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

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].

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. In this context, decentralized means user-centric; the user is the only person storing and managing their data. 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 Section 3.

Afterwards, the possibilities for the communication protocol will be evaluated and discussed. The best one will be implemented and discussed in the section about the engineering contribution, where also the design will be explained. Then, I'll reflect on the ethical aspects of my research 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 identifying: The more parts of one's identity are revealed, the less anonymous the individual is. SSI applications do have a solution for this problem, which will be explored in section

[1]Instagram's terms of service 2021

3. Afterwards, the communication protocol that will be used to send data to other applications will be explained.

3 Verifiable claims

Verifiable claims (VC) lie at the heart of SSI solutions. Almost all data is sent through these claims. In that process, 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 date of birth or the fact that the subject has a drivers license. These proofs are called attestations and can be revoked, for example when the 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.

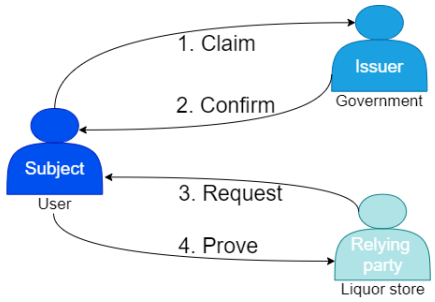

Figure 1: Parties involved in attesting data

Upon receiving such a verifiable claim, the subject does not have to send the data to prove the claim. The VC acts as a polar question to which the subject can provide an answer. Instead of providing the subject's date of birth to verify they are over eighteen, they provide the signature of the government that was used to sign the attestation. 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].

Only forwarding these attestations has the advantage that no actual data about the user is sent over a network. If a malicious user were to get hold of the data they would not get any information about the subject. To ensure anonymity of users, it is paramount to send as little information as possible. The more is known about a user, the less anonymous they are.

Perfect decentralization

In many SSI solutions, the relying party uses the same application as the subject and issuer. However, that would require a lot of work to replace currently popular applications and services. Every service in use would have to use the SSI application. This is not practical, so this research will try to find a way to enable communication between an SSI application and another service. In this case, the SSI application is the SuperApp specifically, but the general idea could be used for other applications as well.

The drawback is that verifiable claims are limited in the amount of data they are able to contain. Using only a polar question does not allow for any additional data to be sent. This implies that VCs alone will not be enough if SSI aims to replace all centralized services. Those services store more data about a user than can be requested through a verifiable claim. Take for example the full name of a user. Almost every service that makes use of accounts, stores the name of a user. This results in a great amount of duplication of stored data. However, it is hard, if not impossible, to request the name of a user with a verifiable claim without storing it locally, as the service would have to guess the name of the user.

In many SSI solutions, this is solved by using an identifier for a user. Both Blockstack and uPort have public profiles which not only include signing keys but also names and profile pictures

So to reach a fully decentralized solution, verifiable claims will not be enough. There must be a secure way to send data that cannot be requested using a polar question. However, claim portability is a key step towards full data portability, so this research will represent a universal architecture for the portability of verifiable claims. Further research could be conducted towards full data portability, as will be discussed in section 9.

4 Communication protocol

The SuperApp already includes an application for proving that the subject in over eighteen years old. However, this information currently cannot be transported to outside of the application. for this purpose, a communication protocol that can verify claims from various services should be designed. This section will explore all decisions that need to be made, such as the information that should be transmitted and the most secure way accomplish that.

Information

In the SuperApp, data transfer 1 and 2 from figure 1 have already been implemented for an 18-plus use case. In that case, the issuer and subject both use the SuperApp. The issuer is another user in the blockchain in this case, there is no distinction between a government and a random user. For part 3 and 4, a communication protocol will be designed in this paper.

It is important to decide which data needs to be sent. In section 3 it was already mentioned that an attestation includes some metadata. This metadata should at least contain a validity period or expiration time of the transaction. This makes sure that malicious users cannot take advantage of unused claims. This validity period should depend on the average response time. Next to that, a identifier or name of the transaction should also be included. If there are multiple transactions in progress between a subject and relying party, the identifier will make sure data does not get mixed up and it's clear which VCs are confirmed and which are denied.

Last but not least it is important to know if a claim has to be attested by a trusted issuer. This could be the case when buying alcohol: The government should have attested that

fact that the subject is of legal drinking age. However, some claims might be attested by the user themselves. An example of this could be accessing the website of the liquor store. For this, identification by the government isn't necessary, but the user has to testify that they are actually of age. Currently, this happens by pressing a button to verify you are old enough. Using the SuperApp would actually store the data that you visited the website. This could be used for legality purposes.

Encryption

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.

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

Voor een attestation zal ik eerst gebruik maken van Rowdy's app. Voor het deel data portability: De relying party moet een public key hebben, mogelijk op de blockchain, maar ik moet nog kijken of dit mogelijk is. User heeft een identifier op de BC. De VC wordt eerst gesigned door de relying party door te encrypten met diens private key, daarna wordt hij encrypted met de public key van de subject. Zo weet de subject waar de VC vandaan komt en kan niemand anders de VC lezen. De subject kan nu de signature van de issuer, of van zichzelf in het geval van een simpele claim, encrypten met zijn eigen private key en daarna met de public key van de relying party.

De data die nodig is bij het versturen van een claim is natuurlijk eerst de claim zelf. Dit kan een claim zijn op leeftijd, bezit van documenten of iets anders. Ook moet er natuurlijk meegestuurd worden of de claim attesten moet zijn, of gewoon een antwoord van de user zelf mag krijgen. Ik vraag me af of het nodig is om een identifier voor de VC zelf mee te sturen, hierdoor wordt het wel duidelijker waar antwoord op komt. Verder is een verlooptijd natuurlijk nodig om te voorkomen dat aanvallers oude VCs gebruiken die misschien niet aangekomen zijn om informatie te vergaren.

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?

Meeting 20-05-2021

Focussen op verifiable claims. Andere probleem een beetje uitlichten, maar niet iets mee doen.

Soort library maken, net zoals iDeal.

Decentralized uitleggen. Autonomie ook gebruiken.

SuperApp zelf is niet decentralized, maar biedt de mogelijkheid om een decentralized solution te maken.

Wat maakt mijn oplossing anders dan andere oplossingen, waarom niet gewoon OAuth gebruiken.

Ipv data portability, claim portability. Key step towards full data portability. Represent a universal architecture for the portability of verifiable claims.

Before this section, make a section about VCs (Verifiable claims lie at the heart of SSI).

https://www.tno.nl/nl/aandachtsgebieden/informatie-communicatie-technologie/roadmaps/data-sharing/ssi/

https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf

Present problems that need to be addressed when building the app: Where to store keys (on/off blockchain). Usability (both developer and user). Evaluate usability.

Relying party is another application in figure 1, make this clear.

5 Engineering contribution

Claim registry model

https://arxiv.org/pdf/1807.06346.pdf section 6b

6 Responsible Research

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

7 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.

8 Conclusions

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.

9 Further research

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