Credential-based Trust Management in Self Sovereign Identity

Rahma Mukta [1], Hye-young Paik[1], Qinghua Lu [2], Salil S. Kanhere [1]
[1]University of New South Wales, Sydney [2]Data61, CSIRO, Sydney

ABSTRACT

Self Sovereign Identity (SSI) facilitates self-control on digitized credentials without depending on a centralised authority for trust management among interacting entities. However, in current SSI solutions, credential issuers are still assumed to be from "official" sources (e.g., government agencies) and there is no systematic support for personal issuers in terms of managing trust of the issuers. This engenders lack of trust between personal issuers and verifiers. We propose a blockchain-based, decentralised credential and identity management system that allows issuer authentication through the establishment of a verifiable credential based 'Web of Trust' of personal issuers. Our work aims to establish an effective governance framework for personal issuers by introducing multi-layered issuer authorities and credential-based trust management for authenticated issuer on-boarding.

KEYWORDS

Blockchain, self-sovereign identity, public issuer, verifiable credential, web of trust, governance

1 INTRODUCTION

A secure and trustworthy digital IDentity Management (IDM) is a prerequisite for digital interactions. Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) have been proposed as a self-sovereign and decentralised IDM platform. This platform promises much freedom and autonomy for individuals with their identity and the ability to manage identity related claims by themselves. The cryptography involved in SSI is used to prove and verify the possession of the claim.

According to core Self-Sovereign Identity (SSI) principles, each DID owner should have the same technical reliability to be an issuer as the well-known, "official" issuers (e.g., accredited universities issuing degree certificates, governments issuing licenses)[1]. Because every DID has an associated public-private key pair, anyone with a DID should be able to digitally issue and sign verifiable claims and other documents [5]. However, in the current working SSI solutions only the well-known institutions grant a level of trust and authority as credential issuers [2–4]. The trust issue arises when a "personal" issuer needs to be on-boarded as an authenticated issuer (e.g., a busy parent needs to authorise his neighbour to pick up a child from school, the patient needs to authorise his relative to take decision in critical health condition). Figure 1 shows the missing relationship between "personal" issuer and SSI platform. The cryptographic solution of SSI are well suited to prove and verify the possession of a DID (claim), however, there is not yet a SSI oriented solution to describe how the trust in "personal" issuers can be established. But for the whole exercise system to work, we need that "personal" issuers to be introduced in SSI infrastructure and being able to have the trust.

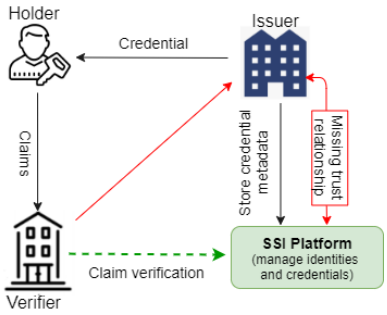

Figure 1: SSI ecosystem highlighting the missing relation among SSI platform and personal issuers. This missing trust relationship has direct impact on trust between verifier and personal issuer, because verifier needs to verify issuer legitimacy through SSI (without direct communication to issuer)

Our proposed solution extends our previous works of SSI management using blockchain named *CredChain* [3]. In *CredChain*, we presented an architecture for secure credential sharing, where we assumed registered well known issuers as trusted. This paper aims to build up issuer trust that can support "personal" issuers.

2 PROPOSED SYSTEM

In this section, we describe the proposed solution including the idea of credential based trust management and the high level view of our proposed framework.

2.1 Credential-based Trust

A VC [1] is a digitally signed assertion by a credential issuer about the credential holder. SSI uses public key cryptography to guarantee the unforgeability of VC.

'Web of Trust' is a cryptography concept that establishes an authentic binding between a public key and its owner's attributes. Some other people who want to assert the owner's attribute, signs it with their private key. We propose the concept of "supporting credentials" for personal issuers as a way to introduce this assertion to create 'Web of Trust' principle in our framework. A "supporting credential" is a VC that specifies the issuer's trust on the supporting credential holder. With this trust, the holder is able to be on-boarded as a credential issuer. For example, in fig 3 Hospital A (issuer) can generate a supporting credential to assert a newly appointed General Physician (GP) as a medical record issuer.

