Industry Grade Self-Sovereign Identity

Rowdy Chotkan
R.M.Chotkan@student.tudelft.nl

Introduction

This document describes a research proposal into the development of an *Industry-Grade Self-Sovereign Identity* (IG-SSI) scheme. This scheme will be developed with collaboration of the Dutch Ministry of the Interior and Kingdom Relations and will serve as research into a digital identity scheme for the Europen Union. As this thesis is written per requirements of the 4TU Cyber Security programme, it will focus on applicable Cyber Security concepts and as such privacy and security will be the core of the design.

Research Area

Self-Sovereign Identity (SSI) can be described as the decentralisation of ones identity: moving the power of managing ones identity and attributes from central authorities to the individual. As such, SSI has the capability to provide one to interact in the digital domain with the same (or an ever greater) level of trust as one would in the physical domain. Main research attributions have been performed with such a revolution in mind: bringing power to the individual and, as such, removing power from central authorities. However, with the massive scale adoption of SSI being far from realised, there is still much to gain.

Consider the existence of a unified European SSI that is valid throughout each European member state, providing the ability of identification throughout the entirety of the European Union. We shall refer to such a construction as requiring an *Industry-Grade Self-Sovereign Identity* scheme (IG-SSI). Such a construction raises a tremendous amount of problems to be solved. Broadly speaking, there exist three types of problems to be solved: (1) privacy and confidentiality, (2) deployment, and (3) revocation. Next, we briefly touch on these aspects. To set more grounds to this analysis, we shall discuss possible drawback using the Cyber Security Triad CIA (confidentiality, integrity, and availability).

Privacy & Confidentiality

Such an SSI scheme must remain confidential to at least the extent a traditional identification measure is: a third party should only have access to the attributes he is provided access to by the owner. In a traditional approach, the owner, as well as the issuing authority, have full access to the document. However, this raises an issue when such an infrastructure is applied to an Industry-Grade SSI construction: which government/authority has access to what information? In the case of a European SSI: providing all countries access to the identities of all European citizens has the drawback of broadening the landscape for possible security breaches, thus possibly weakening the *confidentiality* and *integrity* constraints. Providing a sole country access (e.g., the issuer or the country of current residence of the owner), leads to the issue that a single authority has access to all identities of all European citizens. As now a sole country has access to all identities and as such, overlooking possible miss-use, a security breach could now possibly impact the entirety of the European population (as apposed to only the residents of said country). As apposed from the authoritarian problems, in order to safeguard unauthorised access and, as such, guarantee confidentiality and integrity, proper encryption mechanism must be set in place. The selection of cryptography is non-trivial as it must have properties such as future proofness and compatibility.

Deployment

Based on the privacy and confidentiality analysis, an IG-SSI scheme, is best to be developed and deployed distributed. As we can identify additional problems with providing access to single/multiple authorities: firstly, a possible shortcoming of *availability* in case the authorities' digital infrastructure is insufficient. Alternatively, availability may be in peril in case a single authority now may possess the capability to nullify the digital identities of e.g. the entire European population. Finally, integrity may be jeopardised as one can not be sure that a single authority does not have alternative motives impacting the data of other users. As such, a distributed deployment model may prove to overcome these shortcoming, enabling for the data of the digital identities to stay in the hands of the owners which are the sole users.

By decentralising an SSI scheme to such an extent that it is fully managed by the owner, no single authority nor multiple authorities require full access to the identity; they can simply act as a signing and verification party.

Revocation

The final aspect of an SSI scheme is *revocation*. Revocation allows a party to revoke attributes from a digital identity. In a centralised construction, revocation is trivial to develop

through, e.g., a blacklist, however, for a decentralised SSI scheme such a functionality can prove to be more cumbersome to design. An example design would be making an attribute no longer be verifiable. Revocation is still a fairly open topic in SSI. Proposed solutions include the usage of special authorities being delegated the role of marking attributes as revoked for identities (Van Bruggen, 2020).

