Submission: Oral Communication

A Word on Policy-based Credential Disclosure in SSI

Stefano Bistarelli[1], Chiara Luchini[1] and Francesco Santini[1]

[1]*Department of Mathematics and Computer Science University of Perugia, Italy*

Abstract

We survey issues that may exist during the authentication process between the holder and verifier in the *Self-Sovereign Identity* (SSI) approach. Some possible solutions are also mentioned, such as data policies, negotiation protocols, and constraint-based validation.

Keywords

Self-Sovereign Identity, Blockchain, Access Policy

The blockchain technology has experienced huge success in different areas, including managing digital identities. This technology adapts to new methods of personal data management thanks to its decentralized consent protocol and distributed approach [1]. Also, *Identity and Access Management* IAM models have been increasingly recognized due to the ever-growing need for digital identities: these systems collect services that support the creation, modification, and removal of identities and associated accounts, as well as the authentication and authorization required to access resources. SSI is the state of the art solution for allowing a high level of privacy with users' information. However, some situations may need additional control on how and which credentials are disclosed.

Some recent studies have attempted to create an IAM system without a central trusted third-party, through the help of *Self-Sovereign Identity* (*SSI*). The main idea is to enable individuals to own and manage their digital identity, leading to a user-centric model [2]. To accomplish this goal, the user's credentials are managed exclusively by the user itself, and they are usually stored in private storage. These credentials are issued by a claim *issuer* and they are indicated as *verifiable credentials*. They describe many claims, which are nothing more than assertions concerning the user, and they are verifiable through a signature of an attestation issuer. So an attestation can be seen as proof in the form of a signature, by the claim-issuer's private key. The holder can use these verifiable credentials to gain access to some resources held by the *verifier*.

Figure 1 depicts an example of SSI flow and some credential swap issues. The verifier may ask for multiple credentials from the user, who is somehow forced to send them to have access to a given resource. This request can lead to an abuse of power by the verifier, which receives more information than necessary. Moreover, there can be verifier/verifier *collusion* issues related to the disclosure of the holder's credentials. Collusion is a non-competitive and often secret agreement in which rivals help each other to achieve an objective: two verifiers may collaborate to gain illegal access to some holder information. Additionally, a verifier could obtain specific information by asking certain questions. SSI is often used with *Zero Knowledge Proof* (*ZKP*), which is a method of demonstrating to know certain information without actually revealing it [3]. It is being used in this IAM template by any party who wants to prove that they know or have a particular credential. For example, it is not necessary for a holder to actually disclose

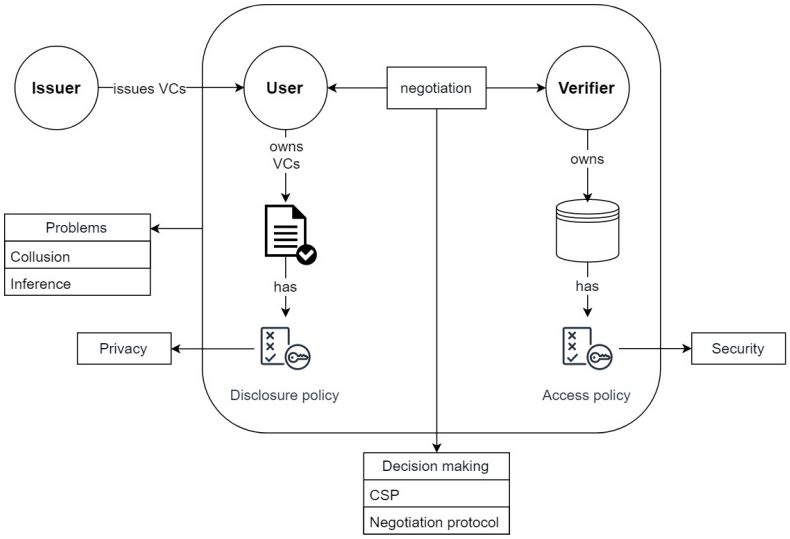

Figure 1: A possible SSI flow with some authentication issues.

his age or date of birth when a verifier asks if she is over 18. But let us assume a verifier first asks if the holder is over 18 and then under 20 years old and she receives a positive response to both; a verifier can easily infer that the holder is 19 years old. In general, we may have sensitive information disclosed from non-sensitive one (i.e., the so-called *inference problem*).

Therefore, a disclosure policy can be applied to verifiable credentials to protect users' privacy. This policy aims to preserve users' privacy by choosing whether a verifier can see this personal data or not. This choice may depend on several factors, such as verifier relationships, data sensitivity, or previous credential disclosures. As well as the holder, the issuer can deliver specific access-policies that are mandatory to use such credentials. The idea is then to enforce both *mandatory* and *discretionary* access control (*MAC*/*DAC*) on the holder's credentials.

In this way, she solves security problems connected to authorization issues, she decides who can access the resource. In addition to the policy, some methods of negotiation between the two parties could be used. Consequently, there is an agreement between the parties on which data to exchange. The negotiation process can be indicated as a decision-making process based on some negotiation protocols or Constraint Satisfaction Problems (CSP).

References

[1] Q. Stokkink, J. Pouwelse, Deployment of a blockchain-based self-sovereign identity, in: 2018 IEEE international conference iThings/GreenCom/CPSCom/SmartData, IEEE, 2018, pp. 1336–1342.

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

[3] U. Fiege, A. Fiat, A. Shamir, Zero knowledge proofs of identity, in: Proceedings of the nineteenth annual ACM symposium on Theory of computing, 1987, pp. 210–217.