Electronic Signature: An Analysis of European and International Legal Regulations

Use of electronic and digital signatures hopefully should give rise to a quantum jump in electronic commerce transactions. Moreover, it will improve relations between the citizens and local or even international government bodies in the near future, especially if national regulations are harmonised. Governments, therefore, should cooperate and make necessary changes across the globe so that a 'single' electronic/digital signature suffices for a person just as a manual signature now.

Handwritten Vs. Digital Signatures

In bygone civilisations, human beings used to seal a deal by the words of mouth (or honor). As social relationships became more complex, and the ability to write became widespread throughout the world, some sort of 'symbols' were written at the 'foot' of a document as "proof of its acceptance and verification" (e.g., commercial documents, marriage contracts or diplomatic agreements). Over the centuries these symbols started to be replaced by letters taken from the author's name, handwritten by the author himself, and further personalised with a flourish. Nowadays, the personal handwritten signature is commonly used as a proof of 'agreement' and 'acceptance' between different parties.

In the modern era, with increasing presence of 'digital' documents, it has become very difficult to continue with the 'traditional' handwritten forms of authentication. There is, therefore, a need to create 'new' paradigms and methods, which can maintain the same level of legal validity. "The Electronic Signatures in Global and National Commerce Act of 2000" has given digital signatures the same legal status as those of handwritten signature. Laudon & Laudon rightly observes: "For an electronic signature to be legally binding in Court, someone must be able to verify that the signature actually belongs to whosoever sent the data and that data were not altered after being signed."

Some legal experts assert that digital signatures, when used properly, are more trustworthy than handwritten signatures because of the use of the 'message digest' which provides strong evidence that the original document has not been altered since the signature was made (Watt-Morse). The detection of changes made to the content of a digital document is only possible when special data is generated and linked to the digital document. These data are technically called "Electronic Signature" (or Advanced Electronic Signature, in some specific cases) as it is defined in the Special Law 59/2003 on Electronic Signature that adopts the European Directive 1999/93/EC on the same matter.

Unfortunately, the digitisation of handwritten signatures is not a feasible solution due to the ease with which digital data

-Dr. Madan Lal Bhasin

The author is Head of Accounting Department at Mazoon College for Management, Muscat. He can be reached at madan.bhasin@rediffmail.com

An 'electronic' signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. Electronic signatures, therefore, can be used to sign emails, making the electronic documents legally equivalent to documents with a handwritten signature. The author has contrasted handwritten and digital signatures, and provided explanation of digital and electronic signatures. Further, the author has analysed the legal regulation on electronic signature at the European and International level, from the International Model Law proposed by the UNCITRAL to the European Union Directive. The article further aims to compare the legal experiences at both levels on this matter in France and Germany.

can be copied and duplicated. The delivery of electronic legal agreements on the Internet is typically via 'electronic' form, with a delivered statement that the user (signer) 'reads' and "clicks" on an "I Accept" button. However, this type of agreement has been upheld in a few Court cases. Greenstein and Feinman cautions the user's here as: "The clicking of an 'I Accept' button is not considered to be a sufficient legal signature by many members of the legal profession because it lacks some 'formal' requirements necessary for a signature to be enforceable in a Court of law, especially for negotiated contracts that may be reasonably expected to go through a few iterations of revisions before final signing".

Computer programs nowadays are entering into another form of electronic contract called "electronic or intelligent" agent. Here, the computer-programmed agents are essentially 'authorised' to contract on behalf of the party owning and operating the program. The general guidelines for laws governing commercial transactions are set forth in the US' "Uniform Commercial Code (UCC)." A recent effort to upgrade the UCC to bring it into the digital age is the proposal of a new article, Article 2B (see: http://www.law.upenn.edu/library/ulc/ulc.html for a draft of Article 2B). Article 2B proposes guidelines for contracts formed and entered into by electronic agents.

