LEGAL REQUIREMENTS FACING NEW SIGNATURE TECHNOLOGY

Mireille Antoine Jean-François Brakeland
Marc Eloy Yves Poullet

Centre de Recherches Informatique et Droit (C.R.I.D.)
Namur, Belgium

Abstract

The recognition of electronic signature and electronic message creates many legal problems in its application in the different law systems (ex: Automatic Teller Machines, Odette, ...).

The electronic signature could be declared inadmissible before the Courts; even if declared admissible, the parties will still have to demonstrate its evidence value before a judge, not aware of the technique and who therefore will be suspicious. In fact, the electronic signature, even if so far ignored by the lawmaker, offers a guarantee of quality and certitude unrivalled by the manuscript signature.

Nevertheless, if legal texts are unsuited to reality, a simple concealment of these texts is not an adequate answer to the problems faced. Therefore some legal modifications must be done.

Jurists are aware of this necessity: International Institutions both public and private are now fighting to encourage the recognition of standard norms in specific areas (customs, banks, ...).

What are the legal requirements related to the definition of the traditional signature ? How can the definition of an electronic signature fulfill these legal requirements ? From the legal point of view, which lessons could be drawn from the comparison between the two types of signature ? What is the technical impact of the norms proposed by International Institutions (UNCID) about ETD (Electronic Transfer of Data) ? These are some of the questions which will be dealt within the context of this paper.

I. INTRODUCTION

It is a common assertion that law has always some delay with respect to reality. In regards to the electronic signature, it is our duty to confess the truth of this assertion.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 273-287, 1990.

Nevertheless, the lawyer is able to develop *appropriate* regulations, when he has understood the techniques. Such a regulation will not strain the technical developments but impose the committment to use secure technical means according to the evolving level of technical knowledge.

The paper presented here is a collective work made by a computer scientist and lawyers of the research center for computer and law of Namur.

In a first step, we will make a comparison between traditional and electronic signature. In a second step, we propose to make a short analysis of the recent UNCID-rules which can be considered as an international standard for EDI transactions. And finally, we will pay a particular attention on the way the signature and encryption techniques could be used regarding these UNCID-rules.

II. COMPARISON BETWEEN TRADITIONAL AND ELECTRONIC SIGNATURE

1. Traditional Signature

1.1. Functions

Although there is no universal legal definition of the signature, jurists nevertheless recognize that it fulfills a double function[1]. First, in the identification of the signatory and, second, in the expression of a will to accept the content of the document.

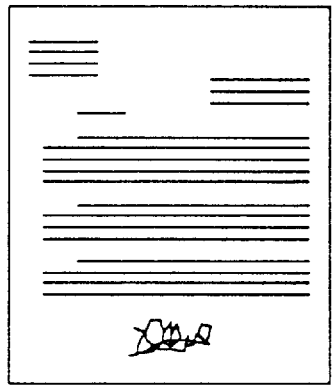
Identification of the signatory: The signature, the very "personal and unique trademark" of a person, when appended to a document, can determine the author of the act, as well as his physical presence.

Expression of will: By signing the document, the signatory Party expresses his will to become an integral part of the legal consequences it implies.

1.2. Form

The signature must achieve the same end in all legal regimes, but the actual physical requirements for it to fulfill these ends (the form), may change from one

[1] M. Van Quickenborne,"Quelques réflexions sur la signature des actes sous seing privé", note sous Cass. 28 juin 1982, *R.C.J.B.*, 1985, 68-69.



legal system to the other. For example, in common law countries, the signature must be physically and immediately readable.

2. Electronic Signature

2.1. Functions

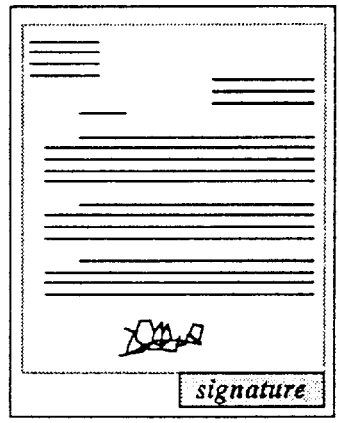
The electronic signature is an irreproducible "mark" (as a series of characters) appended to a document. It is the output of a complex algorithm of which the input data can be grouped in three different classes of variables: 1) secret data peculiar to the sender, 2) data known by both the sender and the addressee; and 3) data related to the content of the document itself. In these conditions, the electronic signature will allow:

- to identify the sender of the document;
- to authenticate the content of the document (which means that one could verify if the document had been modified).

