDM system gives the identity owners(**the holder**) the ability to hold, manage and control their own digital identity through the credentials. The trust relationships between authoritative organizations or institutions (**the issuers**) that must follow a rigorous process to issue their credentials. The trust agents (**the verifiers**) in the most SSI-based projects or proposals are pre-built off-chain. Current SSI systems avoid recording the transactions between two entities in order to protect the entities' privacy. However, Adrian pointed that the transaction has to leave residual documentation acceptable in case of dispute (Web of Trust II, 2020)[1]. Without capturing the persistent data exchange between entities may result in the lack of reliable and authentic evidence being required for legal or audit as a factual support when the dispute happend between entities[3]. In addition, the individual users who issue delegate credentials that claims the delegate credential holders can act legally on behalf of the individual issuers. However, there are few SSI systems that support the individual users to be on-boarded(been give the rights to issue a credential) to the SSI systems as an individual issuer who can issue the delegate credentials[4]. How to offer systematic support to the individual issuers for issuing a delegate credential in the context of business process while avoiding the abuse of authority by the individual issuers or the holder is still a big challenge.

2. Terminology

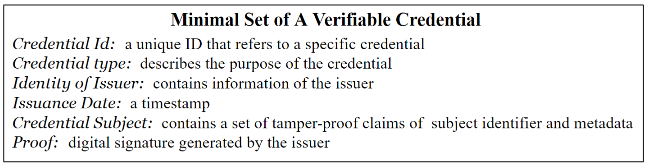
- Delegate Credential: A particular verifiable credential with a certain expiration which claims that the holder can act legally on behalf of the individual issuer.
- Transaction Records: Exchanged data containing the proof requests or presentation of credentials between the interacting entities.
- Proof Registry: An trustable data structure that stores a persistent source of evidence about the requests, presentation, and verification of verifiable credentials.
- Consent Approval Credential: A credential created to request for permission from a person or a group of people (e.g, the consent approval letter) and stored in the proof registry, which has a specific consent receipt ID as one of its attributes.

A Verifiable Credential is a tamper-proof assertions about the credential holder signed by the credential issuer, and it can be verified cryptographically.

It should contain:

- a unique credential id that refers to a specific credential;
- describes the purpose the credential;
- embeds some information about the issuer such as the issuer's DID[*1];
- has a fixed timestamp;
- contains a set of tamper-proof claims about the credential subject(the credential holder) such as the holder's id, the holder's name, an so on;
- a cryptographic proof generated by the credential issuer.

This is summarised in Fig. 1.



Minimal Set of A Verifiable Credential

Credential Id: a unique ID that refers to a specific credential
Credential type: describes the purpose of the credential
Identity of Issuer: contains information of the issuer
Issuance Date: a timestamp
Credential Subject: contains a set of tamper-proof claims of subject identifier and metadata
Proof: digital signature generated by the issuer

Fig. 1　Example of A Minimal Set of A Verifiable Credential

3. TXA-IMS

Fig. 2 shows the proposed framework of TXA-IMS with certain core components in it. The government in the governance layer sets the governance framework and acts as an endorser to approve the organizations be in the governance framework. Credential exchange happens in

[*1] https://www.w3.org/TR/did-core/

the middle layer, the issuers such as a school or a company issues a specific-purpose credential (namely **verifiable crendential(VC)** e.g, transcript, certificate of employment) to the holder, and then the holder presents the zero-knowledge proof(ZKP) based **verifiable presentation**(namely VP, an aggregation of some subsets of VCs about the holder) to reveal selected information to the verifier. The blockchain(the ledger) used to store and answer to the queries for non-privacy information such as the public key and DID, which technically enabling the decentralized governance of the SSI system. The Verifier verifies the authenticity and tamper-evident nature of the VP by querying the information from the blockchain. The verifier can trust that the credential holder and the person claiming to be the credential holder are the same based on a pre-built trust relationship between the issuer and the verifier. All the transaction records are captured and stored in the proof registry of the auditing layer, which can serve as an reliable and authentic evidence of transactions after the fact. Therefore, the proposed framework which follows the concept of 'private by design'[2] is successful in preserving the privacy of the holder while recording the exchanged data between the interacting entities(interacting participants) to meet audit and accountability requirements.

