# Digital Signature and Multiple Signature: Different Cases for Different Purposes

Chafic Maroun Rouhana Moussa

GSEC Practical Assignment
Version 1.4b
Option 1 - Research on Topics in Information Security

July 7th, 2003

## Abstract

Like paper-based signatures, digital signatures intend to respect a number of security assumptions. Methods of digital signature apposed by a single user have been defined and are widely used. But is it sufficient? What if a legal document requires witnesses and notarization, or a contract needs the signatures of several officers?

This paper will first show the basics to understand digital signatures and how the security properties of integrity, authentication, and non-repudiation are respected. We will then present the purposes of multiple signature schemes and introduce a possible classification of cases that need multiple signatures. This paper is not intended as a presentation of a particular multiple signature scheme, but the classification presented should help researchers identify more appropriate new multiple signature schemes.

# Introduction

A few centuries ago, signature and eventually a wax seal were the only way to certify the authentication of a document. Since that time, and until today, when a signature is apposed to a treaty by a president or to the wedding license by a happy couple, it is assumed that [2]:

- The signature binds the signer to whatever the document states.
- The document will not be changed once the parties have signed it.
- A signature on one document will not be transferred fraudulently to another.

It is a challenge to make these assumptions respected by the electronic equivalent of the traditional handwritten signature: the Electronic signature, or E-signature. Today, an e-signature is *any* signature in electronic form, attached to or logically associated with an electronic record. E-signatures allow easier processing of documents, by reducing paperwork, travel, delays, and delivery costs

E-signatures are generally divided into two separate categories: digital signatures and electronic signatures. In contrast with digital signatures, electronic signatures do not rely on cryptographic methods and are often biometrics-based solutions. This paper will only cover the Digital Signatures category.

Digital signatures can be classified into two main categories: single signature and multiple signature (or multisignature). Single signature refers to the cases where only one party signs a document, while multiple signature refers to the cases where more than one party sign a single document.[1]

Methods of implementing digital signature have been developed and are widely used today. This paper will first present the basics to understand digital signatures and how the assumptions we presented in the first paragraph are respected. We will then present the needs for multiple signature schemes and introduce a possible classification of multisignatures.

# Digital Signature

The digital signature category is the most secure and most full-featured type of e-signature. It relies on public key cryptography (PKC). Different PKC schemes have been used to implement digital signature and data encryption. For example:

- The RSA (Rivest-Shamir-Adleman) scheme,

[1] In this paper, the term "digital signature" refers to *single* digital signature.

- The Digital Signature Algorithm (DSA) scheme,
- The ElGamal scheme,
- The elliptic curve digital signature algorithm (ECDSA) scheme

When using these schemes to implement digital signature, a pair of mathematically related keys is involved: A private key, and a corresponding public key. Public keys are published and can be stored in directories. Private keys must be kept secret and only known by the user, and so are usually stored on encrypted portions of a hard drive, on Smart Cards or stored on a network and delivered only after the appropriate password is entered. The algorithms used are asymmetric. This key system obeys to these mathematical properties:

- Encrypting a message with a private key, and then decrypting the result with the corresponding public key, will restore the initial message.

- Given a public key, it is not possible to find out the corresponding private key.

Today, Diffie and Hellman's signature scheme is the most standard type of crypto-based digital signature.

The next figure shows the steps followed when a single user signs a document.

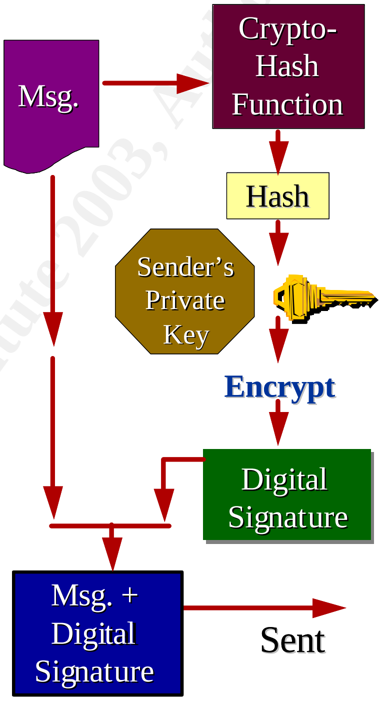

**Figure 1 A single user signing a message [3]**

The *Crypto-hash function* is a one-way algorithm that converts a sequence of characters into a shorter fixed-length value.

The next figure illustrate the steps followed by the receiver of the signed message.

