International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

# Proposal for a Way to Counter the Falsification of e-Mails Exchanged using the Outlook E-Mail Client

**Assistant Bertin Lobo Minga**

**Abstract:** ***The purpose of this article is to provide a way to ensure the integrity of e-mail exchanged using the Microsoft Outlook e-mail client. The information exchanged by e-mail, from one correspondent to another in a professional environment or not, is very sensitive to the point that it is necessary to ensure their integrity. Nowadays, one of the most used email clients in the professional world is Outlook which is a product of the Microsoft business. It is technically proven that any message already sent or received using the previously mentioned e-mail client, that is Outlook, can be falsified by both its sender and its recipient. The solution proposed in this article is the use of electronic signatures using digital documents called certificates, obtained through a certification authority. The experimentation of said solution is simulated by means of the virtual machines by considering an illustration made on the basis of the exchanges made between two fictitious users created for demonstration purposes.***

**Keywords:** certificate, cryptography, public key, signature, mail, Outlook

## 1. Introduction

The need to communicate is natural and its appearance is as old as that of man. Since his existence on earth, man seeks to exchange information with his fellow men. He does it in many ways and uses the means that are within his reach. Some of its ways are faster and some others are not.

For ZARIFIAN, "to communicate is to talk about something". To talk to each other is also to exchange messages by email, from discussion forums, on social networks. Talking to each other is expressed through the use of words, gestures, facial expressions. Communication has two major characteristics that are the reciprocity and the understanding of others in what they say and what they are (their culture, their reactions, their opinions ...).

Information facilitates collaborative work and the creation of collective intelligence. Therefore, it is necessary to exchange and share this information. The main vector of this sharing is communication. Relationships and communication have become the core values of work. But this requires defining communication rules and organizing the sharing of information to acquire collective knowledge. (SAUVAJOL-RIALLAND, 2013)

Since information only makes sense when it reaches its recipient with integrity at the right time, people are always looking for faster and more secure means of communication.

In the past, he could use very basic means of communication, but nowadays he uses very advanced techniques, taking full advantage of the evolution of technology.

At the same time he is in search of faster means, man does not tire of making efforts to improve the security of his trade. Thus for several years, certain great personalities, like Julius Caesar in the field of the army, used certain techniques to make more secret the messages that they could transmit to their troops.

With the evolution of technology, one of the most used ways to exchange information is email. The latter is very fast if it is compared to the means used in the past and remains one of the most used means of communication in business today.

No user may want a message that has been falsified by the recipient to continue to be considered as having come from him. Nobody will want to hold a message whose authenticity is disputed by its issuer.

Our major concern can be summed up in this question: what solution to put in place to validate the identity of the issuer and thus fight against any falsification during the exchanges of emails made using the Outlook email client?

The solution we are proposing is the use of electronic signatures using digital documents called certificates obtained through a certification authority. We propose to use a kind of signature that is only present on the document as long as its integrity is verified and disappears as soon as a lesser change is made.

According to the Robert Dictionary, the signature is "an inscription that a person makes of his name (in a particular and constant form) to affirm the exactitude, the sincerity of a writing or to assume the responsibility for it. ". According to C. Devys: the signature is "any sign intimately linked to an act to identify and authenticate the author of this act and reflecting an unequivocal desire to consent to this act. (DEVYS, 1995). It can also be defined as "the sign by which the signatory asserts himself as the author of what he signs, an intentional personal mark that manifests his identity and concentrates on his head the effects attached to his initiative ". (CORNU, 2007)

## 2. Methodology

In order to propose a solution to the problem related to the falsification of messages, we will proceed as follows: first, illustrate the problem to be solved by means of a simulation made on the basis of two fictitious users using virtual machines created with VMware software. Then we will install and configure a mail server and two Outlook mail clients. Finally, a certificate authority will be installed and the certificates will be distributed to both users, and their application to email clients.

The problem we want to solve is so simple. It is linked to the validation of the emitter of a message exchanged via e-mails via Outlook in order to guarantee the integrity of these messages.

This problem arises less and less for modern web browsers by the simple fact that the latter integrate natively a list of certificates from different certification authorities chosen according to the rules well defined by their developers.

To understand the real problem, we use a scenario illustrated on the basis of exchanges made between two fictitious users created for the purpose of illustration: user A and user B.

When a user A writes an e-mail to a user B, he mentions the addressee's details. Some information is mandatory and some others are not. It is good practice not to leave empty fields such as the object and to sign the message. The signature on an electronic document has the same value as the signature on a paper document: validate the issuer of the document.

If the user A signs a mail, it shows the user B that this message really comes from him. The signature makes sense if the integrity of the mail or its attachments has not been affected.

What will happen if the message sent undergoes changes or falsifications in User B's box when it was signed by User A? The answer to this question is so simple: the content of the message sent should not, in principle, engage the user A. This message should no longer be considered as coming from the user A, even if the modification had not touched only one character.

