FUNDAMENTALS OF DIGITAL SIGNATURES

Establishing Trust in a Cyber World

BY TRAVIS SPANN AND THE AEGISOLVE TEAM

ÆGISOLVE

VERSION 1.0

Project Background and Description

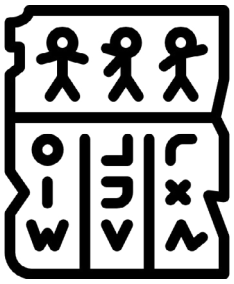
Identify and explore simplistic opportunities to leverage cryptography as the basis of trust in a cyber world.

Origin of Signatures

In the physical world signatures serve to permanently affix identity to documents. The impact of signatures to build trust and move our world cannot be understated. From the earliest discovered signature on a Sumerian clay table in 3100 BC to the first verifiable signature from a historical figure in 1098 by Spanish nobleman El Cid, signatures have evolved in lockstep with human society.

Prior to the advent of written signatures, the need to communicate trust in human society was still present. Rings, wax and rods, and, even today, handshakes were often used to convey authority and instructions. Written signatures have played a pivotal role in establishing trust between strangers, a pivotal component underlying trade and commerce. While the function of signatures has remained consistent throughout time around the world, their form has evolved time and time again.

The latest evolution of signatures came at the dawn of the information age and has generated rapid changes to our governing law, corporate practices, and technological innovation. Digital signatures have brought about a rapid transformation to many industries and processes, from home buying to professional sports. Without digital (electronic) signatures our technological world might resemble the physical world before written signatures. Needless to say, digital signatures are essential for the world we live in today.



The Earliest Autograph Signatures
Lexical lists written in ancient Sumerian pictographic script on clay tablets are the earliest literature known, and also the earliest known evidence of school and learning.

From historyofinformation.com

VERSION 1.0 | AUGUST 2018

ÆGISOLVE

But really, what are signatures?

The premise of any signature scheme (whether it be a hand written or electronic) is that there exists the ability to rely on the validity of the signature as a verifiable artifact of both intent and implementation of a stated act/objective.

Entities not involved in the act of signing must somehow be able to determine whether the signature "AND" the information (act/objective) associated with the signature are legit.

In the olden days, signatures and corresponding information were physically tangible and needed to be physically protected from tampering (e.g. trusted couriers, special containers, etc.).

Nowadays digital signatures fulfill the equivalent protections and trust establishment all at once, everywhere at once (with all sorts of caveats).

As per the FIPS 186-4 Digital Signature Standard:

> *"Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time. A digital signature algorithm is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication."*

As legend has it, Hancock made his signature so flamboyant in order for King George to read it without his spectacles. Alas, the story is apocryphal and originated years after the signing of the United States' Declaration of Independence.

Introduction to using digital signatures

For now, let us assume that the cryptographic algorithms involved here are perfect, and the matters of cryptanalysis are out of scope (a convenient way to keep this paper readable to most).

Furthermore, in the interest of simplicity let us consider three main objectives for an effective and overly simplified digital signature scheme:

> **1) Keep your private key, well, private (i.e. nobody/nothing else in the universe holds this value but you forever and ever). This way there exists trust that data is being signed by you, and only you.**
>
> **2) Ensure the person/thing relying on your signature (i.e. whomever/whatever is verifying the signature) is confident in your public key. This way there exists trust that your public key can be used to verify data that you signed.**
>
> **3) Ensure the person/thing relying on your signature is confident that you successfully achieved objective #1. This brings this simplified trust model full circle.**

