

Vincenzo MAGGIO

---

# Digital Signatures



**A Short Essay On The Masters of the Keys  
and Survival Guide versus the Codebreakers**



## Index

|                           |       |   |
|---------------------------|-------|---|
| Introduction              | ..... | 3 |
| Information Hiding        | ..... | 4 |
| Certification Authorities | ..... | 5 |
| Digital Signatures        | ..... | 6 |
| Economics and Legals      | ..... | 8 |

*"There is no security on earth; there is only opportunity" ~~ Douglas Mac Arthur*

## **I. Introduction**

Since the times of the Romans, perhaps earlier, kings and monarchs used to sign or seal a document to give it an official validity. While in other types of documents the presence of a testimony establishes trust between parties.

Never as in these times of high insecurity over the Internet, there is the need-  
ing to authenticate the signer of a document or the sender of a message. As we  
will see later, this has implications not only in the IT world, but also economic  
consequences and legal impact. Authentication is needed because any given user  
could commit a transaction from her bank to any company. So for example any  
pirate could intercept the transaction and replicate it, but addressed to his own ac-  
count, perhaps multiplying the amount by ten times.

So rose the necessity of a framework to authenticate computer based informa-  
tion, while saving its integrity. Hence the brand new field of electronic signatures,  
which can be used for any type of transaction, either individual to company, or  
company to company, and so on. Some of those are the telegraph signature and  
the faxed signature. Another subset is called Digital Signatures.

*“If you would wish another to keep your secret, first keep it yourself” ~~ Seneca*

## **II. Information Hiding**

Before going deeper we take a short tour into Cryptography. Derived from Greek κρυπτός *kryptós* "hidden" and the verb γράφω *gráfo* "write". Its primary purpose is hiding the meaning of messages, not usually the existence of such message. It contributes to information security, authentication and access control; it relates to techniques used in computer and network security as access control and information confidentiality. Cryptography is also used in many applications used in everyday life, like security of ATM cards, computer passwords and electronic commerce.

In the beginning Cryptography was related almost entirely to Encryption, the way to convert plaintext into ciphertext, as opposed to decryption, the reverse process. Both operations are referred to as cipher, a pair of algorithms. *“The details are controlled both by the algorithm and, in each instance, by a key. This is a secret parameter (known only to the communicants) for the cipher algorithm”* <sup>[1]</sup>.

So sender and recipient have the same key. This is called symmetric key and kicks in more problems, because it involves the exchange between the parties of a

key in clear text. That could be intercepted. Thus a better approach is the so-called asymmetric key cryptography.

This involves also two keys, this time they are not identical but uniquely paired, so that the text encrypted with one can be decrypted by the other and vice-versa. So Alicia encrypts a message with her private key and sends it to Bob. Bob uses Alicia's public key to decrypt the message and at the same time is sure the message comes really from Alicia. On the other side Alicia can use Bob's public key to encrypt the message before delivering it. So it works both ways, depending on the purpose, what you want to achieve: make sure a message can be read by only one person, or make sure a message comes surely from a person.

◦ ----- ◦

*“He who is not everyday conquering some fear has not learned the secret of life”*

~~ Ralph Waldo Emerson

### **III. Meet the Certification Authorities**

So, have we solved all of our problems? No way, life is even more complicated. The problem created from the previous solution is that ownership of a pair of private/public keys does not make sure that the owner is who she claims to be! Hence the needing of a trusted third party.

While in the paper world this was a notary public, to whom you need to prove your identity, after which the notary affixed his seal, in the e-world there are companies which issues digital certificates for use by other parties.

The duty of a Certification Authority (CA) is to check the applicant's credentials, showing they trust her. So other companies or individuals who trust the CA, can trust also the identity of the recipient.

CA can be commercial vendors like VeriSign, Entrust, and Digital Signatures Trust. However any trusted public institution can issue its own certificate, like government, banks, universities, or DMV.

As final comment to this paragraph, we have to consider also that all these recursive layers do not offer protection neither from the loss of a key, nor from eavesdropping, nor - in case the key is stored on a PIN protected external memory - from a keylogger installed on the PC.

