Interoperability in the Self-Sovereign Identity SuperApp

Merel Steenbergen[1] , **Martijn de Vos**[1] , **Johan Pouwelse**[1]
[1]TU Delft
M.A.Steenbergen@student.tudelft.nl, {SUPERVISOR1, SUPERVISOR2}@tudelft.nl

Abstract

Do not forget to change this afterwards.
This should be rewritten with academic language use.
This needs more work or a meeting with my supervisor.
The abstract should be short and give the overall idea: what is the background, the research questions, what is contribution, and what are the main conclusions. It should be readable as a stand-alone text (preferably no references to the paper or outside literature).

1 Introduction

When the World Wide Web was introduced in 1990, users identified themselves with usernames and passwords, creating a new account for every service. Even though Single Sign-On has reduced the number of passwords per user, passwords are still a major security risk. In 2017, the password manager LastPass analysed the data of employees of over 30.000 companies using the service and found that the average amount of accounts per employee is 191 [1]. This is because identity storage is still centralized. If one wants to login to a service, the username and password are stored in a database owned by the service.

This approach has many disadvantages. The first being that the service has control over the users' data. As an example, the terms of service of Instagram state the following[1]: "We reserve the right to modify or terminate the Service or your access to the Service for any reason, without notice, at any time, and without liability to you". [2] clearly explains the impact that this might have on end-users: "Because the only online identities most people have are centralised, the removal or deletion of an account effectively erases a person's online identity which they may have spent years cultivating and may be of significant value to them, and impossible to replace." In addition, these data duplicates ensure that the estimated total cost of identity assurance in the UK exceeds 3.3 billion pounds. CTRL-Shift has estimated that using 'make once, use many times' strategies could reduce this to 150 million pounds [3].

[1]Instagram's terms of service 2021

Self-sovereign identity aims to solve the problem by providing users with complete control over their data. This is achieved with decentralized data management, such as blockchain. The TrustChain SuperApp is a mobile application under development by the Delft Blockchain Lab. It aims to create a digital foundational identity. However, it currently cannot transfer data to other applications. This is an essential aspect of SSI to ensure third parties, such as the government, can request data from a user to confirm their identity.

This research will focus on creating a secure and reliable way to transfer data from the SuperApp to a third party. A possible use case for this is buying alcohol online. The SuperApp could be used to confirm that the buyer is actually of legal drinking age. There are some challenges to transferring data outside of the blockchain. These will be explored first in the Problem Description, then the chosen solution will be explained in the section.

Afterwards, the contributions to the SuperApp will briefly be discussed. Then, I'll reflect on the ethical aspects of my research in section 5 and a reflection on the results will be given in the Discussion. Finally, the conclusion will contain a brief summary of the problem and solution and elaborate on future research that might be conducted in this field.

Briefly explain my contributions

2 Problem Description

To define Self-Sovereign Identity, the ten principles that were devised by Christopher Allen are often used. The sixth of which is Data Portability: "Information and services about identity must be transportable" [4, p. 14].

The SuperApp currently does not support the transfer of data across applications. Thus the identity that a user builds and stores can only be used within the application itself. This situation is not desirable as it implies that each service currently in use by end users would have to be replaced with an equivalent in the SuperApp. As mentioned before, the average employee has 191 accounts across different platforms. The SuperApp has been designed to be able to replace most, if not all, of these. Still, it would be more effortless, both for users and developers, to make the SuperApp collaborate with other applications, rather than making it replace them.

Naturally, one of the difficulties of transferring data out of the blockchain is security. Data could be intercepted or possibly even altered by a malicious user, who could reveal the

data to anyone. A trade-off exists between anonymity and identity: The more parts of one's identity are revealed, the less anonymous the individual is. One way to solve this is to not send the data itself, but only the evidence that you identity has been proven. For instance, the government may attest that you are actually over eighteen. When a liquor store wants confirmation of this, the attestation that the government provided can be sent. This way, proof is provided that you are old enough to buy liquor, without providing a precise age, which prevents malicious users from intercepting any useful data. The approach to sending attestation in the SuperApp is through private and public key pairs. The problem that this research will aim to solve is the problem of sending attestations to other applications, which will require a framework for other applications to use.

There is another problem to sending these attestations, as they can only confirm certain facts, also called claims. Per example, Spotify would not be able to retrieve the last listened to song from the SuperApp, they could only claim it is a certain song. Therefore, they could not easily use the extensive algorithms they now use to recommend new music to users based on their listening history.