The American Bar Association (ABA), in "Digital Signatures Guidelines," discusses the following important attributes of signatures:

- ***Signer authentication:*** A signature should indicate who signed a document, message or record, and should be difficult for another person to produce without authorisation;
- ***Document authentication:*** A signature should identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection;
- ***Affirmative act:*** The affixing of the signature should be an affirmative act which serves the ceremonial and approval functions of a signature and establishes the sense of having legally consummated a transaction; and
- ***Efficiency:*** Optimally, a signature and its creation and verification process should provide the greatest possible assurance of both signer authenticity and document authenticity, with the least possible expenditure of resources.

The ABA, however, contends that the use of digital signatures, when performed correctly, not only meets these attributes, but it can surpass the handwritten signatures on paper technology. There cannot be "one-single" signature for all documents; each document needs a different signature. Each electronic signature must be created from a set of data only known to the author of the signature while the verification process requires the original document, the signature, plus some data available to the verifier. A digital certificate system uses a 'trusted' third party, known as a certificate authority, to validate a user's identity. Thus, digital signatures and digital certificates help with authentication.

Meaning and Scope of Digital and Electronic Signatures

Digital signatures take the concept of traditional paper-based signing and turn it into a digital "fingerprint". This fingerprint (or 'coded' message) is unique to both the document and the signer. The digital signature ensures that the signatory is indeed the originator of the message. Any changes made to the document after it was signed invalidate the signature, thereby protecting against forgery. Digital signatures, therefore, help organisations sustain signer authenticity, accountability, data integrity and non-repudiation of documents and transactions. For example, in traditional payment methods, a signature is often the legal proof that the consumer did indeed agree to the payment. In the electronic world, however, it is difficult to sign a document that is not printed anywhere. That is where digital signatures come into play.

The digital signature ensures that the signatory is indeed the originator of the message. Any changes made to the document after it was signed invalidate the signature, thereby protecting against forgery. Digital signatures, therefore, help organisations sustain signer authenticity, accountability.

According to Slyke and Belanger (2004) "A digital signa-

ture is a 'unique' code attached to an electronically transmitted message that identifies the sender." This unique code (called a 'hash') is generated through the 'encryption' techniques. Digital signatures use 'public key' cryptography to generate a number (the hash or message digest) based on the document that is being sent. The document and the hash are, therefore, closely linked. If either the document or the generated number is altered, they will not match and it will not be possible to open the document. The hash is very secure because once it is generated; it is encrypted using the user's 'private' key. Only the user's 'public' key can then be used to decrypt the hash. The decrypted hash and the hash generated by the user's public key are then compared at the receiving end, and if they match, the user did indeed "sign" this document (see Figure-1: How to Use Digital Signature). Since in theory, only the sender has the access to the 'private' key, only he or she can sign a document with it. Many governments across the globe now recognise digital signatures as legally binding.

It may be noted here that the terms "digital signature" and "electronic signatures" are usually used interchangeably, unless the context specifies otherwise. Unfortunately, these terms themselves have created considerable confusion. Thus, for purposes of this paper, we will define these terms as most commentators have:

- "Electronic signature" is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can "sign" an electronic record. Although all electronic signatures are represented digitally (i.e., as a series of ones and zeros), they can take many forms and can be created by many different technologies.

  Examples of electronic signatures include: a name typed at the end of an e-mail message by the sender; a digitised image of a handwritten signature that is attached to an electronic document (sometimes created via a biometrics-based technology called signature dynamics); a secret code or PIN (such as that used with ATM cards and credit cards) to identify the sender to the recipient; a code or "handle" that the sender of a message uses to identify himself; a unique biometrics-based identifier, such as a fingerprint or a retinal scan; and a digital signature (created through the use of public key cryptography).
- "Digital signature" is simply a term for one technology-specific type of electronic signature. It involves the use of public key cryptography to sign a message, and is perhaps the one type of electronic signature that has generated the most business and technical efforts, as well as legislative responses.

