Journal of Information, Law and Technology

Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication

Christina Spyrelli
Law School
University of Strathclyde
christina.spyrelli@strath.ac.uk <mailto:christina.spyrelli@strath.ac.uk>
christina.spyrelli@oftel.gov.uk <mailto:christina.spyrelli@oftel.gov.uk>
christine77us@yahoo.com <mailto:christine77us@yahoo.com>

This is a **refereed** article published on: 16 August 2002

Citation: Spyrelli, C, 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication', *The Journal of Information, Law and Technology (JILT)* 2002(2) <http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html>

Abstract

The security in the electronic transactions over the Internet is regarded as one of the most crucial issues in the digital world. Since 1996, both international and supranational organisations on governmental and business level have been trying to promote the use of electronic signatures in the electronic commerce and set forth a common legal framework for electronic authentication over the Internet.

In particular, this article will deal with the current technology used for electronic authentication and the international approaches towards electronic signatures. It will critically analyse and compare the EU Directive on electronic signatures (1999) and the US E-Sign Act (2000). In addition, it will assess the transatlantic co-operation on both governmental and business level in relation to the creation NOTICEof a secure and user-friendly platform for electronic transactions. The paper concludes with a discussion of the legislative measures taken by the EU and the USA and the possibility of the achievement of a common global consensus on electronic authentication.

Keywords: Electronic signatures, Digital signatures, Directive on electronic signatures, E- Sign Act, digital approach, two-tier approach, minimalist approach, electronic authentication, e-commerce, Identrus, TABD.

1. Introduction

Electronic commerce is considered to be the key to the development of a promising global digital economy. It is estimated that $30 billion worth of transactions took place over the Internet in 2000 and according to really impressive forecasts, the business to business (B2B) and the business to consumer (B2C) e-commerce will triple from $500 billion in 2000 to $1.6 trillion in 2003**(1)**.

Although these predictions are high, the nature of the Internet as an open network and the globalisation of the economy- with the USA being the pioneer**(2)** - produces legal issues concerning security and electronic authentication of transactions over the Internet. Both businesses and consumers are reluctant to get involved in an electronic transaction because the present legal framework does not offer the necessary guarantees for a trustworthy and secure online commerce. Therefore, the security issues need to be addressed, not only on a national level but also and most importantly on an international one in order for the e-commerce to proliferate.

This paper attempts to explain the existing security methods of electronic transactions, in particular the e-signatures, and study, based on international initiatives that have taken place in order to promote and establish a reliable environment for e-transactions, the legislative measures taken both by EU and USA and their continuous co-operation towards a common legal platform on electronic authentication.

2. Electronic Signatures

2.1 What is an E-signature? Forms of E-signatures

International bodies, organisations and countries have adopted different definitions of e-signatures. In essence, e- signatures are computer-based personal identities. They can take on a simple form, like bitmap signatures which are scanned images of handwritten signatures onto a document, or an advanced one, like the biometric signatures (e.g iris scan) which require a special writing pad that records strokes and pressure**(3)**. The most advanced and widely used form of e-signature is the digital signature, which is founded on the public key cryptographic method.

2.2 Functions of Digital Signatures

The basic characteristic of this secure encryption technology is that two different but mathematically related keys, the private and the public key (the so called 'key pair'), are used in order to create a digital signature and encode the data and to verify the signature and decode the data. In practical terms, the sender of an e-document can sign it by using his private key, which must be kept secret. Thus, the signature can only be verified with the public key of the sender, which is available to the public. A process strongly associated with the public key encryption and applied both in creation and verification of a digital signature is the hash function, which when applied to a particular message creates a unique number in the form of a hash value (message digest)**(4)**.

An example could illustrate the whole process. Assume Christina (sender) wants to send a message to Catherine (recipient) over the Internet:

- ►Christina creates a key pair**(5)** keeping one key private and making the other key widely known.
- ►Having written her message, Christina uses the 'hash function' of her encryption software to generate the 'message digest'.
- ►Christina, then, enciphers the message digest with her private key. The enciphered message digest, which is sent to Catherine with the original message, is Christina's digital signature for that message.
- ►Catherine can decipher the message digest, only if she uses Christina's public key, and thereby she can verify that Christina sent the message, assuming that the public key is correctly associated with Christina. She can also verify the integrity of the message by creating her own message digest of the message and comparing it to Christina's deciphered message digest. If the two message digests are identical, the integrity of the message is confirmed**(6)**.

