BILETA
BRITISH & IRISH
LEGAL
EDUCATION
TECHNOLOGY
ASSOCIATION

**13th Annual BILETA Conference: '*The Changing Jurisdiction*'**

**Friday, March 27th & Saturday, March 28th, 1998.**
**Trinity College, Dublin.**

# Cryptography and the Law

*Fernando Galindo*
*Professor Titular of Philosophy of Law*
*University of Zaragoza (SPAIN)*
*Foundation FESTE.*

**Abstract**

In the paper after making reference, shortly, to the weaknesses of Internet and the main juridical problems that it outlines the installation of the cryptographic techniques, it is considered which are the possible juridical solutions in the existent juridical norms to the problem of the regulation of the digital signature. Finally a concrete solution is exposed. The solution comes from an experience in which the author of the paper participates.

## *I. Weaknesses of Internet and juridical problems*

### Weaknesses of Internet

The weaknesses of Internet consist in that the mechanism of operation of the net allows the interception of the messages for their users. The net works by means of the shipment of packages of information among originators and receivers, of one to another part of the world, using to the connected computers, what behaves that it is very easy to observe the content of messages, for example in those that consist numbers and keys of credit cards, or any other type of communications maintained by the users. It is also possible to modify the sent messages.

This generates several disadvantages of the means, the main is that this practice goes against the security and trust of the electronic trade, source of wealth and work. That which worries industries and governments and, at the same time, it limits the expansion of Internet. It is this way it, because the trade freedom cannot be satisfied if channels of transmission of the information so vulnerable exist as the existent, or if technical solutions contrary to fundamental principles of the established juridical regulations as the secret of the communications are adopted.

The solution goes by two procedures. The first consists on the use of mechanisms and institutions required by the ciphered of messages that:

(a). allow to guarantee the shipment and destination, or what is the same thing to know with enough certainty that the message has been emitted, has arrived, in what day and hour has been made, who has sent it and who has received it, and its content has not been altered, and

(b). prevent to observe the content of the communications.

The second remedy consists on the co-ordination of the use of the mentioned mechanisms with the execution

of the effective juridical regulation, once the use of the ciphered of messages can injure fundamental principles of the legal norms.

In this paper it becomes special emphasis in the juridical remedy, in definitive in making compatible the use of the mechanisms of ciphered of the messages with the execution of the Law.

The most serious juridical problems refer: to the democratic allotment of the power and the preservation of the intimacy, the freedom of speech, the preservation of public security and that of public faith. Next these problems are explained shortly.

**Allotment of power and protection of the intimacy**

The cryptography solves the identification problems, confidentiality or intimacy, but creates other many. From a juridical point of view the most fundamental is the problem of the power. Regarding the identification the problem is in the deforcement of the power of identifying. In that referred to the confidentiality or intimacy the problem consists on the possession of the keys of ciphered and deciphered.

The problem relative to the power of identifying consists in that, outside of the private relationships in that the person assumes the revelation of her data because she interests him, this imperium is conferred by the laws only to the public authorities. These have the obligation of respecting the Right to the disposition of their own data that have the identified citizens. For the confidentiality the problem consists fundamentally on the safeguard of the keys.

With the cryptography these powers are in possession of the possessors of the techniques. In one and another case the possessor of the personal data or the keys can dominate the user of the cryptographic techniques, with more effectiveness even that with the use of the weapons. This is one of the reasons for those that the cryptographic resources are compared those of armament in the regulations to the export of products of double use, picked up in treaties and agreements.

To stop these difficulties it is not enough the established mechanism for the protection of personal data, the Agency of protection of data or Register, once the preservation of the personal data, the private key or the secret of the communications is not function of the Agency. Their function consists on giving publicity on the existence of files of public or private character that contain stored personal information. This declaration has as exclusive end that the citizens can carry out a democratic control of the use that is made of this information, once they are owner of a right to the informative self-determination.

The transmission to this institution of the content of the identifications or the private keys and the deposit of the same would be the prelude, on the other hand, to the establishment of a dangerous -state central unit - of control of the data of all the people, and the keys that would be adequate to disclosure the content of all the communications. The Agency would be good exactly for the opposite for what has been created: it would be the central organ of an organisation expert of all the secrets (publics and private).

