Practical Decentralized Key Recovery Solution

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Gerhard Hassenstein, Prof. Dr. Annett Laube
Expert: Dr. Andreas Spichiger

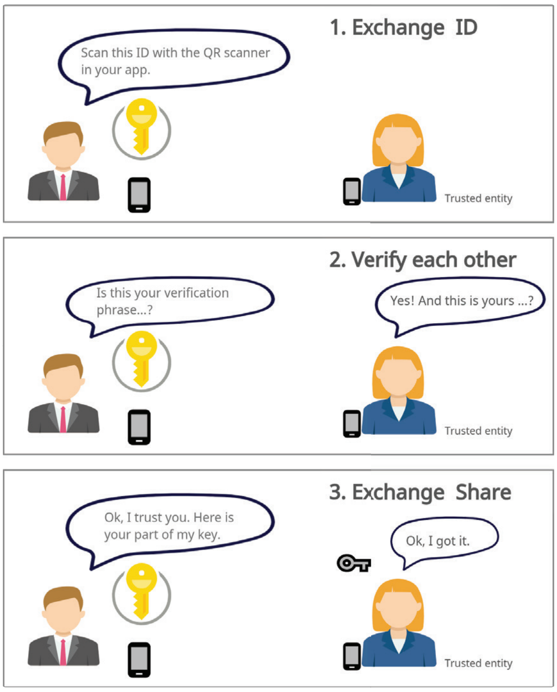
Lots of applications rely heavily on cryptographic keys without providing an appropriate option of recovering them in case of an incident. This could result in losing access to all resources and relations that rely on said key. A simple and practical solution is presented in this thesis. The solution is integrated into the existing mobile application uPort that features an Self-Sovereign Identity (SSI) wallet which is protected by the developed key recovery solution.

Problem

Whether in the emerging Self-Sovereign Identity (SSI) technology, in Bitcoin or even in simple logins - the field of application of cryptographic keys is huge. But for all these use cases, the demand arises for a simple way to recover a key after a loss without compromising its security. In particular, the use case SSI shall be in focus.

Solution

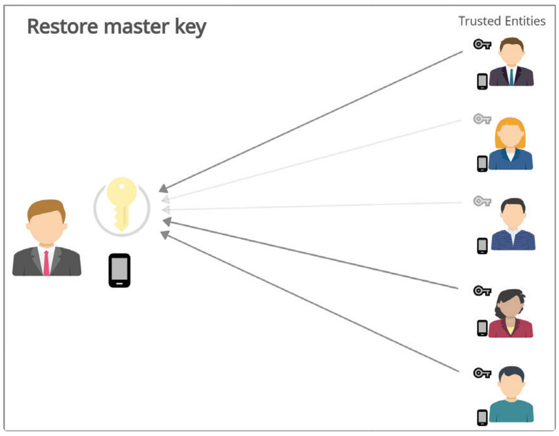
A social recovery protocol is developed that allows SSI users to securely encrypt their wallet with a master key, store the encrypted wallet on a server, then split the master key into multiple pieces and distribute them to different trusted entities like friends or relatives. This protocol is embedded into the existing mobile SSI application uPort to show the usability and simplicity of the proposed solution. The picture on the left side shows that there are only three steps needed to successfully backup the master key. They include the exchange of an ID, either via QR scanner or other out-of-band methods, the verification of the public key represented by a verification phrase and the confirmation. Using this procedure, the master key is protected securely and can be used to encrypt and decrypt the SSI wallet.
The thesis makes use of the Shamir Secret Sharing algorithm, which delivers the basis to split the key into multiple shares and combine them back to the original key even if some of the shares are lost.
To distribute these shares in a decentralized and anonymous manner a generic API is developed. This API supports not only the distribution but also the recovery of the master key. Out-of-band verification of the other party with the verification phrase ensures impersonation safety.


1. Exchange ID
Scan this ID with the QR scanner in your app.
Trusted entity
2. Verify each other
Is this your verification phrase...?
Yes! And this is yours ...?
Trusted entity
3. Exchange Share
Ok, I trust you. Here is your part of my key.
Ok, I got it.
Trusted entity

Three simple steps to backup a key

Conclusion

The project has shown that the concept of social key recovery has a lot of potential that goes far beyond the SSI use case. Wallets for cryptocurrencies in particular could also benefit enormously from such a possibility.



Restore the key by combining three of five shares

Dario Furigo

Beat Pascal Schärz