2.2. Form

An electronic signature is a short series of characters pasted at the end of a document.

With respect to the requirements of Civil Law systems, it is obvious that the regulatory requests in regards to the form of the signature are not met in all encryption techniques so far. Firstly in certain cases, the electronic signature is readable in a first step by the machine and not directly by the receiver and secondly, in other cases electronic signatures are not readable at all.



In many Civil Law countries, another requirement can be considered as an argument against the recognizance of a legal value of the electronic signature. According to certain courts (the Belgian Supreme Court for example), the signature must express the personality of the sender[2]. This requirement is met by certain techniques of authentication like electronic recognition of physical characteristics (iris, blood, face, ... which present the advantage of identifying the person and not only the holder of the access device) but not by electronic signature.

Certain regulations (like Luxembourg regulation in 1986[3]) have been expressly modified in order to accept the new authentication procedures, like electronic signature. Luxembourg regulation defines the signature as all the means for identifying the sender of a message including secret code. The problem of the regulatory form of the signature can be viewed definitively as the major difficulty for receiving electronic signature as admissible before the courts.

3. Comparing the Traditional Signature With the Electronic One

The introduction of a new identification technique, the electronic signature, will force the business world to adapt to it. So before major changes are forced upon, one has to make sure that the traditional and the electronic signature can fulfill the same functions. A comparison analysis of the different functions will help us to check this.

[2]Cass. 7 janvier 1955, *Ann. not.*, 1955, 307.

[3]Loi du 22 décembre 1986 sur la preuve des actes juridiques, *Journal Officiel du Grand-Duché de Luxembourg*, 30 décembre 1986, 2745.

3.1. Comparative schema

functions	traditional signature	electronic signature
Parties Identification *– sender* *– receiver*	 yes no	 yes no (yes)
Content of the document	no	yes
Will to agree to the content of the document	yes	yes

3.2. Explanation of the schema

a. Identification of the parties

Identification of the sender: The "manual signature" is the traditional authentication form of a document. Therefore, it is possible to recognize the person who wanted to agree with the content. However, the security of the signature is not absolute: a manual signature may fluctuate with some circumstances; it may also be imitated $_{\text{etc.}}$

As far as the security factor is involved, the electronic signature is far more reliable, and this for two reasons: On one side, the automated signature is systematically checked and, on the other side, it is intimately related to the content of the document.

Identification of the receiver: Moreover, the electronic signature could be done in a such way that it is also related not only to the information about the sender and the content, but also to some data on the receiver. In that case the signature would also identify the person it is sent to. Something which obviously is impossible to attain with traditional signature.

b. Will to agree with the content of the document

An identification technique should show the approval of the signatory to the content of the document. But this can only be assured of if one meets a specific condition:
The signature must be a distinct operation from the writing of the text itself[4]. The electronic signature must be initiated through a different process; most likely by the person (or legal representative of this person) whose signature it should

[4]M. Van Quickenborne, *op. cit.*, 80.

represent. Therefore, the electronic signature, just as the traditional one, would require the physical presence of a human being, but instead of the person having to be there during the actual signature, the electronic signature could be just initiated by the person.

This will transpire in the fact that the electronic signature will be physically separated from the corpus of the text, showing at the end of the page.

c. Content of the document

The signature shows that a particular person has actually agreed with the content of the document. This can only be the case if the document has not been modified, by error or by fraud, after its signature. The electronic signature will allow, in addition to the traditional functions of the manual signature, to assure this authentication function. This is made possible because of the definition of the electronic signature according to the content of the signed document. The coded digital signature is therefore the best feasible guarantee one can get against modifications to the text.

d. Towards New Norms

Even if the electronic signature fulfills the different functions of the manual signature and gives us a much better reliability and security degree than the traditional signature, its recognition requires an adaptation by the legal system, regarding the problem of form requirements.