And if B does not admit to having falsified the message transmitted to him by A? A can not use the version of the message in the section of his messages sent to prove that the message that B has is not the one he actually sent. If it is true that A is not an author, who else could then be the signature and the address present in the falsified mail are those of A?

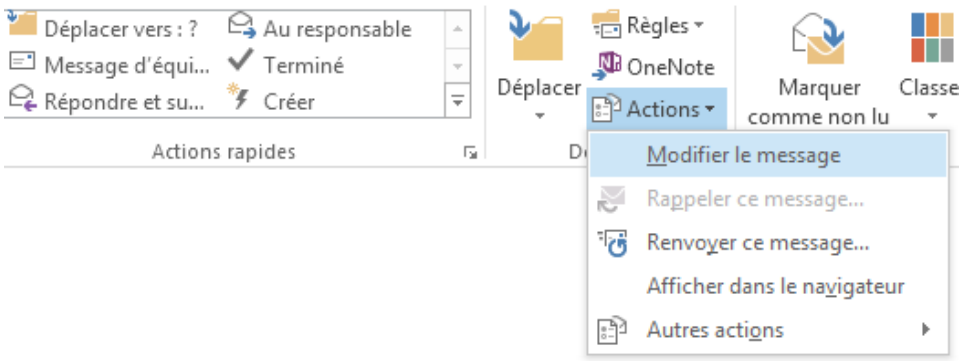
And in addition, this defense is still not valid insofar as a sent message can undergo changes by the sending user after sending. The nuisance can come from two sides.

On the one hand, user A may, for example, be a manager who can write a letter asking his subordinate B to disburse an amount of a certain value X. B may take advantage to disburse a higher amount and to falsify the message of A while keeping the identity of A and even his signature, and subsequently transfer the falsified mail to a witness C.

On the other hand, user A can write a mail asking his subordinate B to disburse an amount of a certain value X and modify the message sent by replacing X with X -1 and transfer the message sent to a witness C while keeping the identity of A attached to the mail sent and falsified. Who can be blamed for this situation? Lack of appropriate infrastructure to ensure the authenticity, integrity and non-repudiation of electronic exchanges.

The danger as presented in this scenario is the one that runs Outlook to several of its users, if a more effective solution is not envisaged in order to secure the exchanges of emails.

Here is a screenshot showing how to edit a message in Outlook:




Here is the dialog inviting the user who modified the body of a message to validate the modification


## 3. Results

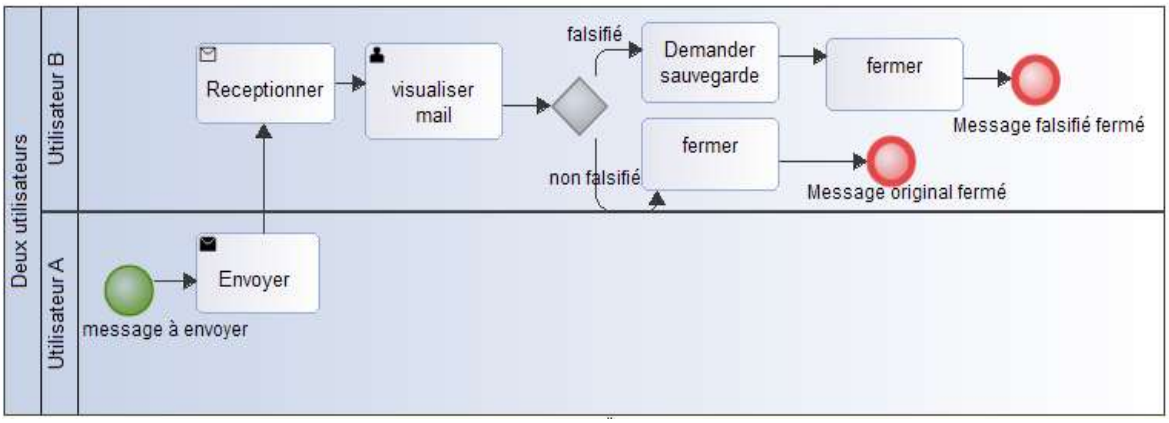
As stated in the introduction, the proposed solution is that of the use of the signing of messages by means of digital certificates, obtained through the establishment of a certification authority that is a trusted entity to authenticate the identity of the correspondents.

Each user with an electronic mailbox within the company must also have a certificate that will allow him to validate all the mail he will be the issuer. In this way, if one of his messages undergoes any falsification, his signature will automatically disappear from the message sent and the latter can no longer engage him.