This makes necessary the establishment of a group of independent institutions that are able to identify people with the enough guarantees of reservation of the personal data, in the case of the digital signature of messages, or, in the case of the ciphered of messages, if it is opportune because the users of the system consider it or the laws prescribe it, be able to keep with the enough guarantees the secret keys.

**Freedom of speech and security**

The problem of the power of the key derives in other: the restriction to the freedom of speech. It is this way it because the technical solutions, mainly those that prevent to observe the content, facilitate the freedom of speech but they also hinder and in occasions impede actions directed to the prevention of the crime: the interception to the telecommunications of legal character. That which requires the establishment of measures that allow the interception of messages for the services of security and with it the generation of possible excesses that can affect at the beginning of freedom of speech, besides, of course, to that of personal intimacy.

This requires the installation of institutions that are able to ponder the degree of zeal there been in the execution of the interception on the part of the services of security legitimated for it and the one of lesion to the freedom of speech that can cause certain interceptions.

**Public faith**

A problem not smaller, also of power and more concrete than the previous ones, it is that the installation of measures of security, consistent in the use of techniques of ciphered, it requires, like it has been expressed, the establishment of adjusted organisations to the existent nets of security and trust of the economic, social relationships and communications. These networks work from beginnings of the XIX century at the same time that the liberal State was implanted. It is in that moment when state registrations were constituted that had for function to facilitate and to protect the exercise of the rights of people at the same time that to guarantee the mercantile traffic and the right to the vote.

The fundamental problem in this environment resides today in that the telecommunications, whose resources by means of the use of Internet are used in the first place in a country of Anglo-Saxon law as United States, with organisation different to those of most of the European countries, are introducing as basic agents, trusted or certification services, of Internet to companies or new institutions. With that which the new techniques change in the practice is a fundamental juridical system of the State of Law: the system of public faith whose pillars are constituted by different agents: notaries, trade corridors, lawyers and public registrations of judicial, mercantile or administrative character.

***II. Juridical solutions***

Next (III) we will observe an existent juridical solution to the problems mentioned in the previous section. Here we centre ourselves in the juridical answer that one can give to the problem of the digital signature, first cryptographic mechanism that is putting into practice thanks to the same technological development. To effects of exposing the ideas with the biggest clarity the discussion is centred in the problems that can have in trial the electronic documents elaborated by means of the use of the digital signature.

**The digital signature**

From a technical point of view, and if we assist to the effects of the same one, the digital signature is the mechanism that allows to guarantee the identity of the signatory of a document as well as the non alteration of its content (PASTOR, J., SARASA, M.A., Criptografía digital. Fundamentos y aplicaciones, Prensas Universitarias de Zaragoza, Zaragoza, 1998, p. 343).

A definition of digital or electronic signature that explains the description of its generation process happened by means of the use of the asymmetric cryptography is the one that says that the digital signature is the "information that identifies to the public key with its user, when having been signed by the person owner of the certificate of public key using the private key with which has generated its public key" (German Federal Bill establishing the general conditions for Information and Communication Services, June 1997, art. 3, 2; POHL, H., Guidelines for the Uses of Names and Keys on a Global TTP Infrastructure. Final Report, INFOSEC, European Commission DGXIII, July 1997, p. 100; NRC project, Cryptography's Role in Securing the Information Society, May 30, 1996, ap. B, to see in http://www.replay.com/mirror/nrc)

This last description makes see that, assumed the technical statements that guarantee identification and content of the transmitted texts, the most characteristic problem to the judicial probe in trial of the digital signature consists in that is always precise to demonstrate the intervention of a person, entity or organisation different to the signatory that credit the information, or what is the same thing the attribution from the public key to the holder of the digital signature of a message. This entity, denominated certification service, will be able to give the accreditation because the holder of the signature has declared that it is his and, also, because the entity will have checked, through appropriate procedures, its statements or attributes. It is for it that the use of the digital signature always requires this certification to have validity.