3 Sending attestations

Here will be a paragraph explaining the structure of this section. I need to add my sources (are now in my bib file as hyperlinks). This section is not using academic language use, so I need to rewrite it, but making the entire section blue was distracting.

The process of attestation

SSI solutions, such as the SuperApp, currently send their data through verifiable claims. In the process of sending data, three parties are involved. The first party is the subject. This is the user of an application and the person that needs to identify themselves. The key idea of SSI is that the subject is in full control over their data and identity, deciding which other parties gain or lose access. However, often data has to be verified or issued by a trusted party, the issuer. An example of an issuer is the government, because they can provide a proof of your date of birth or of the fact that you have a drivers license. These proofs are called attestations and can be revoked, for example when your drivers license expires and the subject does not get it renewed. The third party involved in the flow of data is the relying party. This party often is a service that requests the subject for identification, which is done by making a verifiable claim, for example: "You are over eighteen."

Upon receiving such a verifiable claim (VC), the subject does not have to send the data to prove the claim. The VC acts as a yes-no question and the only acceptable answer is the signature that was used by the issuer to verify the identity of the subject. So instead of providing your date of birth to verify you are over eighteen, you provide the signature of the government that was used to sign the fact that you are over eighteen. These signatures are combined with some metadata to ensure they can only be used on this particular data. This metadata can, among others, contain a name, expiration date and signature scheme [5].

Private-public key pairs

This issuing of identities and signing of VCs is done with private-public key pairs. The advantage of private-public key pairs is that they are self-authenticating, they do not require a third trusted party to assign or verify the keys as opposed to, for example, Universally Unique Identifiers [5]. This strengthens the decentralized aspect of SSI as you do not rely on a third party to verify your identifier.

To give the user full control over their identity and keep the solution decentralized, the private keys should be stored on the user's device, which usually is a smartphone. The smartphone is portable and widely used. In 2018, 84% of the Dutch citizens had access to a smartphone with internet connection [eurostat]. This poses some threats of loss of keys upon losing the phone, for which several solution have been researched. However, the problem of data resilience is out of the scope of this research.

The public keys are stored on the blockchain. This way, a protocol like Pretty Good Privacy (PGP) could be used. In short, this means that messages are encrypted using a random key, which itself is encrypted using the receiver's public key. The receiver can decrypt the random key with their private key and subsequently decrypt the message using the random key.

This is where my writing ends and the template (and my notes) begins

URL schemes

Can send more data than just a confirmation, but is less secure and can be intercepted more easily.

Private-public key pairs

Is very secure and can only be decrypted by the receiver or a quantum computer, but can send limited data. It can only verify claims, not send data such as "history of songs listened to"

Pretty Good Privacy

https://w3c.github.io/webpayments-ig/VCTF/charter/faq.html Service-centric vs self-sovereign: Is the complete switch possible?

4 Experimental Setup and Results

As discussed earlier, in many sciences the methodology is explained in section 2 and this section only discusses the results. However, in computer science, most often the details of the evaluation setup are described here first (simulation environment, etc.). Very important here is that any skilled reader would be able to reproduce this setup and then obtain the same results.

Do we include the tools used here? E.g. Android Studio

Then, results are reported in an accessible manner through figures (preferably with captions that allow them to be understood without going through the whole text), observations are made that clearly follow from the presented results. Conclusions are drawn that follow logically from the previous material. Sometimes the conclusions are in fact hypotheses, which in turn may give rise to new experiments to be validated.

You may want to give this section another name.

5 Responsible Research

Reflect on the ethical aspects of your research and discuss the reproducibility of your methods.

6 Discussion

Results can be compared to known results and placed in a broader context. Provide a reflection on what has been concluded and how this was done. Then give a further possible explanation of results.

You may give this section another name, or merge it with the one before or the one hereafter.

7 Conclusions and Future Work

Summarize the research question(s) and the answers to the research question(s). Make statements. Highlight interesting elements.

Discuss open issues, possible improvements, and new questions that arise from this work; formulate recommendations for further research.

ideally, this section can stand on its own: it should be readable without having read the earlier sections.

References

[1] LastPass Enterprise, "The password exposé. 8 truths about the threats - and opportunities – of employee passwords," tech. rep., LastPass, 2017.

[2] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," March 2017.

[3] A. Mitchell and J. Smith, "Economics of identity. the size and potential of the uk market for identity assurance," tech. rep., October 2015.

[4] K. Wagner, B. Némethi, E. Renieris, P. Lang, E. Brunet, and E. Holst, "Self-sovereign identity: A position paper on blockchain enabled identity and the road ahead.," pp. 13–14, October 2018.

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

A This is an appendix