The United Nations Commission on International Trade Law (UNCITRAL) finally, adopted a "Model Law on Electronic Signatures" in 2001 (see details at www.uncitral.org). The Model Law aims at bringing additional legal certainty regarding the use of electronic signatures. It follows a technology-neutral approach and avoids favouring the use of any specific technical product. It is worth noting here that legislation based on the UNCITRAL model have been adopted in several countries, including: Australia, Bermuda, Colombia, France, Hong Kong Special Administrative Region of China, Mexico, Ireland, Philippines. Similarly, the United States legislation is also based on the minimalist approach of the UNCITRAL model in "US Electronic Signatures in Global and National Commerce Act (E-SIGN)" Public Law 106-229 (2000). "The Federal Electronic Signatures in Global and National Commerce Act, 2000" declares the validity of electronic signatures for inter-state and international commerce. The European Union, however, has taken a somewhat different approach (also known as "community framework") under "EU Electronic Signatures Directive, 1999" (visit for details at www.europa.eu.int). The Directive emphasises the principle of 'technology neutrality' and prohibits Member States from imposing a 'licensing' requirement. Many countries have adopted or proposed e-signature laws that are too regulatory, denying potential companies the flexibility that e-commerce requires. For example, the Russian Electronic Digital Signature Law that took effect in January 2002 establishes encryption as the only method whereby a valid electronic digital signature may be created under Russian law. The law is drafted to internationally omit other analogues of personal signatures and exclude the use of other technologies for electronic digital signature creation (see details at www.bmck.com/ecommerece/Russia). The Argentine law provides for the creation of a Federal Digital Signature Infrastructure consisting of an Application Authority, a Pub-

lic Key Infrastructure Advisory Commission, a Digital Signature Administrator Institution; Licensed Certification Authority, etc. (see details at www.pki.gov.ar). We are, however, going to survey briefly the International and European legal scenarios, with specific reference to 'electronic signatures' in the forthcoming sections of the article.

The International Model Law Proposed by UNCITRAL

The elimination of physical borders, as a result of the way information and digital technologies are developing today, is accelerating the sharing and exchange of information between people who are conducting their business in different nations and who often move and work in different regulatory environments. The need to define the legal relationships arising out of the meeting of the 'wills' of two parties located in different nations gives rise to a series of problems related to the decisions as to which body of law should regulate the validity of transactions conducted electronically and hence, the legal relationships arising as a result thereof.

"The rapid spread of modern technologies of electronic commerce and data authentication under the 'divergent' legislation drafted by different countries in matters of electronic signature has created some obstacles to the practical use of certification and electronic commerce tools," remarks Bertin. With the express purpose of 'harmonising' the variety of legislation governing electronic signature to be found on the international scene, the "United Nations Commission on International Trade Law (UNCITRAL)" drafted a 'Model' Law, which aims to create a 'uniform' worldwide regulation of electronic and digital signatures (visit official Website http://www.uncitral.org).

On 5 July 2001, the Assembly General of the United Nations adopted the UNCITRAL "Model Law on Electronic Signatures" and recommended it for the adoption by all the Member States. Based on the Model Law proposed in 1996 for standardising legislation on electronic commerce internationally, it aims to introduce uniform legislation on electronic signature in an attempt to increase the level of 'harmonisation' of national legislation regulating the legal relationships arising from and developed on the Web. The main purpose, as defined by the Commission, is "to promote the international standardisation of legislation applicable to the transmission and safeguarding of data transmitted over the Internet." In various international organisations, States have constantly and unanimously voiced their opinion that the creation of a uniform model, which is easy to incorporate into each State's legal system, would facilitate economic and commercial growth in general. Moreover, the adoption of a uniform legislation would make electronic commerce possible (or at least easier to conduct) since the Model Law sets out uniform criteria for the drafting of legislation on electronic commerce and digital signature.

The Article 7 of the UNCITRAL "Model Law on Electronic Signatures" clearly shows the option proposed by international bodies. It formulates a 'new' approach to the recognition of the legal 'effectiveness' of electronic signature—technological "neutrality". International legislation, in fact, provides for the adoption of the functional 'equivalent' approach. This legislative option (new on the international and European scene) aims to avoid attributing a priori legal validity to any 'single' electronic signature technology, and allows for the viability of the replacement of "handwritten signatures" with "electronic signature" to be tested on a case-by-case basis. Similarly, in Article 3, it establishes the principle of technological neutrality for the different electronic signatures and also states that no provision of the Model Law should be interpreted in such a way as to limit or deprive of legal effectiveness to any particular electronic signature technique. At the same time, the international proposal defines the 'requirements' an electronic signature should meet for the legal effects of a document signed with it to be recognised.