It implies the necessity to regulate two basic requirements so that a concrete digital signature can be kept in mind in a trial: the certification for an entity different to that of the holder of the signature, and the procedure

that follows this entity to define qualities or a person's attributes. This way it would be paid legally, at least in a country of continental right, the problem of the test in trial of the digital signatures.

Made this delimitation of the problem, there are precedent normative in the continental environment. Another thing happens in the Anglo-Saxon area. Next we make reference to both.

**Precedents**

In Anglo-Saxon law precedents that can be considered rules to give value to signatures non manuals exist. These precedents (the data have been given by Juan Andrés Avellán, Queens Mary and Westfield College, University of London) made reference to the value of the signature made by means of fax, to the value like signature of a stamp printing instead of a signature or to the value like signature of a sign fixed by an illiterate in a place different to the one foreseen for the signature in a document. The problem is in that these precedents that can be in any regulation, don't affect to the substantial difficulty of the probe in trial of the digital signature that before has been expressed: the necessity that they have participated, direct or indirectly, at least two people in its emission.

Others mention that the commercial uses that have given the value of the telex or of the bank documents of payment can be considered precedents (BOHM, N., Do we need new digital signature law). These arguments forget that in the use of the digital signature we are speaking of the relationships maintained among all the citizens, or between the citizens and the Administration. In these cases there are not relations among companies, relationships of bank type or commercial relationships.

It must be solved the problem at least of endowing from validity to a signature in which is necessary the intervention of two people. The solution must also be so safe that it must allow that the doubts arisen in the communications carried out by electronic means can be solved without necessity of going, in first instance, to the judges or tribunals.

**Norms**

The next regulative mark to the requirement of the intervention of a third in the signature of a document is constituted by the norm that prescribes the action of the Notaries of continental Law, when they participate in the daily traffic, to effects of granting public's character to a document signed before the same ones. It is also it the procedural norm that indicates that these Notaries certifies the juridical contents of the acts or transactions of those that they are witness. It is not of missing, for it, the one that the technical proposals referred to the electronic communications reiterate the expression notarising when they denominate succinctly which the indispensable requirements are for their security and guarantee.

But these circumstances that can be precedent total as soon as they exemplify the characteristics of the action of validating a signature, it can only be a partial precedent to a hypothetical regulation on certification of the digital signature, because the Law doesn't require the presence of the Notary in the signature of all the documents or transactions. With the effective legislation if a signature is recognised as own by a person, or its ownership is proven by technicians in graphology, even when it has not been recognised by a Notary, the signature is perfectly valid. It doesn't happen the same thing with the digital signature, since, by definition, to her it cannot be considered existent if it is not recognised by an instance to which is denominated certification service. This requires a law that prescribes who can be certification services for all the digital signatures.

For the certification of characteristic or a person's attributes are not only precedent the action from the Notaries when certifying the content of the public documents. It must keep in mind that certification of properties or a person's attributes, of course that with very different object, reach and effects, it can also be given by another type of officials. This way those in charge of a census registration or the judges responsible for a judicial registration. With regard to the properties of a person the certification must give it the Registration of the property. The profession is certified by the ownership to a professional School or the habiliment that gives the Ministry of Education or a private Centre of Studies. The existence of a company is certified for their inscription in the Mercantile Registration. In countries where a National Document of Identity exists an official it can compare the image of the picture of the document or the holder's print with those that the identified person has. The quantity of existent money in a certain bank bill of which is regular a person can be certified by the same bank entity. A matter, third in good faith towards the established relationship between two people, can also testify or “to certify” with regard to this relationship... A law of digital signature should

assist to this casuistry and to point out the object, reach and weight of the certifications emitted by different certification services.

On the other hand regulative precedent cannot be considered for the probe in trial of the digital signature the one that prescribes the intervention of technicians in the probatory phase of the process. In this case the technicians would be the experts in cryptography that, hypothetically, they demonstrated the ownership from a digital signature to certain person. This comparison is not possible because the verification of the identity of the holder of the digital signature cannot be carried out for indications. It is necessary to have the declaration on the part of the holder of the digital signature of the secret or private key starting from which the public one has been generated. The secret key is only known by who the public and private couple of keys generates.

