Data security and formation of contracts

Elias, Lieve

Published in:
Data security in computer networks and legal problems

Publication date:
1992

Document Version
Publisher's PDF, also known as Version of record

Data Security and Formation of Contracts

Lieve Elias

1. Introduction

The question of data security in a contract formation process can be viewed from very different perspectives. For instance, one could ask what will be the criminal procedures applicable in case of a non-authorized access to the data bases, who will be declared responsible in case of damages suffered by parties, etc... However, prior to these preoccupations the contracting parties might face two more urgent questions : 1. first of all, do they have to execute a contract that was formed as a result of a message that for one or another reason has been altered during its transmission and secondly, if they have to, which version of the message will they have to execute : the message as it was sent by the sender or the message as it was received by the recipient ?

Currently neither any legislation nor any case law specifically applicable in the field of EDI is available on this matter. Therefore this analysis refers to other more traditional techniques of communications such as postmail, telex or telefax.

We will first define the type of risk we are dealing with in this analysis. Without entering into any more technical details, we shall also present a survey of the security procedures available in an EDI- environment.

Secondly we will examine what solutions law has applied to the paper-based communication systems.

Finally we will consider whether these solutions are still appropriate in an EDI-environment.

2. The risks and security procedures

Generally, we can distinguish four risks arising from the use of EDI for the transmission of commercial data.

1. The transmission of uncomplete or falsified data to the recipient

2. The transmission of the data to an erroneous recipient

3. the transmission of the data by an unauthorized sender

4. delay in the transmission of the data.

In this analysis we are only dealing with the first type of risk, namely the transmission of uncomplete or falsified data to the recipient. To give a very simple example : party A sends

a purchase order to party B asking for 500 units of product X. The message arrives at destination and is understood by the recipient as an order for 5000 units. If the error in transmission is not detected, party B will deliver 5000 pieces of X according to the message he received. Party A, not willing to pay 4500 units more then he asked for, will try to send them back. A dispute may arise.

Commercial partners communicating by EDI have the possibility to protect themselves against such a situation by assuring a higher level of technical security. A well known way to assure data integrity is the use of an electronic signature. Moreover, the data integrity can be checked by the sender of the message in so far the recipient sends a verification message.

– An **electronic signature** is a short series of characters pasted at the end of a document. To this extent an electronic signature is the output of data related to the content of the document itself, it will allow the content of the document to be authentical. This means that one could establish whether the document has been modified[1].

– A **verification message** can take essentially two different forms. An acknowledgement of receipt is a message acknowledging or rejecting with error indication a received interchange, functional group or message. A confirmation of content is a message stating that the confirmed message has been correctly understood and is complete. This second message includes the identification, authentication and verification of the integrity and origin of a message.

100% technical security however is difficult to guarantee. For two reasons, technical security measures cannot make complete secure systems:

- technical security measures are never 100 % effective, they sometimes introduce new risks or endanger other measures [2];
- in every operational environment unpredictable risks are a fact

Moreover, the parties may not be ready to pay for such a high degree of technical security.

Therefore, to avoid any conflict, it is necessary to combine the technical security provisions with legal obligations dictating what to do when something goes wrong.

3. Solutions adopted by law

Until now, as there is no specific caselaw concerning this matter, it is very difficult to predict what a court will decide in case of a garbled electronic transmission.

However, a somewhat similar problem arose before a British court[3] concerning a garbled telegram : two commercial partners were negociating the purchase of rifles. Party A wrote to Party B that he could fix an order for 50 rifles at 34 s. Party B replied that he could not

[1] M. Antoine, J-F. Brackeland, M. Eloy, Y. Poullet, "Legal requirements facing new signature technologies, C.R.I.D., International Course on Computer Security and Industrial Cryptography",

[2] J. Van Ausloos, "Technical security : the starting point", Eurocrypt '89, S.W.I.F.T. presentation.

[3] Henkel v. Pape, (1870) L.R. 6 Ex. 7.

sell them for less than 35 s. Thereupon Party A sends a telegram saying : "send *three* rifles". The telegram arrived at destination in the form "send *the* rifles".

Party B sent to Party A 50 rifles, but it was held that Party A was not bound to accept more than three. In this case, the recipient was bound by the buyer version of the message.

Although there are no reasons for generalisation, this decision gives an indication of what might be the court's decision in case of a garbled electronic transmission.

4. To a new solution in an EDI-environment ?

The major question in this paper is to know whether in an EDI-environment it would be plausible to submit above-mentioned questions to the judgement of a court or whether a better solution can be negotiated by the contracting parties.

Within this context it is important to consider that electronic technologies offer contracting parties a wider series of possibilies to maintain a certain level of security. This together with the provisions of the UNCID-rules may place the question in a different light.

The UNCID-rules (Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission) were elaborated by a special Joint Committee of the International Chamber of Commerce. They provide a model contract for users of EDI. The UNCID-rules also define an accepted level of professional behaviour, a "code of good conduct"[4]. Articles 7 and 8 of the rules are of particular interest to our matter.