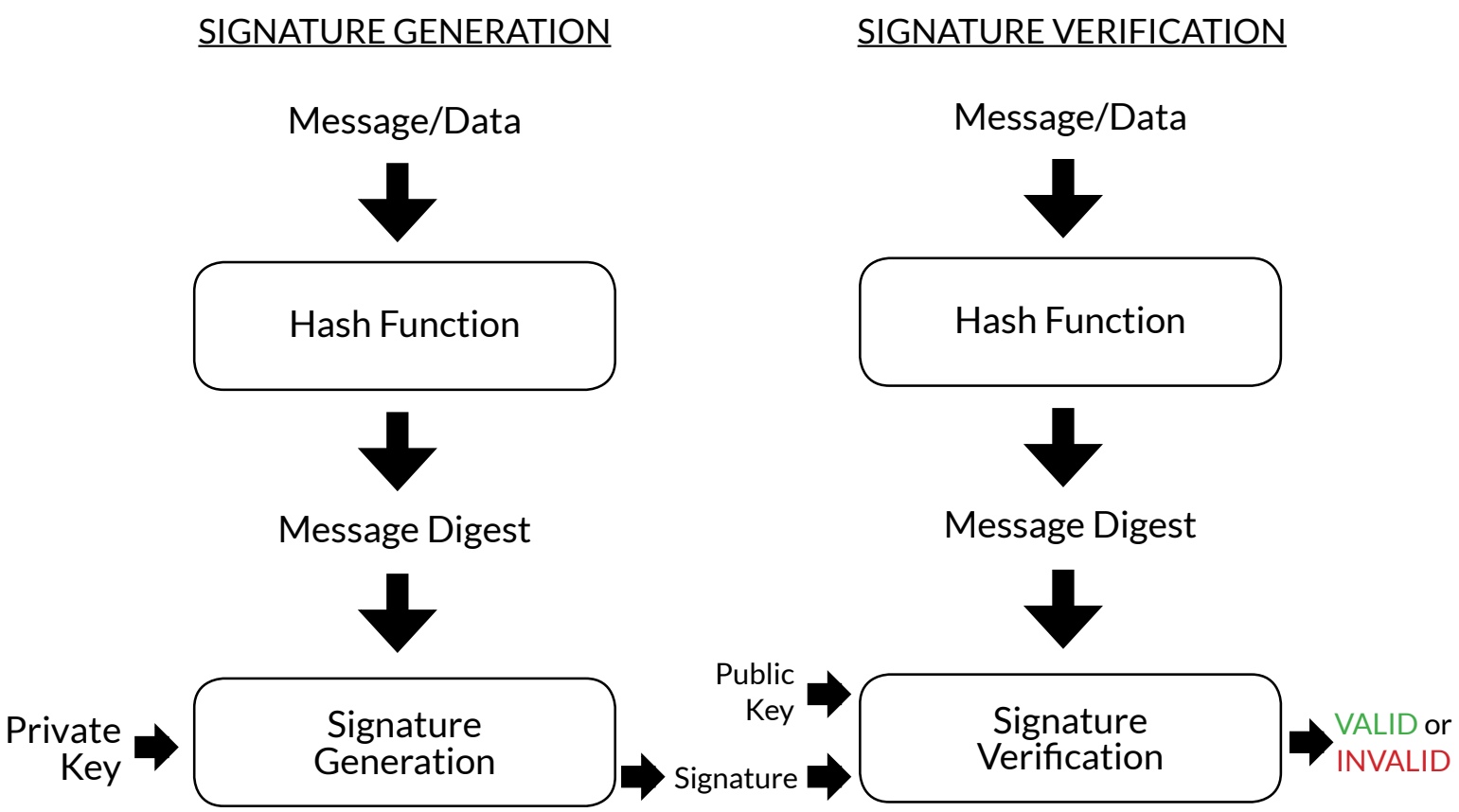
Notwithstanding many obscure and complicated topics, if the three objectives above are accomplished, at a 10,000ft view your digital signature scheme has some legs so to speak:

You as the signatory (the entity that possesses the private key), can perform a digital signature generation; a cryptographic operation that applies your private key to a hash of the data being signed (also known as a message digest) to produce a digital signature.

