Thanks Thore Hildebrandt for review and discussion

Intro

1 billion people globally have trouble proving their identity. To propose a solution to this let me first describe the most important characteristics of a “good identity system”.

1. Users have a private key and can sign statements
2. One ID per person
3. Private
4. Decentralized

Here we describe a system that fulfils criteria 1 and 2. With a view to also solve 3 and 4.

This would be useful in the developing world as well as in the cryptocurrency community where individuality guarantees are important for things like quadratic voting. It could also be merged with proof of public key posession to ensure that participants do not hold their private key inside trusted hardware.

ZKP inspiration

The system is inspired by how zkps work. Basically the prover and the verifier play a game where the verifier asks the prover to do some operation if the prover can do this correctly they increase the verifier confidence that they know some secret information.

Then after doing this many times the verifier becomes convinced that with overwhelming probability the prover knows the secret information. Otherwise they would not have been able to do these operations.

Roles in the system

The system has 3 roles

1. Users

: have a private key and IDs. We can provide users withnfc hardware wallets so that having a mobile phone is not required to join. Also so that they cannot forget their IDs by copying the private key to another device.

1. Hosts

: gather Users

regularly in “Parites” to create, renew or update their IDs. A host can be basically anyone with a smartphone.

1. Auditor

: does not trust the Hosts

or Users

but by asking multiple questions can validate that there is a mapping of 1 to 1 between users and IDs or other information such as location. This is the remote centralized party to which we want to prove individuality.

Issuance and Validation

1. Hosts

hold monthly parties at the same time. Users

can attend a party to get an ID but must stay for the duration, this prevents Users

from attending two parties and getting two IDs.

1. Users

can attend these regular parties to initialize their ID. Their ID is created and public key signed by ever other User

. Users

attending the party validate that other Users

have been given only one ID.

1. The Auditor

doesn’t want to trust that the Users

of any given party are reliable notaries. So she randomly sends the Users

from one party to another. Note the Host

also validates and attests to their ID.

1. We repeat this increasing the number of Users

who need to lie in order to create “fake” IDs. Over time we build a web of trust. If we find a User

that participated in fraud we reduce our confidence in all Users

that they audited and that audited them.

1. We can speed this up by physically auditing the system, checking Users

ID’s are correct.

After doing this for many iterations our confidence that there is one ID per person becomes high. We can also score various IDs based upon their activity.

How do we check IDs

A user provides their ID to the checker. The checker has a smart phone app that sends a random string to the users nfc wallet. The users wallet signs the random string and returns it to smartphone. The smart phone validates the signature, gets the public key and queries the auditor for information about that public key. The auditor then returns that users ID information.

Final thoughts and future work

The system is transparent and centralized. It is also transparent to the Auditor but private to everyone else. It is possible to decentralize and add privacy. This can be explored in future work. Starting out with a centralized system seems important for initial experiments so we can see how the system is running.

This has applications in the developing world where access to IDs are sometimes a major problem.