Thus, the process of creating, using and verifying a digital signature provides important functions for legal purposes**(7)**.

Firstly, the asymmetric cryptography (PKI) ensures a high level of security in e-communications and of confidentiality of the context of a message sent over an open network like Internet.

Secondly, digital signatures provide authentication of the identity of the signer by attributing the message to the signer; so it is known who participated in a transaction. The rationale of this function is based on the fact that digital signatures cannot easily be forged, unless the signer loses control of his private key either accidentally or intentionally.

Thirdly, the digital signature protects the integrity of the transmitted data so the recipient can be sure that comparing the two message digests has not altered the message.
Even though these functions of digital signatures can guarantee security over open networks and strengthen consumer trust in e-commerce, another challenge needs to be drastically confronted. At a late time, how can it be proved who participated in a particular transaction, so that it cannot be denied who the sender and the recipient of the data was? In other words, how secure is the security provided by digital signatures?

2.3 Trusted Third Parties (TTPs)

In order to answer the aforementioned question, it must be kept in mind that the 'key pair' has no inherited connection with any person; it is simply a pair of numbers. Hence, there are two ways to associate a particular identity with a key pair and, consequently, to prove beyond any doubt, the existence of this association, the identity of the signer and the integrity of the message in order to prevent a party from denying the origin, submission or delivery of the message and the integrity of its contents:

When there is a prior contractual or even friendly relationship or when the parties transact over a closed network (e.g EDI), each party can simply communicate the public key of the key pair each party will use.

However, as e-commerce moves from a bilateral level to a multilateral one of the www on the Internet, where most of transactions occur among strangers who usually have no prior contractual relationship and will probably never deal with each other again, the authentication procedure is not a simple task. Therefore, in this case the **non-repudiation** of digital signatures (the last and most crucial function) can be guaranteed by the involvement of TTPs, the certification authorities (CAs)**(8)**.

The C.As issue a certificate, which attributes explicitly a public key to a specific identity and, according to the level of inquiry used to confirm the identity of the subject of the certificate; there are several types of certificates (e.g the identification, the time stamp)**(9)**.

Furthermore, in order to assure in the most efficient way the authenticity of the identity and the context of the certificate, the C.A digitally signs it. As it is essential for both parties who use different C.As to trust each other's authority, there are some methods of certifying the C.A's identity and the authenticity of the issued certificate (self-certification, cross-certification and root C.A)**(10)**.

In reference to the functions of digital signatures, the use of this technology in relation to TTPs is currently the most efficient system of establishing a secure and user-friendly environment of e-transactions and reinforcing both businesses and consumers trust on e-

commerce.

2.4 Benefits of Electronic Signatures

Not only commercial but also non-commercial entities benefit from the implementation of e-signatures- especially digital signatures- in e-commerce.

First of all, as far as B2B and B2C e-commerce is concerned, e-signatures can offer greater security, reliability and transparency in e-transactions by minimizing the risk of dealing with frauds, or persons who attempt to escape responsibility by claiming to have been impersonated. In particular, digital signatures can satisfy the need of message integrity by preventing unauthorized access to data, detecting any message tampering and diminishing the danger of false claims that data was changed after it was sent. Therefore open network systems can be gratified with efficiency in data interchanges among businesses and cost-effective and safe information gathering respecting consumers right of online privacy**(11)**. In addition, when an e-contract is digitally signed, the formal legal requirements (writing, originality of signature and of document) are satisfied, since digital signatures are functionally equivalent to paper forms.

Furthermore, e-signatures, if properly utilised in the public sector**(12)**, can assure a high quality of security and transparency in dealings with the public as they can guarantee time and cost-efficiency in the bureaucratic procedures by facilitating the handle, process, storage and transmission of data. The first e-signed international governmental document at APEC meeting (1998) and the digitally signed US-Ireland communiqué on e-commerce (1998) were the predictors of a future global e-governmental structure.

Therefore, the benefits of e-signatures cannot be less recognised and ratified by international organisations, which constantly scrutinize any possible scenario in order to meet the requirements for a legally harmonized e-authentication system. The following international approaches towards e-signatures legislation and some of the most important initiatives on accreditation, certification and standardisation of e-signatures are regarded as the foundation stone of the EU Directive on E-Signatures (1999) and the US 'E-Sign Act'(2000).