According to the article 7 a) The sender of a trade data transmission [interchange] may stipulate that the recipient should acknowledge receipt thereof. Acknowledgement may be made through the teletransmisson technique used or by other means provided through the TDI-AP concerned. Recipients are not authorized to act on transmissions [interchanges] stipulating acknowledgement until the requirement of this Article has been satisfied.

According to the article 8 a) The sender of a trade data transmission [interchange] may request the recipient to advise him whether the content of one or more identified messages of the transmission [interchange] is accepted as correct, without prejudice to any subsequent consideration or action that the content may warrant. Recipients are not authorized to act on transmissions [interchanges] until this requirement has been satisfied.

It should be noted that according to the UNCID-rules the initiative for requesting an acknowledgement or a confirmation of content belongs to the sender of the message. These provisions would lose much of their sense if the sender knew that *his* version would prevail in case of dispute. Wouldn't it make more sense logically to link the consequences arising from the absence of any functional acknowlegment or confirmation of content to the initiator?

In order to promote the use of security procedures, it may be useful to adopt a provision in an intechange agreement that gives priority to the message as it is received by the recipient.

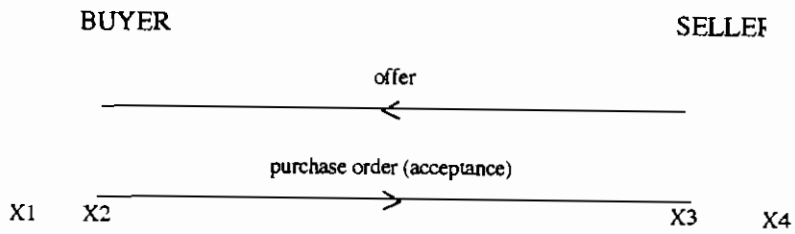
[4] B. Wheble, "Think data, not documents", *I.F.L.R.*, june 1988, 37.

It will be up to the sender to decide whether he considers his message important enough to ask for an ackowledgement or confirmation of content.

Another approach is currently being examined within the UN/ECE. They favour the rule that electronic messages lacking verification are not to be given any real value : no legal consequences can be attached to the message. The notion of fairness is being respected by the fact that the rule is reciprocal[5]. This rule imposes to the parties an even more radical obligation of guaranteeing security in electronic transmissions.

For both approaches, it is very important to consider all the questions that might rise from the application of these rules. For instance, will the duty of systematic verification have an influence on the location and the time of conclusion of contract ? This question may be important in order to determine the law applicable to the contract as well as to determine the capacities of the contracting parties or the moment of transfer of the risks and ownership of the goods.

With regard to the determination of the place and the moment of conclusion of a contract, four rules have been developped. In order to illustrate these theories, we first present a chart identifying the four theories.

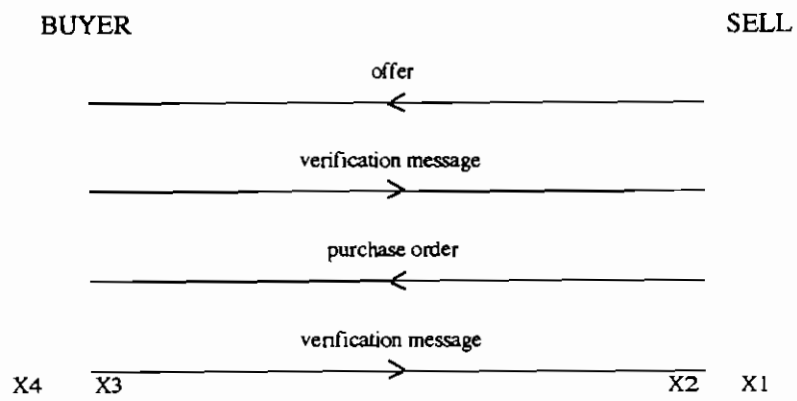


Following

- the declaration rule, the contract is formed at the moment and the place the decision to accept has been taken (X1);
- the expedition rule, the contract is formed at the moment and the place the declaration of the acceptance is sent (X2);
- the reception rule, the contract is formed at the moment and the place the declaration arrives at destination (X3);
- the information rule, the contract is formed when the offeror takes notice of acceptance (X4).

[5] J.B. Ritter, "Electronic commerce and international law : a tapestry in the making", Third International Congress of EDI users, Proceedings, pp. 117-126.

example : sales transaction with verification messages



Let's suppose that the parties choose for the rule of reception. In that case they expect that the contract will be formed on the moment and the place where the acceptance arrives at destination. This will generally be the nation where the seller has his residence.

Will the duty of verification postpone the conclusion of the contract ? If it will, the place of conclusion will in application of the same rule of reception be in the nation where the buyer has his residence. There seems however no good reason why such a verification would postpone the conclusion of contract. Indeed, these messages provide only evidence that the original message has been received without errors. Even if it stated that the original message is deprived of any legal value, this fact doesn't give a contractual significance to the verification message.

By means of conclusion, I would like to add that the use of EDI raises new questions which demand new solutions. As to these solutions however, all possible consequences should be foreseen and prepared in advance.