Another party known as the recipient, or verifier (the entity that possesses a copy of your public key), can perform a digital signature verification; a cryptographic operation that applies your public key to the signature to extract (decrypt) the hash, then recreate the hash from the original data and compare the two hashes; if the two hashes match, the signature has been verified/validated; else something went wrong and the signature is deemed as invalid and cannot be trusted.

If any tampering has occurred with the keys, data, or signatures, the signature verifications should fail and trust in the associated data/processes will not be established.

Visualizing Digital Signature Generation and Verification in the FIPS 186-4:



Assurances (...overly simplified)

So how do you know if you are really interacting with the right person/thing and vice versa when it comes to digital signature verifications? And how does everyone/everything involved know that the three simplified objectives (page 3) are being realized?

Well, at some level of abstraction the answer is: "it's really hard to know for certain". That's a bit unsettling, but there exists some amount of hope!

VERSION 1.0 | AUGUST 2018

ÆGISOLVE

Solving the riddle of objective #1

1 *Keep your private key, well, private (i.e. nobody/nothing else in the universe holds this value but you forever and ever). This way there exists trust that data is being signed by you, and only you.*

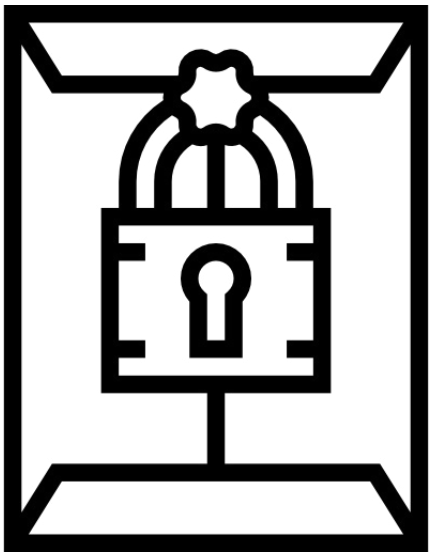
Private keys can be protected from unauthorized disclosure in a myriad of ways (such as generating and storing them inside of FIPS 140-2 validated cryptographic modules). Providing some assurance to the person/thing you are talking to that you possess your private key can be achieved in quite a lot of ways.

There are some very simple challenge/response approaches that work reasonably well. For example, the recipient (the person/thing that will eventually rely on your signatures) can challenge you with a value to sign (typically a random number known as a nonce).

Upon receiving the challenge value, you proceed to sign it with your private key and send back the signed response.

If tampering occurred on any of the data items or keys, or in some awful world if you are lying and don't really have the private key you claim to, the signature verification is going to fail.

Else, voila! You have provided some level of assurance (trust) that you indeed have your private key.



VERSION 1.0 | AUGUST 2018

ÆGISOLVE

Finding some comfort in objective #2

2 *Ensure the person/thing relying on your signature (i.e. whomever/whatever is verifying the signature) is confident in your public key. This way there exists trust that your public key can be used to verify data that you signed.*

The most common practice is to manage public keys via digital certificates (data containers with public key(s), digital signatures from trusted entities, and other unique identifiers) and a public key infrastructure (PKI) which likely includes involvement of trusted third-party certificate authorities. PKI is rather complicated, so we'll save that discussion for later.

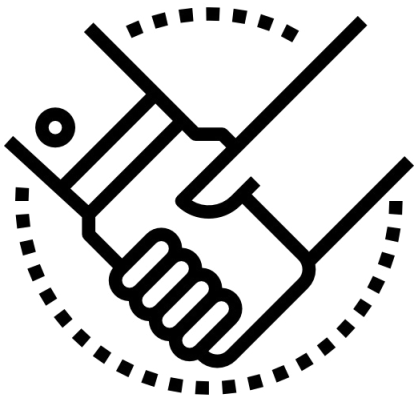
Plaintext email or other simple electronic delivery of your public key to the recipient followed up with a verbal confirmation of key contents over a trusted communications channel might do the trick.

The overly cautious types and those with lots of time on their hands might even opt for a manual inspection of public key contents as a face-to-face ceremony and in real time. With objective #2 closed, we're almost off to the races on trust binding "auto-magic".