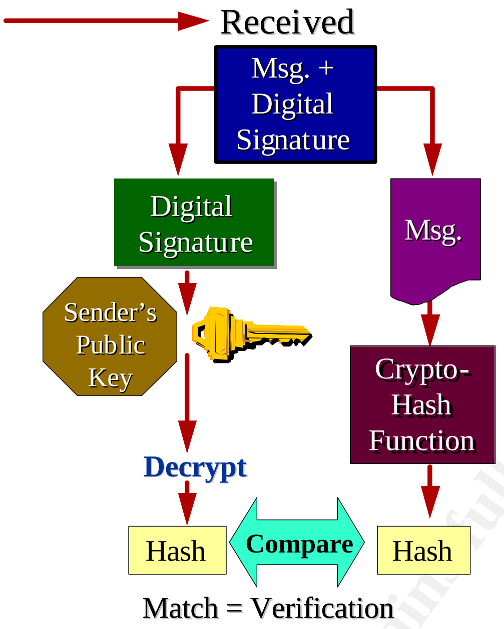

**Figure 2 Receiving a signed message [3]**

The encrypted hash that came with the message is decrypted using the sender's public key, and the result is compared with the hash generated by the receiver from the message itself. If they match, then the message can be considered as authentic. If the hashes don't match, this can be a sign of message modification, transmission error, or identity usurpation.

This digital signature scheme guarantees three information security properties:

- **Authentication**: The signer is well identified by the private/public key relation.

- **Non-repudiation**: The signing party cannot later on deny performing the action, since the private key was used for encryption process. Note that if a *symmetric key* cryptography was used, the non-repudiation properties could not be guaranteed.

- **Integrity**: Since the signature itself is associated to the content to the message, any message alteration would make the signature invalid. This also implies that the signature cannot be copied from one message and applied to another.

To guarantee the confidentiality and privacy of the communication, the entire message can be encrypted by the sender using the recipient's public key, and then decrypted by the recipient using its own private key. It is also possible to have a digital signature "time stamped" to allow the transaction to be traced in the future.

Most of today's digital signature schemes incorporate more technologies, including block cipher, public key certificates and complicated key distribution and management methods.

The Single Digital Signature category is complete, but does not aim to replace all the utilizations of traditional written signature, since in many cases, more than one person are required to sign a legal document. Therefore Digital Multiple Signatures are very important.

## Multiple signature

In everyday life, many legal documents require signatures from more than one party: contracts, decision making processes, petitions, workflow systems… The purposes and uses of multiple signatures are various.

The usage of signatures for different purposes requires different handling procedures. According to the purposes and operations of multiple signatures, K. Leung and L. Hui [1] identified some fundamental cases. This paper will present these cases. More complicated cases can be composed by these fundamental cases.

### Sequential Multiple Signature

In our everyday life, very often a decision has to be taken by different officials, and a multiple signature is required to show their authorization. Let us consider this example to illustrate the Sequential Multiple Signature: A large company wants to launch an expensive marketing campaign. The Marketing department needs the approval of both the Financial Controller and the Public Relations department. This is a "*signature on signature*" situation. That means that the first signer signs the form, and then the second signer signs on the content of the form and the first signer's signature. The form is considered signed when the last signature is appended.

Depending on the company policy, two situations can be distinguished:

#### Independent Sequential Multiple Signature

In this case, the company policy states that the order of approval by the Financial Controller and the Public Relations department has no importance. The form can be signed by either party first, and then passed on to the second party.

Since the sequence of signing is no important, the second party can sign without having to validate the previous signers: this implies that the signers only sign on the content of the form. A Multiple signature scheme that implements this case has to incorporate a validation process which will check the validity of each signature, and that all the form contexts obtained from the digital signatures are consistent.

#### Dependent Sequential Multiple Signature

In this case, the company policy is set up in a way that the order of approval is important and has to be respected: before launching the campaign, the Public

Relations department has to approve the project first. After that the Financial Controller can gives his OK.

Since the sequence of signing is important, the "signature on signature" can be easily used. This means that the last signer has to sign not only the context of the form, but also the signatures of the previous signers to form the new digital signature. Before appending its signature, a party has to validate all the previous signatures. The preceding signature is then validated by decrypting it with the public key of the previous signer. The form content and the signature of the "signer before this signer" are obtained. Afterwards the signature of this signer can be checked in a similar manner… Finally, when validating a dependent sequential multiple signature, the sequence of actors signing the form has to be checked also. The last signature guarantees the integrity, authentication and non-repudiation of "lower" signatures.

## Parallel Multiple Signature

In many cases, an approval must be signed concurrently by a number of parties. Signing a contract by 2 (or more) parties is a good example to illustrate this case. The signature of an international convention by several officials represents another example: all the signatures are "equal", and respect no hierarchy.

In a parallel multiple signature scheme, the signature of each signer is on the content of the form, and not on the signature of other signers. In order to put in place this scheme, some information will be needed, like the number of potential signers who will receive the form, the potential signers who will sign the form, and finally the number of signature required. If the form can be duplicated, a copy of the form will be distributed to each of the parties. This mechanism is called *fork*. The mechanism to collect the signatures will be called *join*. The *fork* and *join* mechanisms can be classified as follows:

### Fork

The *fork* mechanism can be divided into two types: *fork-all* and *fork-some*.

#### Fork-all

In the example we used before, the marketing department can make copies of the form and send it to both parties involved concurrently. The approval and the signature will be performed simultaneously.

#### Fork-some

If we consider the same example, but with an additional constraint: In addition to the approval of the Financial Controller and the Public Relations department, the marketing department needs the authorization of three out of six members of the Board of Directors (BoD). So in addition to sending a copy of the form to the Financial Controller and the Public Relations department, the marketing department may choose to send a copy of the form to three, four, five or six members of the BoD.