The cryptography guarantees that it is not possible to discover the correlation among both keys, of there its reliability. This is the last reason for which the public authorities specify the derived personal responsibility of the loss, forgetfulness or subtraction of the private key, or what makes them prepare, in other cases, of mechanisms that facilitate the recovery or escrow of the private key. Reason that is barely used by the authorities to the regulation of the recovery or the deposit of the private key, once they are based fundamentally on arguments referred to the prevention of the delinquency and the terrorism.

Of there it is necessary an organisation of institutions of trust that guarantee the secret of the private key. In continental law these institutions can be, partly, the Notaries forced by law, even penal sanction, to the safeguard of the confident secrets to the same ones. Partly new institutions, the certification services that make public the public keys.

These Notaries, also, has the social trust, that is to say they are trusted professional entities for several centuries. A law of digital signature would should, therefore, to have these facts and to establish the appropriate conditions for the deposit or the mechanism or procedure of recovery of the private key when it is necessary.

**An juridical solution**

For all the solution to the problem of the probe in trial of electronic messages signed digitally specifies at the present time of the elaboration of proposals directed to the promulgation of a norm that defines with enough clarity the characteristics of the digital signature and specify the content and reach of the actions carried out by the certification entities. This last is of special importance in that referred within reach of the certifications that emit, or what is the same thing to the definition of the main elements, work and values to satisfy for those entities.

In short the law must specify the characteristics of:

1) the digital signature,
2) the certification authorities or entities,
3) the registration entities,
4) their object, function and ends or values,
5) the certificates: classes,
6) the recovery or deposit of the private key, and
7) the corresponding contracts, regulations and indispensable practice codes for their operation.

***III. The solution FESTE***

All the above-mentioned has made build a suitable juridical solution to the exposed situation. This solution began with the investigation project AEQUITAS and FESTE has become the solution Error! Reference source not found.. FESTE has juridical proposals for the present, for lack of a state or European environment regulation, in form of the net of security and trust of the electronic communications that, with the same name, it has constituted. The established contracts between the certification services and registration of the electronic communications and their clients are also part of their proposal. Whose object is presented, succinctly, at the end of this section.

**AEQUITAS**

AEQUITAS is an investigation project that finally has to reflect how is possible the probe in trial of ciphered and signed electronically messages.

The project began in 1997 as an investigation project, selected through the corresponding public competition, promoted by the European Union, General Directorate XIII-7, group INFOSEC, Security of the systems of Information. From the beginning of 1997 until the present time. the project works together with other six European projects with the objective of building between all the basic infrastructure to the construction of an European network of trusted services of the electronic communications. It is the only juridical project of those promoted by the DGXIII with this object in 1997. This year the Commission have incorporated to the same work other six projects (one is juridical).

The project AEQUITAS had from their beginning the participation of a group of thirty Spanish and French jurists of different professions and work place. The investigation group was constituted by teams of the Faculty of Law and the School of Engineers of the University of Zaragoza together with the Spanish company Intercomputer S.A., specialised in the development of telematic systems.

The beginning of the project was limited to gather information to reach the final objective of the same, that is constituted by the elaboration of a Report on the probe in trial of ciphered messages. It leaves of the information it is integrated by the study and summary of the legislation and existent technical measures to achieve the trust of the electronic communications, and for the same thing the possibility that they are considered probe in trial the messages sent using the electronic techniques. The other great part of the information to which assists the project is constituted by the experience acquired by the group of users jurists in the use of these techniques in its daily professional practice, in the relative to the transmission of messages and the access to documentation systems.

Through the reports emitted by the project until this moment, the project have elaborated different proposals of European and state normative referred to the establishment of measures of trust of the electronic communications. The proposals, in more or smaller degree, have been reflected in normative approved or in approval phase for the European Union from the second half of 1997. In short the Communication (97) 503 of October 8 on “The development of the security and the trust in the electronic communication. Toward a European mark for the digital signature and the ciphered” and the project of Directive European on “A common framework for the services of electronic signature”, in elaboration for the Commission at the present time.