Up to now, as long as there is no case law on it, it is very difficult to predict whether a court would give probative value in the event of a dispute to the most recent techniques of authentication. However, with regard to predicting the legal value of the most recent means of authentication, it is useful to know the degree of reliability, courts have granted to older techniques of authentication, that is to say, those used for the conclusion of agreement by telex. Two opposite decisions can be quoted thereabout: the first one is Italian, the second one, German.

- In Italy, with regard to the telex contract, the District Court of Ascoli Piceno held that it is possible to show that a telex sent by a teleprinter is, in fact, written by the sender himself to an addressee. But, this is a presumption that could be broken by different means[5].

[5]Soc. Socona v. Soc. Sioler-Tronto, District Court of Ascoli Piceno, September 7, 1980, (1982) E.E.C., 317, cited by B. Amory and M. Schauss, "La formation de contrats par des moyens

- In Germany, on the other hand, an expert said before a Court that the identification of the sending and the addressee teleprinter doesn't prove that the person who sent the message is the genuine[6].

It is obvious that these previous case law regarding an older and not so secure technique of authentication allows to envisage that more secure means of authentication like electronic signature will be considered by most of the courts as admissible but saying that, at our opinion the debate is not closed.

Indeed two legal solutions could resolve the problem of admissibility. First, one could abolish all legal evidence requirements, and, therefore give way to free evidence techniques. This, in fact, would be in our opinion a false solution. First, the business world would be in a favourable position compared to the private person, and second, the judge would have to weight the value of the evidence without having any fixed or legal criteria, allowing a dangerous discretion.

A better solution would be to assess and determine a priori, certain characteristics of an electronic signature that would have the same value as the traditional one. This second solution was recommended by the Council of Europe in 1981. Therefore, if a document was electronically signed according to the rule, the judge would have no option but to accept the document as a "prima facie proof". He will take it into account in his overall weighing of the evidence, as the case would be for a traditionally signed document insofar it remains possible for the plaintiff to prove that the signed document is false and criminal sanctions exist in these cases.

No rules have as yet been developed to establish the evidence value of an electronically signed document, but we can rely in part on some standards for the credibility for Electronic Data Interchange (EDI) that were adopted by International Organizations. We will study here the International Chamber of Commerce (ICC) rules known as UNCID rules, Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission.

électroniques", *Dr. de l'informatique*, nr. 4, 1987, 211.

[6]OLG Karlsruhe, 12 juin 1973, *Neue Juristische Wochenschrift*, 1973, Heft 36, 1011. cited by B. Amory and M. Schauss, op. cit., 211.

III. THE UNCID-RULES

1. Background of the UNCID-rules

The UNCID-rules must be understood in the framework of international trade, where security plays such an important role[7].

They were drafted by a special Joint Committee of the International Chamber of Commerce (a non-governmental organisation), composed of members of the United Nations Commission on International Trade Law (UNCITRAL), the Customs Co-operation Council, the OECD, the EEC commission and the International Organisation for Standardisation (ISO), ...

The UNCID-rules don't deal with the problem of legal acceptance, they don't affect the law on admissibility[8]. If a written document is required by law, the UNCID-rules are powerless.

Instead, the rules are to provide a model contract for users of EDI, a foundation on which one can build a "communication agreement". The form and details of these agreements will differ according to the size and type of user groups: for example, UNCID-rules were used for ODETTE (Organisation for Data Exchange through Teletransmission in Europe) and DISH (Data Interchange for Shipping: group of exporters, freight forwarders and shipping lines who took part in an EDI pilot project).

However, UNCID-rules are more than a mere starting point: they also define an accepted level of professional behaviour, a "code of good conduct"[9]. By defining some *technical* requirements for EDI, the UNCID-rules will thus increase the security of this form of communications, and therefore the credibility of an "electronic document" in the eyes of a judge.