The legislative bill drafted by UNCITRAL enables an electronic signature to be defined as valid and effective when it enables the issuer to be identified, regardless of the technology used, and at the same time, guarantees the authority of the content of the electronically signed message. In other words, it enables whatever is contained in the document and any subsequent modifications to be reliably attributed to the signatory of that document. The law also establishes a further control aimed at checking the reliability of any particular technique used to sign the document against the requirements set out by the law to ensure its legal effectiveness. However, international legislation grants ample leeway to the contractual

freedom of the parties involved and allows each party to establish evaluation criteria for the legal effectiveness of signature, different from those set out in the Model Law. In fact, the Model Law itself establishes that any electronic signature used, regardless of whether it conforms to the technical reliability criteria set out in that law must comply with specific legislation which regulates and defines the nature of the transaction involved and its consequent legal effectiveness.

To support the international legislators' 'new' approach, the proposal presented by UNCITRAL adopts a multi-tiered approach when defining the requirements of electronic signatures and the legal validity of the documents signed.

The approach favoured by the international legislator adopting the principle of technological neutrality aims to promote free competition in the electronic signature technologies market. It is hoped that it would bring about an increase in the amount of 'certified' information circulating on the Web. The harmonisation of legislation regulating electronic commerce and signature should serve to create more 'trust' in users and to facilitate the conclusion of 'online' contracts. The use of electronic signature should give rise to a 'qualitative' and 'quantitative' improvement in relations between the citisens, and local (or even international) government bodies in the near future, especially if national regulations are harmonised.

To support the international legislator's 'new' approach, the proposal presented by UNCITRAL adopts a multi-tiered approach when defining the requirements of electronic signatures and the legal validity of the documents signed. The model effectively encourages States not to attribute legal effectiveness to 'one-single' type of electronic signature but rather to recognise the legal validity of a 'wide-range' of electronic signatures. By allowing the parties involved to attribute legal effectiveness to certain signature tools (even though they do not provide the minimum standards of security prescribed by law) the bill is a clear reflection of the decision to ensure maximum 'neutrality' and 'openness' with regard to the various technologies available. The Draft Uniform Rules on Electronic Signatures drawn by the UNCITRAL set out some precise criteria to States wishing to adopt the proposed Model Law on which many legislators around the world have based their rules. Community Directive 1999/93/CE is a typical example of the influence that this Model Law has had on the various regulatory systems for electronic signature worldwide.

The European Framework For Electronic Signatures

The 'Model Law' on Electronic Signatures has had a great influence on the rules adopted by various countries, but even prior to this it had been affecting European legislation on electronic signatures, which is largely based on the same criteria adopted by the international legislator in the Model Law. Directive 1999/93/EC (full text available at http://www.europa.eu.int) emerged after a long process of mediation and negotiation to decide on a European and Community reference framework for electronic signatures, with the specific purpose of encouraging its use in international transactions. For this reason the Directive sets out to harmonise current legislation on the matter throughout the Member States. In May 1998 the European Commission published the proposal for a European Parliament and Council Directive on a common framework for electronic signatures with the explicit purpose of ensuring the proper functioning of the internal market.

The Community Directive is based on the principle of technological neutrality already established by international legislators. The European legislators have decided to give users a "freehand" with regard to electronic data 'authentication' systems. The proposal aims to be practical and adaptable to the sudden changes imposed by scientific and technological development, while at the same time it seems to favour an anti-monopolistic legislation. For this reason, the result is a "compromise" between northern European countries, general preference for 'lightweight' signature regulation and the tendency of other States (such as France, Spain and Italy) towards legislative models, which tend to favour the use of 'strong' signature creation devices.