**Join**

The *join* mechanism can be also divided into two types: *join-all* and *join-some*.

**Join-all**

In this case, it is mandatory that all the signatures are present and valid. In the *fork-all* example, the marketing department is required to collect the signed copies from both the Financial Controller and the Public Relations department. Both signatures have to be valid.

**Join-some**

In this case, we don't have to wait for all the signatures, but only those who are obligatory and those that satisfy the additional conditions. If we consider the *fork-some* example, the marketing department can launch its campaign as soon as the signatures of the Financial Controller, the Public Relations department, and three out of six members of the Board of Directors are collected.

In a parallel multiple signature scheme, all the signatures have to be validated, one by one, and for each form.

### Anonymous Signature

Another type of signature used in some business areas can be considered as anonymous signature: it is a type of multiple signature, where copies of the forms to be signed are sent to several actors. Special arrangements have to be made in order to cover the identity of the signers. The anonymous signature scheme has to include methods that make sure that the signatures are made by valid actors.

### Multiple Signature Schemes Examples

Many Multiple Signature schemes have been studied and presented, and are applied to one or many of the cases presented in the previous paragraphs. Here are some remarkable examples, proposed for a multipurpose use of the digital multiple signature:

- Colin Boyd introduced an interesting RSA variation for digital "multisignature" in 1989 [4]. The private key d is split into multiple co-prime portions $d_1$, $d_2$, .. $d_k$. The $i^{th}$ portion $d_i$ is given to the $i^{th}$ user. The user can then jointly sign a message.

- Shieh, Lin, Yang and Sun developed a Digital Multisignature Scheme for Authentication Delegates in Mobile Code Systems. This scheme includes a parallel multisignature scheme, and a sequential multisignature scheme. [6]

- Mitomi and Miyaji introduced a very flexible multiple signature scheme [7]

## Conclusion

This paper developed the importance of digital signatures: single and multiple. Although digital signatures schemes that provide many security properties (non-repudiation, authentication, integrity) have been implemented successfully by public key cryptography, those schemes are not sufficient to satisfy different purposes of the traditional signatures, especially multiple signatures. This paper presented a classification of different administrative purposes of multiple signatures. Proposing a multiple signature scheme is always a challenge, principally because of the multitude of cases it has to respect, like hierarchy, number of signers, etc…

## References

[1] Leung, Karl R.P.H.; Hui, Lucas C.K. "Multiple Signature Handling in Workflow Systems". 2000. URL: http://www.computer.org/proceedings/hicss/0493/04936/04936033.pdf (July 7, 2003)

[2] Noakes-Fry, Kristen. "Digital Signatures: Perspective". August 10, 2000. URL: http://www.securitytechnet.com/resource/rsc-center/gartner/digitalsigs.pdf (July 7, 2003)

[3] Wheatman, Victor S. ; Noakes-Fry, Kristen. "Digital and Electronic Signatures: A Quick Look". May 16, 2003. URL: http://www4.gartner.com/2_events/audioconferences/attachments/sd_16may03.ppt (July 7, 2003)

[4] Boyd, Colin. "Digital Signatures". Cryptography and Coding. H.J.Beker and F.C. Piper Eds., Oxford University Press, 1989, pp241-246. URL: http://sky.fit.qut.edu.au/~boydc/papers/ima89.pdf (July 7, 2003)

[5] Wells, Thomas O. "Electronic and Digital Signatures: In Search of a Standard". IT Pro IEEE, June 2000, pp24-30.

[6] Shieh, Shiuh-Pying; Lin, Chern-Tang; Yang, Wei-Bon; Sun, Hung-Min. "Digital Multisignature Schemes for Authenticating Delegates in Mobile Code Systems". July 2000. URL: http://dsns.csie.nctu.edu.tw/ssp/docs/Digital multisignature schemes for authenticating delegates in mobile code systems.pdf (July 7, 2003)

[7] Mitomi, Shirow; MIYAJI, Atsuko. "A General Model of Multisignature Schemes with Message Flexibility, Order Flexibility, and Order Verifiability". October 10 2001. URL: http://grampus.jaist.ac.jp:8080/miyaji-lab/member/PaperPS/IEICE01-sita.pdf (July 7, 2003)

[8] Information and Privacy Commissioner/Ontario. "E-mail Encryption Made Simple". August 1999. URL: http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=11401&U_ID=0 (July 7, 2003)

[9] Frausto Bernal, Paul. "Controlling digital multisignature with attribute certificate". 2002. URL: http://www.acsac.org/2002/case/wed-c-130-Bernal.pdf (July 7, 2003)

[10] Rubin, Frank. "A Multiple Signature Protocol for Public-key Cryptosystems". August 6,1997. URL: http://www.contestcen.com/crypt004.htm (July 7, 2003)

[11] Hardjono, Thomas; Zheng, Yulliang. "A Practical Multisignature Scheme Based on Discrete Logarithms". 1993. URL: http://citeseer.nj.nec.com/hardjono93practical.html (July 7, 2003)