In these moments the project AEQUITAS works in the final Report. The material of this Report will be on the content possible of a regulation on this matter for a European country that has been picked up at the end of the previous section.

The review of all these elements will allow to constitute the nucleus from an juridical institution, that well can denominate digital signature whose setting in action, by means of the work carried out by the certification and registration services, will grant probatory value in trial to the electronic documents generated with its aid.

At the present time AEQUITAS has become an investigation program in whose setting in practice participates Notaries and Corridors of Trade, Procurators of the Tribunals, Lawyers, Judges, Ministry of Justice, Institutions of state, regional and local character and the own European Union.

In the mark of the investigation program AEQUITAS is building, especially, certification services and systems of trust to those that it is denominated certification and registration services. Norms of state and European environment are also generated. A product of AEQUITAS is the constitution, at the end of November of 1997, of the Foundation for the Study of the Security of the Telecommunications (FESTE). The Foundation has for object the realisation and promotion of studies and investigations on the matter. It also operates as system of trust.

**FESTE**

**The Foundation**

The installation of FESTE responds to the necessity felt by the members of the same (Associate National of Notaries, National School of Corridors of Trade, the University of Zaragoza and the company Intercomputer S.A.) that it is necessary to foment the group of investigations of juridical character that is required by the phenomenon of the security of the electronic telecommunications actively. FESTE also wants to establish a European net of centres of trust of similar character.

The Foundation has solved this task assuming as horizon of own action the satisfaction of two basic objectives: in the first place, the proposal that the traditional Notaries are constituted, as soon as registration services, as basic elements of the networks of security and guarantee of the electronic communications that are constituted in Spain. The first example of this performance is the formed by the net of which FESTE is constituted as certification service. The second objective of FESTE is constituted by the Spanish elaboration of a normative on the security and guarantee of the electronic communications. On it is the following thing.

**FESTE as certification service**

The Foundation FESTE has established the net of security and guarantee of the electronic communications of the same name, integrated by the National School of Notaries, the National School of Corridors of Trade, the University of Zaragoza and the company Intercomputer and the traditional Notaries. The function of the net, once it has assumed that has as objective the one of being constituted as certification service, it depends on the fact that, in coherence with that expressed in the mentioned Communication (97) 503 of the European Commission, FESTE acts next to the same Notaries, registration services, so much in the certification of belongings, presences and capacities, like in the exercise of the safeguard of the security and guarantee of the electronic communications, the last thing especially by means of the conservation of the private key of the users, case that these have interest in the same thing. This means that the net seeks to reduce, insofar as possible since it is an initial experience, the inconveniences that it generates the use from the cryptographic techniques to the security and juridical guarantee of the electronic communications.

The state of the question has made that the Foundation FESTE has assumed as one of its first work objects the elaboration of a Spanish bill about security and trust of the electronic communications that it is coherent so much with the Spanish juridical regulation as with the European precedents and the regulation of other countries that it was collection in the Report titled AEQUITAS “The guarantee of the security and trust of the electronic communications in the European Union”. The elaboration of this bill has been taken charge to a Committee integrated by members of the Foundation and Spanish experts on the matter.

It is will of the Foundation to present to Spanish and community public authorities with the biggest possible brevity the referred project whose works are beginning. At this time it is been awaiting the promulgation on the part of the European Union of the Directive on digital signature.

The proposals elaborated along the experience AEQUITAS, in the measure in that the DGXIII has made them public through its web, will be taken as some of the references for the making of the project. It must keep in mind that several members of the project AEQUITAS is members of the Committee of elaboration of the bill.

The reference for the members of AEQUITAS is constituted by the content of contracts, in occasions already established through two experiences (SISCER and AD AEQUITATEM), in occasions to settle down in a next future conform to it develops the experience AEQUITAS in connection with the performance of services of certification of public or private character. SISCER and AD AEQUITATEM are two certification systems acted from March of 1997 by the University of Zaragoza and Intercomputer S.A., the first one has been used along one year by bank entities, the second is an experimental system.