3. International Activity(13)

Over the past few years, many regulatory initiatives have taken place and, much as they reflect different assumptions on e-signatures legal status and future, they can be classified into three categories:

3.1 The Minimalist Approach

This approach, which is adopted by the USA (4.2), aims at the uniform use, recognition and enforceability of e-signatures**(14)** and e-records by removing existing legal obstacles from online commerce, avoiding new regulations and by establishing a technology-neutral status. One of the most demonstrative minimalist initiatives is the UNCITRAL Model Law on Electronic Commerce which deals with the functions of e-signatures and

their binding power and recognises full legal validity to specific digitally produced and signed documents (Article 7)**(15)**. In addition, OECD sharing the same minimalist view as the UNCITRAL, set forth the following principles with the intention to foster confidence in information and communications infrastructures and to facilitate international e-trade by promoting cost-effective, interoperable and portable cryptographic systems**(16)**:

- Trust in cryptographic methods;
- Choice of cryptographic methods;
- Market driven development of cryptographic methods;
- Technical standards for cryptographic methods developed at a national and international level;
- Protection of privacy and personal data;
- Lawful access to encrypted data;
- Contractual or legislative liability of the Cryptography Service Providers (CSPs);
- International co-operation on cryptography policies.

Based on the OECD Guidelines and the Ottawa Ministerial Declaration**(17)** for a non-discriminatory and legally interoperable use of e-authentication technologies the Joint OECD-Private Sector Workshop**(18)** acknowledged the disparities of business models and governmental policies on e-signatures and underlined the importance of data integrity and security on the Internet and the demand for a trustworthy and less regulated authentication system.

3.2 The Digital Signature Approach

This is a prescriptive approach as it focuses solely on the establishment of a legal framework for the operation of digital signatures as well as of a reflection of formal requirements applicable in the offline transactions. International regulations under this approach adopt the PKI as the approved technology of generating e-signatures, impose certain operational and financial requirements on C.As, prescribe the liability of key holders and define the circumstances under which reliance on an e-signature is justified. ABA-Digital Signature Guidelines**(19)** and EU-wide standardisation initiative (EESSI) **(20)** are characteristic examples of this approach. Both regulations are not mandatory and, in fact, the European initiative appears to be more flexible than the American one regarding the supervisory bodies, as the EESSI report offers two options to the Member States: either voluntary self-certification schemes or governmental licensing schemes.

These initiatives aim at ensuring that digital signatures can fulfill in the most reliable way the requirements of identification, authentication and non-repudiation in e-transactions. However, they are obsolete as their spectrum is solely focused on either the digital signature technology as a technical baseline by means of a legal instrument or on legislation, which regulates digital signatures in order to equate them legally to hand-written ones, or on the structure of C.As and the use of qualified certificates in connection with digital signature applications**(21)**.

3.3 The Two-tier Approach

The objective of this 'hybrid' method, which is adopted by the EU (3.1), is to provide time-resistant regulations by setting requirements for e-authentication methods with a certain minimum legal power (minimalist approach) and by attributing greater legal effect to certain widely used techniques (digital signature approach). In contrast to the prescriptive approach, the two-tier approach does not specify only one technology but leaves room for future technologies to develop and comply with extra requirements as well**(22)**.

The UNCITRAL Model Law on Electronic Signatures**(23)**, which adopted this approach, promotes the progressive harmonization and unification of measures and policies on e-signature issues. Although this Model Law does not provide a clear definition of digital signatures, it is obvious that this authentication method is included in Article 6(3); in addition, under the provisions of Article 6(1,2) when a document is **digitally** signed, it is legally valid as a hand-written signed document. Moreover, under Article 3 new technological developments are more than welcome, as it proclaims equal treatment of signature technologies, and in relation to Article 5, the importance of market driven initiatives is recognised. Articles 8-11 set strict liabilities of CSPs, signatories and relying parties in order to establish a reliable and fair global authentication system. Furthermore, the Model law provides that the legal efficacy of foreign certificates and e-signatures in the Member States depends on their level of reliability, which is determined either by international standards or by the contractual agreement between the parties.