The Directive recognises and gives validity to two different types of electronic signatures—'simple' electronic signatures and 'advanced' electronic signatures. It distinguishes between

them depending on the security level required in terms of the integrity and source of the document. An advanced electronic signature in particular must be uniquely bound to the signatory, who in turn must be reliably identified. The Directive also establish, in accordance with UNCITRAL provisions, that such a signature must be created on electronic media over which the signatory can have exclusive control and be able to direct any modification subsequently made to that document.

The Community legislator, deviating slightly from the path taken by UNCITRAL, has made two corrections to the international approach proposed, one of a 'prescriptive' nature, the other of a 'minimalist' nature. In the prescriptive modification, the Directive requires Member States to grant legal effectiveness to advanced electronic signatures based on 'qualified' certificates generated by 'secure' signature creation devices. The other correction of a minimalist nature, asks States "not to deny legal validity to electronic signatures that do not comply with the minimum requirements laid down for advanced electronic signatures." Instead it asks States to give them the same validity, without prejudice, to their compliance with the provisions laid down in national legal systems regarding the legal effectiveness of transactions.

Community Directive and the Principle of Free Circulation of Certification Services

The Community Directive aims to create a common framework for the legal recognition of electronic signatures and to ensure the free circulation of 'certification' services, and of digital signature devices within the European Community. Moreover, it also aspires to open up the market for certifiers established in "non-community" countries, the only requirement being that of respecting the conditions laid down by the Directive in terms of safeguarding the security of data transmission. In accordance with these principles, the Community Directive does not oblige certifiers to obtain 'accreditation' from agencies specially set up for that purpose, neither does it require them to acquire any prior authorisation. In fact, the Directive puts limit on the number of electronic signatures that can be created in each Member States, with the purpose of encouraging free competition in the certification market so as not to hinder the entry of new technologies.

To borrow the words of Shipley, "The basic principle of not subjecting the provisions of certification services to any form of preventive authorisation effectively ensures a free market." To subordinate the market to any kind of authorisation would have meant effectively restricting the free circulation of services, which is expressly prohibited by the Treaty of Rome (full-text available at www.hri.org/docs/Rome57/). However, the Directive allows each Member States to introduce 'voluntary' accreditation systems with the aim of promoting technological and qualitative enhancement of security standards on the market, provided that access to that market is based on objective, transparent and proportionate criteria and not on discriminatory factors. In order to ensure the free circulation of services, the Directive obliges States "not to deny legal validity to electronic signatures a priori."

The principle established in Article 5.2 of the Directive is also applicable to certification providers operating outside the European Community. This Directive specifies the conditions under which qualified certificates issued by a certification service provider set up in a third country can be recognised as 'equivalent' to certificates issued by a certificate provider based in the European Community. Certificates issued by service providers established outside the European Community are considered to be 'equivalent' to Community certificates, provided that the certifier meets the requirements set out in Annex-II of the Directive and has been certified by a voluntary accreditation system set up by a European Union Member State, or if a certifier who resides in the Community and meets the requirements demanded by Annex-II of the Directive guarantees the certificate, that is, if the certificate or the certification service provider have been recognised by some prior agreement. Finally, with regard to the freedom to set up a certifier, candidates who reside in a Member State and wish to qualify as a certifier must abide by the conditions established in that country. Moreover, once qualified, a certifier can operate in any other country in the European Union.

Comparison Between Two Different European Models: Germany and France

Different Member States of European Union (EU) have adopted the European Directive in different ways. As stated earlier, Directives are instruments by which the EU can oblige Member States to move towards a

specific outcome—to regulate a specific manner in a uniform way (in this case the regulation of electronic signatures). But they leave individual States free to choose which methods to use and grant them a certain freedom to define which legal instruments to employ within the limitations imposed by the obligation to abide by common rules and the constant control exercised by the Commission. An attempt will be made here to summarise the two typical examples of litigation issued by Member States of the EU. Without claiming to be in any way exhaustive, we will attempt to establish the bases for a critical comparison between the two methods of legislative regulation of electronic signature based on the adaptation of the same Directive by Germany and France.

Unlike Germany, France waited for the Directive to come out before regulating electronic signature and responded to it by passing a law no. 230 dated 29 February 2000, which complied with the Directive.