Of the contracts, normative germ of a future one, treats the following.

**Contracts**

The development of the project AEQUITAS has allowed to elaborate several models of contracts that can be considered constitute the basic norms to govern the juridical life of a certification service in connection with its users while laws that regulate its operation don't exist (basic for them it is the content of: CASTELL, S., Report to the Commission of the European Communities for the Code of practice and management guidelines for trusted third party services, INFOSEC, European Commission DGXIII, October 1993). These contracts define

the degree of established commitment between the service and their clients and with they base it the value that the same ones must have in case the electronic documents certified by the service of certification object of acceptance in the same ones could be object of probe in a trial. Presently it is shown, in concise form, the content of these contracts and the denomination of others that should settle down like exemplary sample for the correct operation of a certification service that had to act in the case of law non-existence.

The fundamental contractual types, at this time initial of use of the nets of security and trust of the electronic communications, are those referred to the service of authentication of computers, to the service of certification of electronic signature and that of properly notarizing, here exemplified by means of one of their possible modalities.

**a) Contract of authentication of servers**

The contract of authentication of servers has for objective to guarantee to the user that the computer in which controls the information stored by the user is really the same to that the user's client wants to make this access. This contract guarantees to the user that cannot be offered by another person the information or the product that the user offers, or that the client's demand is carried out the user indeed and not to another entity. It also guarantees that the communication that takes place between the client and the user goes ciphered, with that which cannot be known by a third. Client and user have a secure communication to the power to contrast in all moment with the certification service the authenticity of the public key that identifies the server.

The fundamental content of this contract would be centred in the establishment of a clause that picked up the following rights and obligations: “Both parts agree that the supplier will provide the user and their clients the service of authentication of server web, by means of the certification of the public key of the user's server web and diffusion of the same one and of his certification to the user's clients that request it. Everything will be carried out using the protocol...”

**b) Contract of certification of electronic signature**

The contract of certification of electronics signature guarantees to the user that the data manifested by the user to the corresponding register service (notary, trade corridor or enabled registration), identify the user with regard to the petitions made to the certification service by a third that wants to check the authenticity of the signature of a message emitted by the user. The agent of register must be considered as such by the certification service by virtue of the terms picked up in the law or the established contract between the certification service and the agent.

The fundamental content of a contract of these characteristics would be reflected in a clause that said the following thing: “Both parts agree that the supplier will provide the user the service of certification of the user's electronic signature, by means of the certification of his public key or electronic signature and diffusion of the same one and of his certification at the third that request it. Everything will be carried out using the protocol..”

**c) Contract of notarizing of electronic transactions**

The notarizing contract prepares the registration of the established communications between the user and another person. There are several the existent possibilities of this contract once it is possible the notarizing of different activities. It is necessary this way to think, for example, in the notarizing of the identification of the communicants, of their public keys, of the date and the hour of the messages, of the non repudiation, of the ciphered content of the messages, of the content in clear of the messages...

A simple modality of this contract can be the collection in the following clause: “Both parts agree that the supplier will keep a registration with the date and hour of the connections, as well as of the URL accessed in each one of them. It will be been able to it to make in the user's transactions, or to application of the server of this. Everything will be carried out using the protocol..”

**d) Other contracts**

Besides the mentioned contracts that can be considered basic, other models of great importance exist. In short they are constituted for:

a) the contract in which is specified the characteristics from the borrowed service to the user for the certification service and the registration offices,
b) the established contract between the certification service and the registration entities,
c) the established contract among the certification service and the technological companies in charge of supporting the operation of the system,
d) the agreement of deposit of the private key in the corresponding agent carried out by their holder and the agent
e) the respective contracts of responsability...

**Conclusion**

In spite of the disparity of the Anglo-Saxon and continental juridical world, the juridical solution to the problem of the electronic communications here exposed can expand in both juridical territories. In any event the shown example points out that the integration of traditional institutions of trust, investigation and managerial dynamics, allow to give solutions to one of those that is configuring like one of the most important problems for the advance of the society of the information and the setting in real practice, assisting to all the interested ones, of the phenomenon of the globalisation.


- Return to index


---