The Public Digital Signature System

Edward Gonzalez

Kisdorf, Germany 2016

Introduction.

Signatures for the sake of decisionmaking can sometimes be hard, documents have to be signed and approved in order to perform social/legal actions; since humanity created written language, signatures on some form of communication mechanism have been the way to approve, this method has been efficient, but not so reliable.

Nowadays we have got the internet, and cryptography, the aims of cryptography is to secure data, but it also has another use that is little heard of, to sign data; where old school signatures are based on paper, digital signatures are a piece of data that are able to generate a unique cryptographic hash that "**cannot be falsified**" by no actual means, in fact, using an RSA 2048 algorithm it could take up to 4 billion years to falsify with a standard computer.

There is little introduction of the usage of technology to solve social problems, or to help in legal situations; however the potential is huge, but it could be out of fear or lack of understanding that these solutions are rarely applied but in private corporate environments.

In a given scenario, you need someone to sign a document for you, and for that you'd require to find that person; and then get their signature. In a more formal scenario some form of law enforcer has to be present, this is not efficient, because it's a problem that simple cryptography can solve. Validating such paper can be hard, specially if it gets to court, using digital signatures does not make it just easier, but basically **infallible**.

In another scenario when a social situation is present that needs support people recur to paper but this method is **easy to corrupt**, and **hard to test**; it's also a **waste of time, paper and manpower** for both the person that signs and the people that have to collect such signatures, this is not efficient.

With a digital signature based system it takes **less than a day to validate millions of signatures**, and it requires no personal at all to do so, it also harness the potential of social networks since it can be used in conjuction of it; it also only needs the will of one person to prepare a document and make it public, providing the link for such access. Using a digital signature based system, anyone can use the potential of it to provide ways of social change, being in a local business, community or society, depending to at which level the system is used.

Here I propose a solution I call “The public digital signature system”, which aims to allow anyone to create documents and anyone else that knows the e-address of such document to sign it, all done digitally.

The system I propose is not just simple and secure, but it’s also secured from internal corruption, in this system two parties take action, the core system, which stores data, and the validation system, which provides means to avoid internal corruption; this means that even if you are inside the system (and I don’t mean a hacker but someone that works maintaining the system), and have access to the databases, it’s impossible for you to modify or corrupt any data, without forcing validation keys (and every user has a key) in the validation server, even when you can remove, the data is self-regenerative so you can’t destroy the data; also if you work in the validation server side, you have no access to the databases.

This validation system ensures that no internal corruption has happened, so both must be hold by different parties that have little to zero contact with each other.

What can be done?

1. Create documents and sign yourself as creator.
2. Delete documents (this will leave a trace).
3. Validate and sign documents in a fast an efficient way, without wasting paper and/or time.
4. Create proposals and polls with options.
5. Have a searchable database of all the documents.
6. Revoke signatures (this will leave a trace).
7. Calculate the amount of signatures and the options amount, as well as revocations.
8. Perform deep validation of any document data.
9. Secure the documents from any attempt of internal or external corruption, any attempt would be obvious and traceable; this is different from what is usually done in general security, where data can be easily corrupted once inside the system.

Note.

The solution proposed here consists of the cheapest way possible of creating a such product. More complex and expensive versions can be created using different storage technologies and different authentication ways on top of the ones described here.

How it works.

The workflow is pretty simple, from an user perspective the first time flow is:

10. Download the application, for desktop or for android, or go to the website using a modern browser.
11. Go to the key generation part (anonymously) do not accept help.
12. Press Generate Keys.
13. You'll get a pdf file with huge QRCodes, one says PRIVATE, the other PUBLIC, and a BHASH, store the private in and BHASH in a safe place, and take the PUBLIC one and go to a registration institution/entity (printed).
14. Go back to the website and upload a BHASH file, and use it to login with your id and set a password.
15. Answer some security questions that will be used for recovery.
16. Destroy the BHASH, you have successfully signed in.

After this flow you can do all the basics for your account, including recovery and change your password.

Passwords are also secured using a hashing algorithm and the hashes are never stored.

For someone that wishes to create a document they have to:

1. Login to the platform and press "create a document".
2. Write the title and description of the document.
3. Add an expiration date (optional)
4. Add a list of options to choose (optional)
5. Press create.
6. The user will get a link that will provide access to such document to other people.
7. User can keep track of the document in "My documents", and see how many people have signed and how many have revoked their signature.

For someone to sign a document they have to:

1. Login to the platform and use the link provided.
2. Sign the document pressing Sign.
3. The user can keep track of the document in "My signatures", and see how many people have signed and revoked.
4. User can revoke the signature by pressing revoke, this is one time business.

Also there are several ways to recover an account:

1. Using the recovery process and answering the security questions, you'll be prompted for a new password and new security questions.
2. Using your private key to generate another BHASH, you'll be prompted for new password as well as security questions.
3. As a last resource you'd have to contact the validation system owners and start a process to recover your account in which you must validate your identity, the process should be tedious and complicated on purpose, very similar to the first time flow as you need to generate new keys; someone that loses all recovery methods to access their account should be suspicious. Also, as an extra security method, the newly created public mark should not be usable for the next 5 days, even when it's possible to login and manage again.

Support for two way authentication could be a helpful resource for extra security that will affect solution 1; you are firstly required to input a code that will be sent to a mobile device in order to be able to introduce your password. This step should be optional and anyway increases the cost due to texting reasons.

Consider that the whole process is secured using strong cryptography, and no action can be directly falsified, every action that the user perform is signed, including signatures and revocation of the signatures, passwords are never sent to the servers, they instead decrypt a secondary key that generates signatures. That means that none, not even the person that maintains the servers, can have access to your account.

Also you can perform a strong check up on the validity of a document, which will check all the history of every person that signs to try to find inconsistencies or signs of corruption of data; this can take its time but provides secure results.

All the signatures and documents are signed by the server as well, and such data is downloaded all the time, every time you login and access your account a consistency check is made to autoregenerate data in the server to make sure that nothing is removed.