2. Principles of the UNCID-rules

According to the introductory note written by the ICC[10], the Joint Committee based its work on five basic principles. The rules should:

---

[7]B. Wheble, "Think data, not documents", *International Financial Law Review*, June 1988, 37.

[8]In opposition to the Recommendation R20 of the Council of Europe.

[9]B. Wheble, *op. cit.*, 38.

[10]ICC Publication Nr. 452.

1. aim at facilitating the use of EDI through the establishment of an agreed code of conduct between parties engaged in such electronic interchange;
2. apply only to the interchange of data and not to the substance of trade data messages transmitted;
3. incorporate the use of ISO and other internationally accepted standards - to avoid confusion;
4. deal with questions of security, verification and confirmation, authentication of communicating parties, logging and storage of data;
5. establish a focal point for interpretation that might enhance a harmonized international understanding and therefore use of the Code.

3. Analysis of the Rules

Most articles deal with *authentication*. Authentication in the sense that the data content is correct and complete, and authentication in the sense that the correct authorised person has issued the message. We will come back on this problem in the last part of this report.

Article 7 concerns the *acknowledgement* of a transfer. In the UNCID-rules, this acknowledgment is not mandatory: the sender has to ask for it, through a clause in the "communication agreement".

Following this, article 8 settles that the sender of a transfer may request the recipient to *confirm* the content of one or more identified messages in the transfer, if it appears to be correct in substance.

The UNCID-rules seem to be a compromise on those two points, as acknowledgment and confirmation are not compulsory. It seems obvious that UNCID would provide greater protection from fraud if a system of automatic call-back was a standard feature of EDI. But a particular agreement, based on the UNCID-rules, may of course stipulate the contrary for all or part of the messages and according to the costs of the acknowledgement and confirmation procedures[11]. One can imagine that for certain messages (for example financial transactions of high amount) the judge will in the next future consider that notwithstanding supplementary costs these acknowledgement and confirmation are mandatory.

Finally, article 10 deals with the *storage* of data. Each party must ensure that a complete trade data log is maintained of all transfers as they were sent and

[11]G. Rowbotham, "EDI: The practitioner's view", *International Financial Law Review*, August 1988, 33.

received, without any modification. The trade data log must be stored according to the UNCID rules for the period of time required by national law in the country of the party maintaining such trade data (we denote that in certain countries, the trade data must be maintained up to 30 years !). The log has to be kept on a computer but must be readable; there also must be a person who can certify that the log and any reproduction from it are correct. (This last condition seems to come from American and English evidence law which require that the electronic documents have to be presented before the courts by the person responsible for the computer system. This person explains the procedures for detection and correction of errors and gives evidence on the reliability of the system).

Those technical conditions are thus deemed to increase the evidence value, the credibility that can be attached to an EDI message as a form of binding communication between sender and recipient, by dramatically diminishing the risk of error and increasing the possibility of verification[12].

But the UNCID-rules are not intended to be — and could not be — exhaustive. The introductory note of the ICC suggests that one should refer to a number of elements in addition to UNCID-rules when formulating a specific agreement. Most elements concern liability problems, but two of them are related to evidence:

- **Question 7)** should there be rules on encryption or other security measures?
- **Question 8)** should there be rules on "signature" ?

4. Electronic Signature, Encryption and UNCID rules

Precisely, in answer to the question: "Should there be rules on encryption or other security measures and should there be rules on electronic signatures", we will analyze hereafter how electronic signature and encryption techniques could not only be used regarding the UNCID rules but also how they can ensure the implementation of these rules.

We will analyse the following functions:

- Electronic signature and Identification of the signatory (classical function of signature)
- Electronic signature and Verification of the inalterability of a document (additional function given to the signature by new technical means)
- Encryption and Security of the transfer.

[12]F. Schwank and W. Mitchell, "Data and the documentary credit.", *International Financial Law Review*, August 1988. 35.

4.1. SIGNATURE as identification of the signatory

One of the functions of the electronic signature permits the identification of the signatory.