The advantage of this approach is that not only does it provide legal neutrality by recognising most of the authentication technologies but also it defines a more innovative legal environment by ratifying the freedom of choice regarding authentication systems. The aforementioned shows that no matter how welcome the two-tier approach is, there is still a wide divergence of international policies which could limit the uniform recognition and the interoperability of e-signatures and e-records with disastrous impacts on the emerging digital market.

3.4 Overview

In reference to the diverse approaches towards e-authentication these international initiatives and policies highlight the significance of e-signatures in e-commerce. However, as market and technology are constantly developing and, thus, they are not yet clearly shaped, it seems that it would be rather unwise to either regulate on the basis of digital signatures or to set criteria, which only consider certain forms of e-signatures,

while leaving space for new technologies to emerge.

Both **digital signature approach and the two-tier one** are understandable, as they provide more legal certainty and security. However, they still focus too narrowly on signatures as such, and not on formal requirements as a whole.

On the other hand, the **minimalist approach** gives the opportunity for a uniform legislation on e-signatures based on internationally harmonised criteria to develop, as it focuses on the functions of signatures and the methods in which these functions can be translated into technological applications keeping a technology neutral profile**(24)**.

Taking into account this pluralistic international background, the EU and USA followed different approaches in their effort to regulate authentication in e-commerce. Taking this on board, hopefully some light can now be shed on the diversities between the EU Directive on E-Signatures and the US E-Sign Act and on the co-operation between EU and USA both on governmental and business level in order to develop a flexible and legally effective co-regulatory system of e-signatures with respect to international policies, market trends and consumers needs.

4. The EU and US Approach Towards Electronic Signatures

4.1 EU Directive on a Community Framework for Electronic Signatures (25)

Following the European Initiative in E-commerce**(26)** and as a result of the Bonn conference and the hearing in Copenhagen in 1998 the Commission realised the need for a uniform legal framework for e-signatures at a European level in order to avoid any inconsistencies in the internal market and to catch-up with the international action that has already been taken. The directive on e-signatures set the foundation stone for a secure environment in the online market, as its main objectives are to:

i. ‘Facilitate the use of e-signatures and to contribute to their legal recognition’;

ii. Harmonize the Member States regimes;

iii. Strengthen confidence in the e-signatures and iv. Provide a flexible scheme compatible with the international initiatives and competitive towards cross-border e-activities**(27)**.

The directive provides the legal framework for e-signatures and CSPs and defines two levels of security that organisations may apply to e-signatures depending on the sensitivity of the transaction**(28):**

a) The basic e-signatures which are used for the minimum level of transactions as a method of authentication; and

b) The advanced e-signatures which provide a higher level of security in comparison to the basic ones as long as they meet the requirements led in Article 2(2) of the directive.

Although the directive is not technologically orientated**(29)**, there is a strong suggestion of the digital signature technology under the provisions of Article 2(2b).

As far as **legal recognition** is concerned, the Directive provides a non-discriminatory approach towards e-signatures but it ensures that advanced e-signatures would fulfill national formal requirements, which will be linked to requirements for certificates, CSPs, and signature-creation devices**(30)**. It is obvious that Article 5 (1) refers to the digital signatures and for the time being the directive considers only digital signatures to be equivalent to handwritten ones whilst under Article 5(2) it is stated that e-signatures will not be denied enforceability and admissibility as evidence in legal proceedings simply on the grounds that they are in e-form. However, this legal recognition is limited as all contractual or other non-contractual obligations, where specific requirements of conclusion or validation under national or EU law have to be met, are excluded from the Directive's scope.
In terms of **market access**, Member States cannot subject the provision of e-signature services to mandatory licensing**(31)** but it is left to their discretion to introduce voluntary accreditation schemes, which have to be objective, transparent, non-discriminatory, and proportionate (Annex II). In addition, based on party autonomy and contractual freedom, schemes governed by private law agreements, such as corporate Intranets or banking systems, where a relation of trust already exists and there is no need for regulation, are permitted**(32)**.

Article 6 sets **liability rules** for CSPs, which are liable for damage caused to any entity discloses its data and reasonably relies on a qualified certificate (QC) issued by them, unless they can prove that they have not acted negligently. Finally, the Directive recognises **third countries certificates** as legally equivalent to certificates issued by CSPs in EU as long as there is a link with the EU (e.g voluntary accreditation in the EU) or there is a bilateral/multilateral agreement between the EU and the third countries (Article 7).