Knowledge Gap

The majority of research into Self-Sovereign Identity serves a unified solution for online identification. E.g., see (Tobin & Reed, 2016) which describe SSI as "*the Internet's missing identity layer*", thus resolving the need for different security architectures (with the purpose of identification) for different platforms. Zwitter, Gstrein, and Yap (2020) discuss SSI as an opportunity to separate digital identity from the oligopoly of dominant corporate actors and governments. Ferdous, Chowdhury, and Alassafi (2019) discuss a mathematical framework which can be used to implement an SSI scheme and discuss how such an implementation can be leveraged using blockchain technology. However, they do not address the legal validity nor applicable legislation. Dong, Wang, Chen, and Xiang (2020) describe the usage of SSI for banking using a blockchain approach, thus, describing an SSI feature. More specifically, they utilise SSI for authorisation for the usage of APIs provided by banks to third parties in order to prevent privacy compromises. Wang and De Filippi (2020) describe the need for SSI in order to lower the threshold of economic inclusion. I.e., identification is required for services such as banking, however, a great portion of the worlds population has no access to basic identification documents. Cameron (2005) describe the so-called *Laws of Identity*, where "laws" uses the scientific definition. In their work, Cameron describe the laws to which identity systems need to adhere to in order to create stable digital identities and systems. Allen (2016) describes the steps required for the introduction of SSI as well as the ten principles of Self-Sovereign Identity, on which many of the solutions described in this section adhere to. Stokkink and Pouwelse (2018) describe an SSI scheme that is designed to serve as a Dutch Self-Sovereign Identity implementation through truth establishments of attestations. They propose a scheme utilising zero knowledge proves and adherence to the aforementioned principles of Self-Sovereign Identity by Allen. Stokkink and Pouwelse's design was created in cooperation with the Dutch Ministry of the Interior and Kingdom Relations and they state that the solution is ready to be deployed globally. Finally, Stokkink, Epema, and Pouwelse propose the *IPv8* system, which is described as a complete system for passport-grade Self-Sovereign Identity. The scheme of Stokkink and Pouwelse (2018) is build on the same system.

Contributions

The work set out by Stokkink and Pouwelse and Stokkink et al. will serve as a foundation of the IG-SSI scheme. The contributions made by this thesis will be an SSI scheme that can be said to be of *industry-strength*, which will be substantiated with a real-life trial of an implemention of said scheme. The main knowledge gap currently existing in the research area of SSI is the gap between the theoretical frameworks and the practicality of an implementation of these theoretical frameworks. As such, this thesis will attempt to bridge this gap by constructing an SSI scheme together with developing an interaction model that allows for a practical implementation that is to be verified through real-life user tests.

Research Questions

The topic of Self-Sovereign Identity and the notion of *Industry-Grade Self-Sovereign Identity* shall foremost be investigated through the following research question:

> *"How can Self-Sovereign Identity serve as a digital alternative to centralised identification measures?"*

This research question will allow for the investigation into and the development of a state-of-the-art SSI scheme. As such, we can derive the following sub-questions that can be used to substantiate an answer to this research question. The following sub-questions will be investigated:

1. *What are the problems/limitations that SSI attempts to overcome?*
2. *How can "Industry-Grade Self-Sovereign Identity" be defined?*
3. *What is the current state-of-the-art in SSI research?*
4. *What is the practicality of implementations of the current state-of-the-art research?*
5. *What are the major shortcomings of the current state-of-the-art schemes?*

Through these sub-questions, we will be able to identity the state-of-the-art of SSI schemes and analyse their practicality and shortcomings. Based on these results, we will be able to design an SSI scheme that will overcome these shortcomings and be deemed to be of *industry-strength*.

References

Allen, C. (2016, May). *The path to self-sovereign identity.* CoinDesk. Retrieved from `https://www.coindesk.com/path-self-sovereign-identity`

Cameron, K. (2005). The laws of identity. *Microsoft Corp*, *5*, 8–11.

Dong, C., Wang, Z., Chen, S., & Xiang, Y. (2020). Bbm: A blockchain-based model for open banking via self-sovereign identity. In *International conference on blockchain* (pp. 61–75).

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access*, *7*, 103059–103079.

Stokkink, Q., Epema, D., & Pouwelse, J. (2020). A truly self-sovereign identity system. *arXiv preprint arXiv:2007.00415*.

Stokkink, Q., & Pouwelse, J. (2018). Deployment of a blockchain-based self-sovereign identity. In *2018 ieee international conference on internet of things (ithings) and ieee green computing and communications (greencom) and ieee cyber, physical and social computing (cpscom) and ieee smart data (smartdata)* (pp. 1336–1342).

Tobin, A., & Reed, D. (2016). The inevitable rise of self-sovereign identity. *The Sovrin Foundation*, *29*(2016).

Van Bruggen, C. (2020). *Forward-looking consistency inattribute-based credentials.*

Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain*, *2*, 28.

Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: Universal identity management and the concept of the "self-sovereign" individual. *Frontiers in Blockchain*, *3*. doi: 10.3389/fbloc.2020.00026