Let's see how the UNCID rules have tackled with this. The following rules deal with the subject:

6.a) *A trade data message may relate to one or more trade transactions and should contain the appropriate identifier for each transaction and means of verifying that the message is complete and correct according to the TDI-AP concerned.*

6.b) *A transfer should identify the sender and the recipient: it should include means of verifying, either through the technique used in the transfer itself or by some other manner provided by the TDI-AP concerned, the formal completeness and authenticity of the transfer.*

The UNCID rules recommend the identification of the participants to the transfer (the sender and the recipient) and also the identification of messages and transactions. The electronic signature and other classical techniques of numeration and sequentialization of messages permit such an identification.

4.2. SIGNATURE as inalterability (integrity) of a document

Another function of the electronic signature allows the control of inalterability of the content of a message. In fact, we must say that the electronic signature only detects the fraudulent or erroneous modifications, but it doesn't prevent from any risks. The following rules deal with the subject:

5.a) *Parties applying a TDI-AP should ensure that their transfers are correct and complete in form, and secure, according to the TDI-AP concerned and should take care to ensure their capability to receive such transfers.*

5.b) *Intermediaries in transfers should be instructed to ensure that there is no unauthorized change in transfers required to be retransmitted and that the data content of such transfers is not disclosed to any unauthorized person.*

6.a) *A trade data message may relate to one or more trade transactions and should contain the appropriate identifier for each transaction and means of verifying that the message is complete and correct according to the TDI-AP concerned.*

6.b) *A transfer should identify the sender and the recipient: it should include means of verifying, either through the technique used in the transfer itself*

or by some other manner provided by the TDI- AP concerned, the formal completeness and authenticity of the transfer.

7.c) *If a transfer received appears not to be in good order, correct and complete in form, the recipient should inform the sender thereof as soon as possible.*

7.d) *If the recipient of a transfer understands that it is not intended for him, he should take reasonable action as soon as possible to inform the sender and should delete the information contained in such transfer from his system, apart from the trade data log.*

10.a) *Each party should ensure that a complete trade data log is maintained of all transfers as they were sent and received without any modification.*

10.d) *Each party shall be responsible for making such arrangements as may be necessary for the data referred to in paragraph (b) of this article to be prepared as a correct record of the transfers as sent and received by that party in accordance with paragraph (a) of this article.*

10.e) *Each party must see to it that the person responsible for the data processing system of the party concerned, or such third party as may be agreed by the parties or required by law, shall, where so required, certify that the trade data log and any reproduction made from it is correct.*

Question 8 — *Should there be rules on "signature" ?*

Articles (5.a), (6.a) et (6.b) state that the transactions done and the messages exchanged must be correct, complete and secure. Completeness and authenticity could be verified by the transfer protocol used. We have here a typical example of application for the techniques of authentication and, more particularly, the electronic signature.

Articles (7.c) et (7.d) are a particular case of the three preceeding ones. As a transfer (or a message) is received in an incomplete or incorrect form or if it has not been delivered to the right person, the recipient must inform the sender as soon as possible and must also destroy the message received. These characteristics of completeness, correction and security could be verified by means of identification techniques.

Article (5.b) mentions that no modification could be done on the content of a message by the intermediaries of the transfer. How can we be sure that no modification has been done ? By means of identification and signature techniques, of course !

About the problem of conservation of transactions traces in the trade data log (log file), articles (10.a), (10.d) et (10.e) impose that the conservation must be done in a correct way and without any modification on the content of transfers

or messages (kept as traces) as well as on the support of these. Once again, we're in the domain of application of authentication and signature techniques.

Finally, we can see that writers of the UNCID rules have been aware of problems about the "signature" as explained in their eighth question and that they are in favour of an agreement about the admissibility of an electronic signature.

4.3 Encryption

We will now analyze how the UNCID rules have considered the problem of encryption of documents.