The two-tier approach the Directive adopts seems to be the best legal instrument in order to set the minimum requirements of secure e-transactions and converge different trends and policies among the Member States. Nonetheless, it is more focused on e-signatures and the requirements of CSPs than on the legal recognition and force of digitally signed contracts. The narrow scope (Article 1) of the Directive proves the strict regulatory character of EU on e-commerce and appears to be a regressive factor in the development of a competitive EU e-market. Therefore, it is not questionable why businesses are confused and still wait for a more liberal and less restricted regulation on e-signatures.

Furthermore, even though both E-signature and E-commerce**(33).** Directives underline that the expansion of e-commerce should be market-driven and any policy must take account of business realities, they do not clearly offer the lead to the private sector; no

matter how equally both models of state and self-regulation are promoted, the State is still the leader**(34)**.

Another crucial point of the Directive is that currently only digital signatures are fully legally equivalent to handwritten signatures and seals; as far as other forms of e-signatures are concerned, they are legally recognised but their binding power depends on the relevant provisions of each Member State's law. This point certainly adds obstacles in e-commerce instead of removing them, as it obliges businesses to follow a specific model of e-transaction and e-authentication, a practice against the principle of fair and free competition in the internal market, and it confines the technology industry in order to control its development on cryptographic methods. Finally, it is stated, 'it is important to strike a balance between consumer and business needs'**(35)** but the Directive defines in such detail the liability of CSPs without making a specific provision about the liability of certificate holders and any explicit reference on consumers right against CSPS which are usually banks and the bad banks record on consumer disputes is a common place.

With respect to the aforesaid, the Directive appears to be the starting point of promoting the implementation of e-signatures in Member States and not the backbone of the European aspect of e-authentication. In fact, the prospective of constant adjustment of the Directive to the needs of e-commerce was proved in the meeting of the European Forum on E-business**(36)**, which compared the different timescales, interpretations and implications of the Directive, so e-signatures can take a more solid form and a universal technical and legal standard to be adopted**(37)**.

4.2 Electronic Signatures in Global and National Commerce Act (E-Sign Act) (38)

Following the 'White House Paper'**(39)** on the importance of e-commerce and the adaptation of the 'Uniform Commercial Code' to cyberspace the US experience with e-signature laws passed through different stages (e.g prescriptive legislative approaches on national-ABA- or on state-Utah-level) to end up to the most recent ones which increase the reliability in e-transactions take care more of consumers. The first one is the UETA **(40)**, a model state law that has already been adopted by more than 22 states. This technology-neutral Act provides that:

a) e-signatures do meet signature requirements and are admissible in court proceedings;

b) e-contracts will be enforced; and

c) there will be no special treatment for specific technology but of course courts can take technology into account.

Even though this area is usually a case of state law, the US Congress has the authority to adopt legislation preempting state law. Therefore, the E-Sign Act, 'the most significant e-commerce legislation to pass in this session of Congress' **(41)**, was e-signed into law by President Clinton; the minimalist approach of the Act aims- mainly for political reasons-

to facilitate the use of e-signatures instead of establishing a specific technological protocol.
In terms of **scope**, the Act is applicable to contracts, agreements and records provided in or affecting interstate/foreign commerce, as well as those within the scope of the Securities Exchange Act of 1934**(42)**. In other words, in the 'E-Sign' era a consumer can apply electronically for a mortgage or a loan, can buy a car online, can open an online brokerage account or 'e-deal' with his/her insurance company**(43)**.

What constitutes an e-signature? Provided the wide definition (S.761, sec.106)**(44)** of e-signatures we can assume that an e-signature can be easily made by pressing a touch-tone keypad, clicking 'I agree' on a web page or typing our name at the bottom of e-mail**(45)**. In contrast to the EU directive (2.1), the minimalist Act focuses on verifying the intent of the signatory rather than on developing forms and guidelines. E-signatures, e-contracts and e-records are granted with equivalent legal validity and enforceability to traditional forms and handwritten signatures. Not only does it recognise the 'digital signatures technology' but also empowers the use of any type of technology in order to facilitate the online contracting. However, it is clearly stated that these provisions do not affect any other requirement than the one that a contract /record be written, signed or in non-electronic form**(46)**.