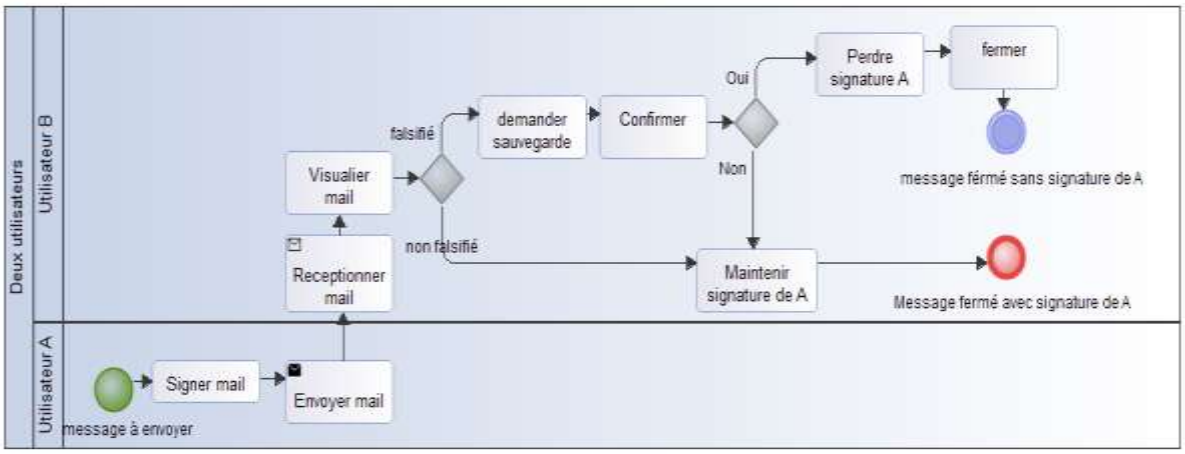
Any attempt to falsify a message will automatically trigger an alert message for the purpose of deterrence. Any message whose signature will be recognized as that of a user can never be challenged by the latter.

We have schematized the results of tests in two stages: before the implementation of the solution and after the implementation of the solution. All screenshots related to the different steps are presented in the appendices.

Situation before signature by certificates:



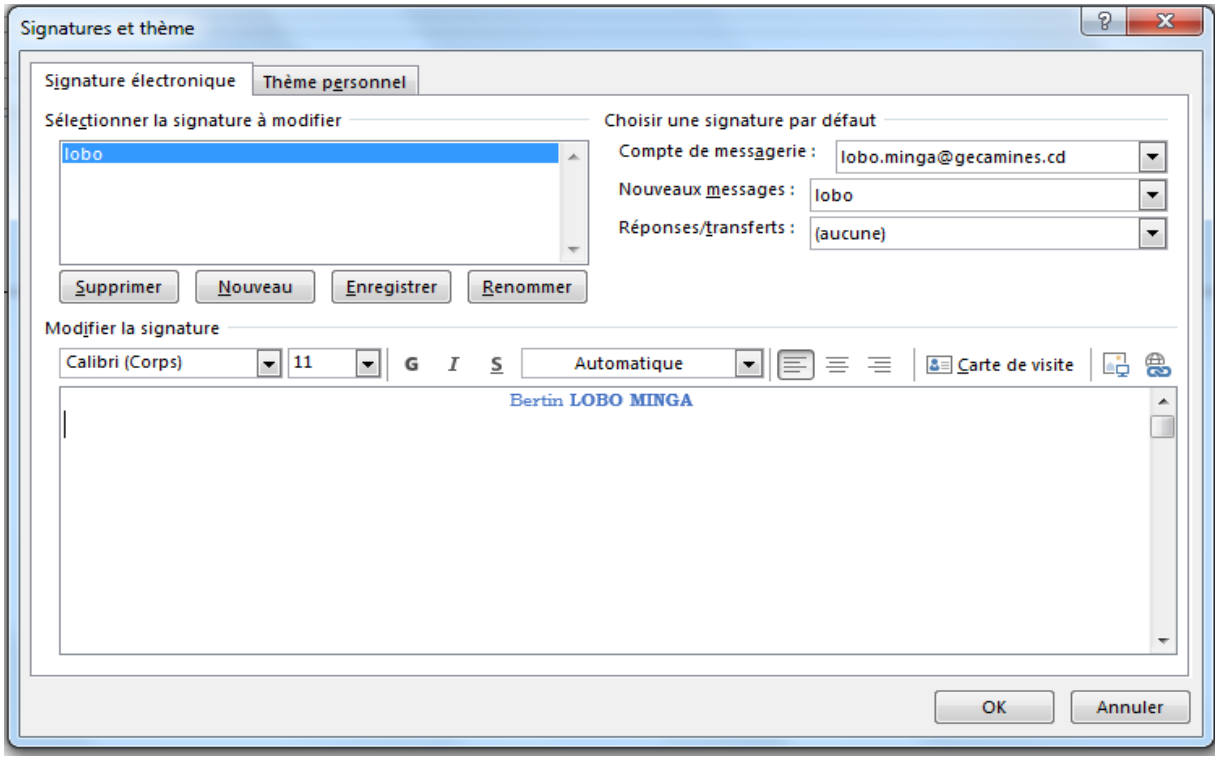

Situation after signature by certificates:




In the case of attachments that undergo changes to the destination (with, for example, more advanced techniques), the reaction remains the same, the signature attached to the attached document will be invalidated at the slightest modification of the document. When the document is signed by means of a certificate, it is possible to display the valid signature associated with it.