◦ ----- ◦

*"We have always said that in our war with the Arabs we had a secret weapon: no alternative" ~~ Golda Meir*

#### **IV. Digital Signatures**

Unfortunately many governments use the term in the meaning of electronic

signature. “*Electronic Signature means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record*” [U.S. Electronic Signatures in Global and National Commerce Act of 2000]. Others mean it including message authentication codes, file integrity hashes and digital pen pad devices, while the most common use is cryptographically based signature assurance scheme.

As we have seen the public key is bind to a specified user, certified by an authority, and its purpose is Authentication, Integrity, Confidentiality, and Non-Repudiation.

So how are signature and cryptography related? How does it works? While the private key is crucial in establishing your identity, it is *not* your digital signature, it is used to encrypt the message (email, text-file, spreadsheet, whatever). The digital signature schema involves three algorithms: a key generation algorithm, a signing algorithm, and a verification algorithm.

Quality encryption include the DES which has been dropped after the AES came out, both are symmetric; while the most used asymmetric cryptosystems are the RSA, Rabin, Diffie-Hellman, DSS, ElGamal, Elliptic curve cryptosystems, LUC, XTR, etc. - The FIPS 186 specifies the bounds of the algorithms’ results.

Their strong point is the difficulty to factorize large numbers in prime factors.

*“It is no secret that organized crime in America takes in over \$40 billion a year. This is quite a profitable sum, especially when one considers that the Mafia spends very little for office supplies”* ~~ Woody Allen

## **V. Economic Consequences and Legal Impact**

*“Since President Bill Clinton signed the Electronic Signatures in Global and National Commerce Act (nicknamed E-Sign) into law last June [2000], electronic signatures now have the same legal status as handwritten ones”* <sup>[2]</sup>. Sounds good, doesn't it? Unfortunately, while not strictly related to digital signatures, e-frauds, identity theft, scams, phishing and the brand new *re-packaging schema* have scaring numbers:

- *“Online merchants are hit by credit card fraud at ten times the rate of their brick-and-mortar cousins”* <sup>[3]</sup>.
- *According the Federal Trade Commission, “Identity theft affects approximately 10 million Americans each year.”* <sup>[4]</sup>
- *“Between November 2004 and February 2005, the DSW Show Warehouse database was accessed by thieves who stole 1.4 million credit card numbers plus 96,000 check transactions and the names on each of those accounts from 108 stores in 25 states”* <sup>[4]</sup>

This just for example, several lists are online available like <sup>[5]</sup>.

Such examples to show the need for security.

However Digital Signatures have different legislation in different countries.

Some states or nations recognize the validity of an electronic signature, some don't. A good list of countries is present at <sup>[6]</sup>.

After this short tour in the state of e-security at the beginning of the 21st century, we can close with the words of the famous Helen Keller: "*Security is mostly superstition. It does not exist in nature*". However keys lengths of 2048 bits or more are believed to be unbreakable for decades.

## References

1. <http://en.wikipedia.org/wiki/Cryptography>
2. <http://www.itc.virginia.edu/virginia.edu/fall00/digsigs/home.html>
3. <http://www.forbes.com/2000/06/21/mu6.html>
4. <http://elamb.org/id-theft-and-finacial-fraud-on-companies-and-you/>
5. [http://outhouserag.typepad.com/online\\_credit\\_card\\_fraud/identity\\_theft\\_index.html](http://outhouserag.typepad.com/online_credit_card_fraud/identity_theft_index.html)
6. [http://en.wikipedia.org/wiki/Digital\\_signature](http://en.wikipedia.org/wiki/Digital_signature)

## Other sources consulted

RFC-3126

FIPS-186

<http://www.ssh.com/support/cryptography/algorithms/asymmetric.html>

[http://en.wikipedia.org/wiki/Electronic\\_signature](http://en.wikipedia.org/wiki/Electronic_signature)

[http://en.wikipedia.org/wiki/Certificate\\_authority](http://en.wikipedia.org/wiki/Certificate_authority)

<http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>

[http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci211953,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211953,00.html)