The German Republic stole a march on the European Directive and the UNCITRAL project with a law dated 27 June 1997, with which the German legislator attempted to create a de facto standard enabling users to determine when a digital signature could be considered to be trustworthy. Later, the German government issued a 'decree' enacting previous legislation, which established the minimum requirements that certification authorities must satisfy in order to provide certification services, and the responsibilities and liabilities they are subject to.

This regulation, which clearly conflicts with the provisions of the European Directive 1999/93/CE, was revised in May 2001 in order to bring German rules in line with the European legislation. The German legal system chose to comply with the Directive by promulgating the "Gesets sur digitalen Signature" (visit for details www.netlaw.it) in which there is no mention of the 'equivalence' between electronic signatures and handwritten signatures. Later, the German legislators decided to make a direct modification of the Civil Code to define the equivalence between handwritten signatures and electronic ones. This addition to the Civil Code is essential to ensure the effectiveness of any legislation on electronic signature.

The German legislation has set up a 'voluntary' accreditation system. Accreditation is handled by State body "TeleTrust", and certification is obtained by means of an administrative procedure, which after a rigorous centralised control leads to the adoption of an administrative 'deed' validating the advanced electronic signature of system seeking accreditation. The German law also permits foreign certification service providers to use the State accreditation system. Once authorised, certifiers are allowed to issue both 'qualified' electronic signatures and 'weak' electronic signatures.

Unlike Germany, France waited for the Directive to come out before regulating electronic signature and responded to it by passing a law no. 230 dated 29 February 2000, which complied with the Directive. This law seeks to include amendments to adopt the "law of evidence" to information technologies and electronic signatures (see details at www.journal-officiel.gouv.fr). The French legislation, however, stands out in the European landscape for comprising only six Articles, which directly modify the provisions of French Civil Code (particularly Article 1316). The new Article 1316 provides that "documentary evidence or written proof is the result of a succession of characters, figures or other signs or symbols having an intelligible meaning, regardless of the medium supporting them or their means of transmission."

In accordance with the provisions of the Directive, the French law expressly states that electronic signatures have full legal validity, and that in the event of a conflict between evidence signed with a 'holographic' signature and another signed with a 'digital' signature, the prevalence of one over the other is to be at the sole discretion of the Judge. France has also privatised methods of electronic validation by means of a legislative provision (Law no. 650 of July 1996 on telecommunications) passed in 1996. This totally new provision was ahead of its time. It followed the principles expressed by international and Community standards at least four years before those standards came out. The French legislator regulated electronic signature by applying article 1316.4 of the Civil Code on electronic signature, which by means of a decree issued by the State Council establishes the parameters required to be able to give legal effectiveness to electronic signature.

This brief comparison between two different legislations on

electronic signature clearly shows how the European Directive has been adopted in different ways by the legal systems of different countries. Approaches range from the strength of the German "security" to the more "liberal" system introduced by the French legislator, even before the European Directive established the same principle. These cases are no more than symptomatic examples of the diversity of legislation in the global landscape.

Conclusion

Traditionally, legal agreements have been made in a written, hardcopy format that bears the handwritten or equivalent (such as, thumb or footprint) signatures of the parties involved. However, transactions conducted on the Internet typically occur in 'real-time'. The process of utilising hardcopy agreements negates many of the desired attributes of electronic commerce, such as, speed of transacting and reduced paperwork. Thus, new methods of delivering enforceable legal agreements/contracts and producing valid signatures in a digital format are necessary for more aspects of completing electronic sales transactions. Government should cooperate and make necessary changes, so that a single commonly acceptable electronic/digital signature suffices for a person just as a manual signature.