## 4. Discussions

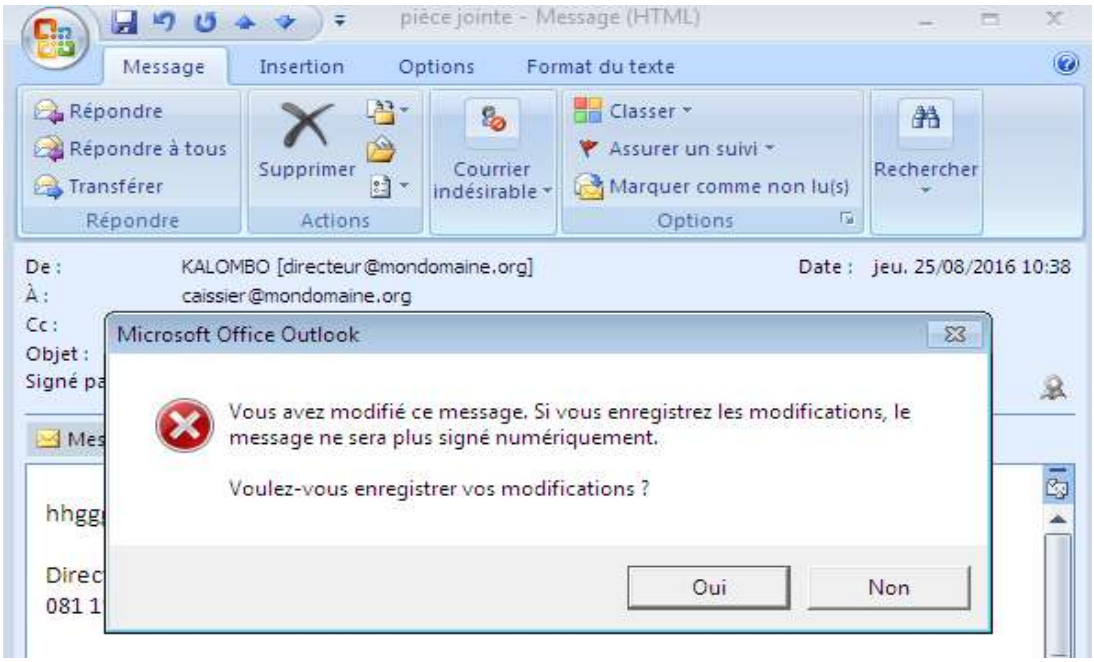
Following the problem, it should be noted that a multiplicity of solutions exist among which, that of the use of electronic signatures such as can be set directly in the mail client, for any sending messages. For the case of the Outlook client, it is possible to set a signature for any sending of messages as follows:




This solution is good and automatically adds additional information to identify the sender of the message as much as possible.

However, this solution is violable in that the email can be modified while keeping the signature of the issuer and obviously his email address. Hence, the need to resort to another type of signature, the one with the digital certificate.

Attempt to falsify a message signed by a digital certificate:




## 5. Conclusion

The main objective of this article was to propose a solution to guarantee the integrity of e-mails exchanged thanks to Microsoft Outlook e-mail client.

The choice on this email client was motivated by the fact that it is one of the most used email clients in the professional world. The presentation of the existing situation was based on a simulation performed using software tools such as VMware, Packet Tracer, Windows Server 2003, Microsoft Outlook, Modelio.

After modeling and experimenting on virtual machines, it was found on the basis of a test scenario that the ideal solution is that of the use of electronic signatures using

digital documents called certificates obtained through a certification authority.

## References

[1] C. DEVYS, *Du sceau numérique à la signature numérique, Rapp. OJTI, nov.1995, pub.in* OJTI, ssdir. C. -DHENIN, *Vers une administration sans papiers*, Paris, La documentation française, 1996, p. 96
[2] G. CORNU, Vocabulaire juridique, Coll. PUF, éd. avr. 2007, Paris, p. 866
[3] SAUVAJOL-RIALLAND C., 2013, *Comprendre et maitriser la défense d'informations*, 1ère édition, Paris : Vuibert, 206 p.
[4] ZARIFIAN P., « La communication dans le travail », Communication et organisation [en ligne], 38 [visité le 14-06-2014]. Disponible sur Internet : http://*communicationorganisation.revues.org/1462*