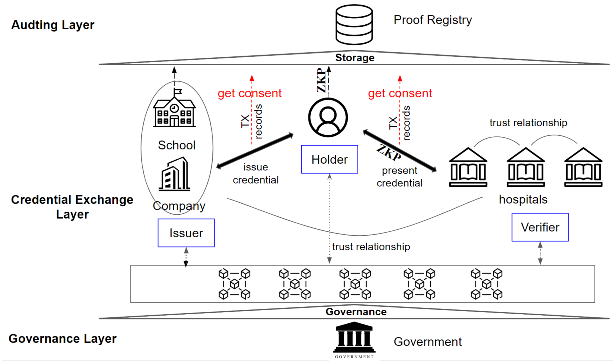


Fig. 2 Core Components in the Framework of TXA-IMS

The following two application cases(Fig. 3) help illustrate how the proposed framework could be applied to solve real-world problems.

In the case 1, the hospital is running some clinical trials, and Alice is one of the participants who is interested in one of the trials and wants to participate in the trial by sharing her verifiable health data. The hospital plays both the role of the issuer and the verifier, as it not only needs to request a verifiable credential from Alice to verify the authenticity and tamper-proofness of the personal data provided by Alice, but issues a **consent approval credential** to Alice. Alice has to make a consent on sharing her personal health data by requesting a consent approval credential(like an informed consent form for clinical research), and all the exchanged data as a whole must be recorded in the proof registry during the credential issuance process. Those records can serve as evidence in case of a dispute between two entities.

In the case 2, the individual issuer is given the ability to issue the **delegate credential**(with an expiration due) via trust propagation in which official issuers(authorized organizations, e.g hospital) signs the delegate credential and passes it to the proxy issuers(e.g the doctor), and then the proxy issuer passes the delegate credential to the individual issuers. The individual issuer's DID is added into the blockchain as part of the information. It helps to increase the level of credibility of the delegate credential issued by the individual issuer when the drugstore or hospital(the verifier) verifies the the authority and tamper-proof of the verifiable presentation by querying the data from the blockchain.

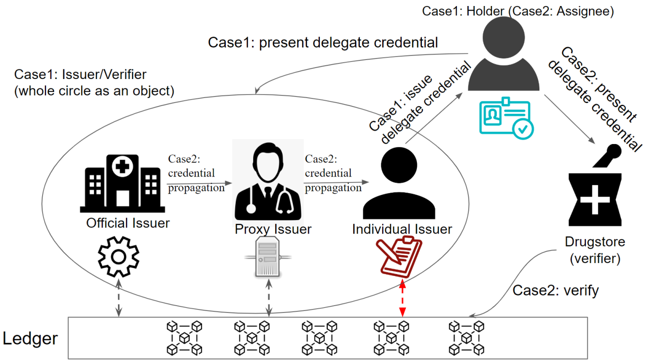

Case1: Holder (Case2: Assignee)
Case1: present delegate credential
Case1: Issuer/Verifier
(whole circle as an object)
Case1: issue delegate credential
Case2: present delegate credential
Case2: credential propagation
Case2: credential propagation
Official Issuer
Proxy Issuer
Individual Issuer
Drugstore
(verifier)
Case2: verify
Ledger

Fig. 3 Case1: Clinical Trials and Case2: Delegation of Authority

4. Conclusion

The proposed core framework is designed to implement the delegation of authority to the individuals while recording the exchanged data between interacting participants to avoid the abuse of authority either by the individual issuers or the holders. We are exploring the practicality solution for the expansion of the application of the SSI systems.

References

[1] MD Adrian Gropper. "Powering the Physician-Patient Relationship with HIE of One Blockchain Health IT". In: *A White Paper from Rebooting the Web of Trust II: ID2020 Design Workshop*. 2020. URL: https://github.com/WebOfTrustInfo.

[2] Uwe Der, Stefan Jähnichen, and Jan Sürmeli. *Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution*. 2017. DOI: 10.48550/ARXIV.1712.01767. URL: https://arxiv.org/abs/1712.01767.

[3] Victoria Lemieux, Artemij Voskobojnikov, and Meng Kang. "Addressing Audit and Accountability Issues in Self-Sovereign Identity Blockchain Systems Using Archival Science Principles". In: *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. 2021, pp. 1210–1216. DOI: 10.1109/COMPSAC51774.2021.00167.

[4] Rahma Mukta et al. "CredTrust: Credential Based Issuer Management for Trust in Self-Sovereign Identity". In: *2022 IEEE International Conference on Blockchain (Blockchain)*. 2022, pp. 334–339. DOI: 10.1109/Blockchain55522.2022.00053.

[5] Nitin Naik and Paul Jenkins. "Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity". In: *2020 7th International Conference on Behavioural and Social Computing (BESC)*. 2020, pp. 1–6. DOI: 10.1109/BESC51023.2020.9348298.