5.a) *Parties applying a TDI-AP should ensure thar their transfers are correct and complete in form, and secure, according to the TDI- AP concerned and should take care to ensure their capability to receive such transfers.*

5.b) *Intermediaries in transfers should be instructed to ensure that there is no unauthorized change in transfers required to be retransmitted and that the data content of such transfers is not disclosed to any unauthorized person.*

6.a) *A trade data message may relate to one or more trade transactions and should contain the appropriate identifier for each transaction and means of verifying that the message is complete and correct according to the TDI-AP concerned.*

6.b) *A transfer should identify the sender and the recipient: it should include means of verifying, either through the technique used in the transfer itself or by some other manner provided by the TDI-AP concerned, the formal completeness and authenticity of the transfer.*

7.c) *If a transfer received appears not to be in good order, correct and complete in form, the recipient should inform the sender thereof as soon as possible.*

7.d) *If the recipient of a transfer understands that it is not intended for him, he should take reasonable action as soon as possible to inform the sender and should delete the information contained in such transfer from his system, apart from the trade data log.*

9.a) *The parties may agree to apply special protection, where permissible, by encryption or by other means, to some or all data exchanged between them.*

9.b) *The recipient of a transfer so protected should assure that at least the same level of protection is applied for any further transfer.*

10.a) *Each party should ensure that a complete trade data log is maintained of all transfers as they were sent and received without any modification.*

10.d) *Each party shall be responsible far making such arrangements as may be necessary for the data referred to in paragraph (b) of this article to be prepared as a correct record of the transfers as sent and received by that party in accordance with paragraph (a) of this article.*

10.e) *Each party must see to it that the person responsible for the data processing system of the party concerned, or such third party as may be agreed by the parties or required by law, shall, where so required, certify that the trade data log and any reproduction made from it is correct.*

Question 5 - *Should there be rules on secrecy or other rules regarding the substance of the data exchanged ?*

Question 7 - *Should there be rules on encryption or other security measures?*

First, we must remark that the UNCID rules have expressly taken into account the problem of encryption as explained by articles (9.a), (9.b) and questions (5 and 7).

Articles (5.a) and (5.b) are dealing with the problem of security and of non disclosure of a transfer or a message to an unauthorized person. The only way to be protected against such disclosure (or wire tapping) is to assure the confidentiality of the document content and therefore to use encryption techniques.

Articles (6.a), (6.b), (7.c) and (7.d) are dealing with the completeness and the correction of transfers and messages. How is it possible to detect any error or fraud during the transfer ? Beside the use of authentication techniques, the encryption allows that detection. Indeed, if a modification has been made on a previously encrypted message, the recipient of the message will be aware of the problem because it will be impossible for him to decrypt it correctly. This is guaranteed by one particularity of encryption techniques which is: if an error occurs during the transfer of an encrypted message, the decryption of the erroneous message will give as result another message profoundly and completely different from the original one. The end result will be an incomprehensible message.

There is a major problem limiting the use of encryption techniques regarding the UNCID rules (7.c) and (7.d). In fact, if someone receives a message with errors or wrongly addressed, he may not be able to decrypt the message in order to find the correct address of the sender. And therefore, it will be impossible for him to inform the sender about the error as he is required by the two articles.

And finally, the log files, described in articles (10.a), (10.d) and (10.e), could also be protected from an eavesdropper by encryption techniques.

IV. CONCLUSION

We conclude with referring to two opinions of American judges.

1. As asserted by the Supreme Court of Nebraska in 1965, it is time now to "bring the reality of business and professional practice into the courtroom". It is time to consider as *admissible* by the courts an electronic signature like a traditional one.
2. In respect to the opinion of another American judge in 1976, "as one of the many who have received computerized bills and dunning letters for accounts paid since a long time, I am not prepared to accept the product of a computer as the equivalent of the Holy writ". In other terms, the *credibility* of an electronic signature will depend on the security level that the chosen techniques are able to prove.
3. In this respect, the court will take into consideration not only the technical but also the organisational measures taken by the responsible of the computer system, according to the importance and the characteristic of the transactions concluded by this system.
4. Finally, in order to avoid uncertainty as to the legal acceptance of modern means of authentication, it is strongly recommended that parties who intend to use them, agree in advance in writing on the validity of the technology they will use for concluding transactions. From this point of view, the UNCID code can be viewed as an adequate model.