The elimination of borders, as a result of the way information and digital technologies are developing today, is accelerating the sharing and exchange of information between people who are conducting their business in multiple countries having completely different legal environments. Governments and policy experts, however, have grappled with ways to provide 'certainty' and trust' to businesses and citizens engaging in transactions online. One solution that has received considerable attention is the adoption of "electronic signature" or "digital signature" laws. In many countries, therefore, policy makers seeking to promote e-commerce and e-government have given priority to enactment of laws intended to create a legal basis for the use and acceptance of electronic or digital signatures. Over the last 5 to 7 years, approximately 50 countries have adopted laws or executive decrees on electronic or digital signatures, and others have them under consideration. A number of these laws anticipate complicated systems of "public key infrastructures" and "certificate authorities" that are expected to manage the technology for creating cryptographically-based digital signatures. Some involve government licensing. Some provide that only signatures made with government-approved technology will be recognised as binding. Deluge of reports, journal articles and news stories predicting that electronic signature legislation will revolutionise business practices and promote electronic commerce have accompanied the adoption of these laws.

The rapid spread of modern technologies of electronic commerce and data authentication under the divergent legislation drafted by different countries, in matters of electronic signature, however, has created some obstacles to the practical use of 'certification' and electronic commerce tools. With the express purpose of 'harmonising' the variety of legislation governing electronic signature to be found on the international scene, the United Nations Commission on International TRAde Law (UNCITRAL) drafted a 'Model' Law, which aims to create a uniform worldwide regulation of electronic and digital signatures. It is worthwhile to mention here that the national laws of most EU countries, defines an "electronic signature" in exactly the same wordings as the Directive. However, some countries did not literally take over the definition of the Directive, but specified the term "authentication" or specified the functions of an electronic signature. The primary aim of the EU Directive was to create a Community framework for the use of electronic signatures, allowing for the free cross-border flow of products and provision of services, together with a basic legal recognition of electronic signatures throughout the EU. This objective has clearly not entirely been met. However, this negative situation is not necessarily the fault of the Directive but rather due to the way in which it has been implemented by the Member States. Some of the Directive's provisions seem to have been, in part, misunderstood and the Member States, when transposing the Directive into national legislation, have not always taken the European perspective of the new regulatory framework into account.

As per June 2004 study, titled as "The Legal and Market Aspects of Electronic Signatures in EU," reported by Baker and McKensie concludes: "The study team discovered that many of the non-EU countries surveyed have based their own electronic signatures and delivery of signature related services legislation on that of the EU Directive. From a technical point of

view the Directive has even influenced international standardisation initiatives, such as the IETF standardisation work on Qualified Certificates. It is clear that the Directive has influenced legal and technical activities outside of the European Union boundaries. Remarkably, new terminology introduced by the Directive (especially Qualified Certificate, Advanced Electronic Signature, Certification Service Provider, etc.) has been taken on board by the EEA countries, Switzerland, the Accession and the Candidate countries."

Differences between the legislations of Member States and excessively formal procedure adopted by the German legislator is an obstacle to the freedom of establishment of certification authorities, and the free circulation of electronic signatures on an international scale. The legislative and technical difficulties are in danger of affecting the proper functioning of the very legal and economic relationships that the introduction of electronic signature is supposed to improve.

Like any other tools aimed at ensuring the authenticity and authorship of a declaration via the use of modern information technologies, electronic signature can validly be used by private individuals for the signature of documents and important transactions between parties, and also in relations between citizens and both national and international government bodies. The use of modern techniques for the authentication of documents should make it possible to remove existing obstacles to the free circulation of people and capital, which are founding principles of the European Union. At the same time, the assurance provided by national, as well as, international constitutional law recognises the need for a closer link and more intense dialogue between citizens and their governments, with a consequent enhancement of information exchange. However, these principles could be put into practice by the rational use of new technologies.

A closer contact between international governments and individual citizens would considerably reduce the democratic deficit evidenced by deliberative and legislative bodies at a Community and international level. In order to do this, we need for countries to have a uniform legislation, along with a determined move at an international level towards a real implementation of the principles of technological and functional neutrality and compatibility between signature creation devices. To do this, we require the coordinated and cooperative efforts of all the institutions at a national and an international level in order to draft regulations, which can adapt to the ongoing evolution of technological developments. We are hopeful that the use of electronic and digital signatures will lead to a quantum jump in electronic commerce transactions, as it addresses the concerns of the transacting parties as to the confidentiality, integrity, authenticity and non-repudiation, thereby boosting 'trust'.

Figure-1: How to Use Digital Signature