Thesis Ideas

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

Research Topics

Topic 1—International Deployment

Proposed solutions in academia and white-papers propose schemes that have the capability to be deployed globally. Additionally, simply stated, most focus on the goal of generating online trust. A form of SSI would be the deployment of an official digital passport, with the prospect of creating a valid digital document that is to be accepted in the entire European Union or even globally. Such a construct would generate additional issues, as it now involves governments of multiple countries acting as signing parties for attributes (e.g. by adapting the signature scheme described by Stokkink and Pouwelse (2018)). This requires trust that each country acts honest and that their activities cannot directly influence the SSIs of others. This research topic can be investigated by the question: *how can an SSI scheme be deployed involving the cooperation of multiple governments?*

Topic 2—Identity Theft

On the topic of identity theft, most literature focuses on MitM attacks and authenticity due to encryption properties or ZKP (thus, mostly focusing on identity theft through attributes), however, what implications are there when an entire SSI is compromised. As managing self-Sovereign Identities is devoid of governmental influences, what can be done against the theft of a digital passport (e.g., private keys are stolen)? Regular passports/IDs are only valid for five years, hence their design limits identity theft after this five year mark (at least to a certain extent). Can such a construct also be created for digital passports?

This topic touches on revocation.

Topic 3—Deployment

In order to deploy a digital passport, a suitable target environments must be selected. This entails the selection of hardware. Most preferably, something as accessible as a smartphone can be used, however, is such a platform secure enough? Alternatively, a hardware device (e.g. Rabo Scanner) could be selection. This topic would require firstly designing a scheme.

Topic 4—Design

In order to combat fraud, a suitable authentication method must be selected (e.g., biometrics, passwords). This topic would investigate suitable measures. Additionally, such a system must last years. As such, best cryptographical practices must be investigated, as well as allowing upgrading of the underlying protocol (e.g. extra functionalities or additional cryptographic algorithms).

Topic 5—Distributed Systems

What is the best type of distributed storage solution? Most solutions use a blockchain, however, there multiple types of blockchain. It can be investigated what type of blockchain or other distributed storage would be best to support such a system. E.g., public/private/hybrid blockchain approach. This comes down to the level of self-sovereignty: Fully public allows for more flexibility for the owner (citizen), however, a private approach would perhaps be less vulnerable to attacks such as identity theft. Depending on the selected blockchain technology, the blockchain itself may be vulnerable to different types of attacks (e.g. Sybil attack).

Topic 6—Legally Valid Signatures

In order for a digital passport to be functional, there must be support for digital signatures that are legally valid. As such, it must be investigated how such a construct can be created.

Topic 7—Digital Euro

The aforementioned constructions of SSI allow for a digital passport. Digital passports can be a gateway for additional transitions to digital alternatives. One such a transitions can be the support for storing a digital Euro coin. As such, it can be investigated how, additionally, support for such a construct can be created.

References

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).