Here, in first supporting credential Hospital A (well known issuer) asserts that GP is a registered healthcare provider. Thus in second supporting credential, GP as a medical record issuer is in a position to identify and assert his patient B. From above example,

[1]W3C Verifiable Credential, http://www.w3c.org/2017/vc/WG

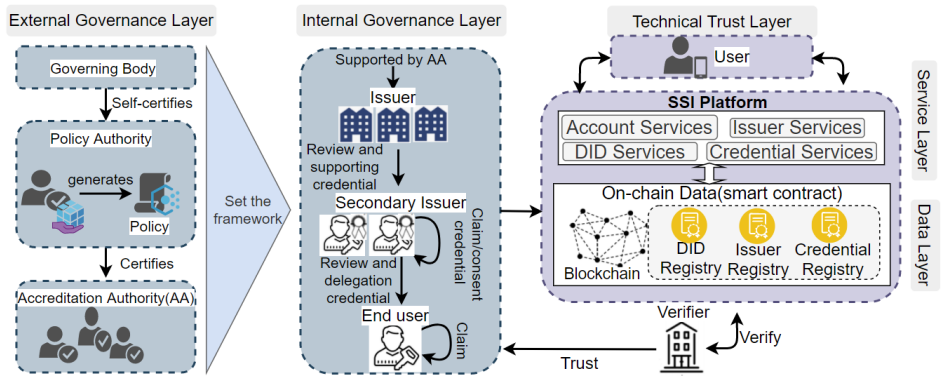

Figure 2: Proposed Framework for Trust Management

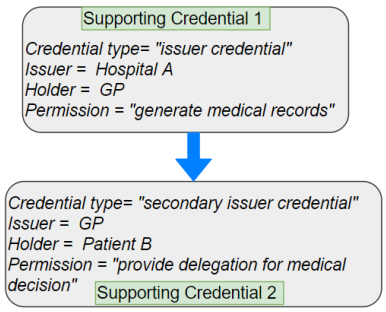

Figure 3: Chain of Two Supporting Credential

GP can assert his patient as a personal issuer to generate "delegation credential" (e.g., delegation to a relative for taking emergency treatment decision while patient is unconscious). In this way, *a chain of credentials* can be created, where the holder of a supporting credential becomes the issuer of the next credential in the chain. Supporting credentials include both issuer and holder DID to trace a web of trust from a well known issuer whose assertion gradually comes to the submitting holder.

2.2 Credential-based Trust Framework

Figure 2 shows the proposed framework for trust management with multi-layered issuer authorities. The *Governing Body* is the root of the authority chain. It must be a real-world entity, established by real people and thus have standing to self-certify themselves as a *Policy Authority* (PA).

A PA defines a policy or set of policies that establish the conditions about who can generate which credential, for example, a doctor can issue credentials related to medical records only. The PA issues a supporting credential to each *Accreditation Authority* (AA) they certify. The responsibility of the AA is to certify *Issuer*. The AA issues a supporting credential to each *Issuer* they certify. According to the agreement with the AA, an *Issuer* may certify other issuers on their own domain. For example, hospital may support affiliated doctors as *Issuer* to generate medical records.

The *Issuer* is responsible to issue a Verifiable Credential (e.g., health records, prescription) and a supporting credential (if needed) to certify his patient as *Secondary Issuer* that conforms to the terms of their agreement with the AA. For example, GP may issue medical records to his patients and when required, GP may support his patients (i.e., personal issuer) as *Secondary Issuer* to generate delegation credential.

Issuers (or Secondary Issuer) send request for issuer registration to SSI platform with their supporting credentials. During verification platform owner receives issuer public key from *Technical Trust Layer* associated with issuer DID. This key is used to verify the authenticity and integrity of shared credentials and corresponding issuer's signature. Upon successful verification, supporting credential holders will be on-boarded as the *Issuer (or Secondary Issuer)*, which means that their user DID from *DID registry* will be registered as issuer DID on *Issuer registry*. When it is desirable for an *Issuer* to be further authorized, verifier may verify their supporting credential from *Technical Trust Layer* using corresponding issuer signature.

3 CONCLUSION

This ongoing research work motivated the need to address the trust issue during issuer on-boarding in SSI ecosystem and described how the credential based 'Web of Trust' can be used as a solution. We are exploring the practicality of the proposed system via a case study to evaluate various metrics in terms of real time performance in addition to analyze the implementation effort required.

REFERENCES

[1] J. Andrieu. 2016. *A Technology-Free Definition of Self-Sovereign Identity.* Technical Report. https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/characteristics-of-sovereign-identity.md.
[2] Valentin Gerard. 2019. *Designing the future identity: authentication and authorization through self-sovereign identity.* Master's thesis. TU Delft Electrical Engineering, Mathematics and Computer Science, Delft University of Technology.
[3] R. Mukta, J. Martens, H. Paik, Q. Lu, and S. S. Kanhere. 2020. Blockchain-Based Verifiable Credential Sharing with Selective Disclosure. In *IEEE TrustCom.* 959–966.
[4] R. Soltani, U. Trang Nguyen, and A. An. 2018. A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger. In *IEEE iThings and IEEE GreenCom and IEEE CPSCom and IEEE SmartData.* 1129–1136.
[5] P. Windley and D. Reed. 2018. *Sovrin™: A Protocol and Token for Self Sovereign Identity and Decentralized Trust.* Technical Report. Sovrin Foundation-Identity for all.