Closing the deal (...literally) with objective #3

3 *Ensure the person/thing relying on your signature is confident that you successfully achieved objective #1. This brings this simplified trust model full circle.*

If all parties involved are satisfied with the fulfillment of objectives #1 and #2, and all parties are confident that the private key is safe (objective #3), then its deal time. Digitally sign on the dotted line, the same will be trusted, and afterwards there exists non-repudiation.



A few reasons to consider using FIPS Approved digital signature schemes:

1) Strength

Known to provide a certain computational resistance to attack. Today the minimum strength is 112-bits of equivalent encryption strength.

2) Well-documented

Associated standards, test specifications, and test vectors are publicly available.

3) Testable

Ability to determine that the algorithm has been implemented correctly.

4) Relevant

When digital signatures are implemented, FIPS Approved digital signatures are required as a prerequisite of FIPS 140-2 validation, which is mandatory for federal agencies and trusted/used by many industries worldwide.

Need FIPS 186-4 digital signature algorithm validation?
Or FIPS 140-2 validation?

Aegisolve is accredited (NVLAP Lab Code: 200802-0) and here to help.

aegisolve.com/ds-request

LinkedIn Follow ÆGISOLVE, INC. on LinkedIn.

VERSION 1.0 | AUGUST 2018

ÆGISOLVE

Validation testing and NIST CAVP approval

Here's a snapshot of how we can determine whether you have implemented the Approved digital signatures correctly (e.g. trust through independent verification):

- **Verification of implemented approved cryptographic algorithms via conformance testing and source code review.**
- **ÆGISOLVE, INC. submits a series of testing vectors to vendor.**
- **The vendor processes the testing vectors using the implemented cryptographic algorithms on the module under test, and submits the outputs back to ÆGISOLVE, INC.**
- **Upon verification of correct implementation, ÆGISOLVE, INC. submits the results to NIST CAVP to obtain algorithm validation certificates for the vendor.**

Need FIPS 186-4 digital signature algorithm validation?
Or FIPS 140-2 validation?

Aegisolve is accredited (NVLAP Lab Code: 200802-0) and here to help.

aegisolve.com/ds-request

Follow ÆGISOLVE, INC. on LinkedIn.

VERSION 1.0 | AUGUST 2018

ÆGISOLVE

Definitions from the FIPS 186-4

DIGITAL SIGNATURE

The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation.

MESSAGE DIGEST - AKA "HASH VALUE"

The result of applying a hash function to a message.

PRIVATE KEY

A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key.

PUBLIC KEY

A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm and is associated with a private key. The public key is associated with an owner and may be made public. In the case of digital signatures, the public key is used to verify a digital signature that was signed using the corresponding private key.

SIGNATORY

The entity that generates a digital signature on data using a private key.

SIGNATURE GENERATION

The process of using a digital signature algorithm and a private key to generate a digital signature on data.

SIGNATURE VERIFICATION

The process of using a digital signature algorithm and a public key to verify a digital signature on data.

REFERENCES

- *FIPS PUB 140-2 Security Requirements for Cryptographic Modules*
- *Derived Test Requirements for FIPS PUB 140-2 Security Requirements for Cryptographic Modules*
- *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program*
- *FIPS 186-4 Digital Signature Standard (DSS)*

VERSION 1.0 | AUGUST 2018

ÆGISOLVE

About AEGISOLVE

AEGISOLVE is the industry leader in providing Federal Information Processing Standards testing and validation certificates (e.g. FIPS 186-4 digital signature, FIPS 140-2 cryptographic module, etc.) for many industries including, but not limited to, cloud, IoT, automotive, banking, healthcare, critical infrastructure and digital cinema (NVLAP Lab Code: 200802-0).

AEGISOLVE.COM

(650) 386-1436

415 Fairchild Dr, Mountain View, CA 94043

Follow us on LinkedIn

VERSION 1.0 | AUGUST 2018

ÆGISOLVE