In addition, the Act establishes **voluntary use** of e-signatures/records through an opt-in system so that consumers, on one hand, choose freely any form of transaction (party autonomy) and, on the other hand, if they agree to transact online, affirm their intention electronically. The Act goes further on this matter by ensuring that companies will provide a 'clear and conspicuous statement' informing the future customer-prior to his/her consent- of any right to have a record in a non-electronic form and to withdraw consent and of the hardware and software requirements for access and retention of e-records (sec.101). As far as the consumer's consent is concerned, it has to be expressed in a way that 'reasonably demonstrates' that the consumer is able to access the information in the e-form, which will be used to provide the information that he/she is the subject of the consent. What constitutes a 'reasonable demonstration' that the consumer can access the information? How can this procedure be implemented in the real business world? Some believe that this provisional 'safeguard' might impose burdens on both the consumer and the company and that it does not take into account the rapid way technologies are developed. Furthermore, this 'conundrum' of consumer consents and verifications with respect to e-commerce never existed in the paper world and it is obvious that it rather confuses and intimidates consumers than creates a user-friendly e-environment for transactions**(47)**.

As far as the **Act's interaction with State E-Signature Laws** is concerned, it is provided (Sec 101,102) that a state may preempt the Act **only** by adopting a 'clean' version of UETA as approved and signed by the NCCUSL or by passing a technological neutral law. The E-Sign Act thus establishes uniform and nationwide standards of acceptance, while taking into consideration the interest of the States and at the same time covering the so-called 'UETA Sec 3(b)(4) loophole'**(48)**. In addition, as the Act's main objective is to create interoperable systems of e-contracting and support the global nature of e-commerce, it forestalls any prescriptive state law, such as the Utah e-signatures law. In

terms of **international validity of e-signatures**, the Act, consistent with the UNCITRAL Model Law on E-Commerce, removes paper-based obstacles to e-transactions and takes a non-discriminatory approach to e-signatures and authentication methods from other jurisdictions.
Comparing the EU Directive with the US Act, the importance that the Act attributes in practice to the private sector and to self-regulatory policies is easily attested; the Act offers the legal framework for reliable and secure e-transactions and at the same time it restricts undue governmental involvement in e-commerce as it abstains from setting up any mandatory scheme regarding e-signatures and certificates. Government's aim is to support and enforce a minimalist and interoperable legal platform for commerce.

Furthermore, the Act, through its technological neutrality, makes clear that there is not only a single technology or technique that can warranty safe online contracting, although the utility of digital signatures is widely recognised in US. In contrast to the EU directive, the Act neither focuses on a 'sole tree form the whole forest' nor provides only guidelines to be implemented by the States at their own discretion; it establishes in an efficient and modest way what R. Gates said about this law:' The new law sets up a framework for trust. The major change is this will provide a legal framework for doing things on the 'Net that heretofore didn't exist […]. As people try to deploy digital certificates as a way to provide more enforceability around things that happen over the Internet, you need a legal structure that still protects the same legal structure that protected them in the paper world'**(49)**.

The liberalised and nondiscriminatory market-driven approach of the Act towards e-signatures underlines the necessity of a technologically impartial and legally well-defined framework in order to meet the challenges of e-commerce. However, the Directive, following a more conservative pattern, cannot deny its strong regulatory character although it makes a respectful effort to promote a competitive and innovative scheme. Still a hesitation is visible. As the Directive struggles to balance between a state and self-driven scheme without offering a precise and practical solution both to governments and businesses, companies consider whether to take the initiative and promote e-signatures or not. Are they free to choose any form of e-signatures considering the fact that all e-signatures are not 'armed' with the same legal validity? Should the European national regimes change their attitude towards e-authentication (especially the prescriptive ones) and be more flexible and open-minded as far as e-signatures are concerned, whilst the context of the Directive is a little bit obscure as it is digital signature-friendly and it is not overall mandatory? In this case, does the discretion power of the Member States regarding the implementation of directives facilitate and promote the global and interoperable character of e-commerce or does it constitute an obstacle to any international effort of establishing uniformity of e-transactions?
Moreover, the US definition of e-signatures is broader and more defined than the EU one ('data in an e-form'); does the EU definition include any sounds and symbols like the US one or does it depend upon the European governments to interpret this provision according to international standards? However, if this is the case, who sets up these international principles and how mandatory can they be? In addition, what if each and every Member State- for political and profitable reasons- recognises and validates either different or exclusively specific forms of e-signatures? For example, Germany may

attribute legal enforceability only to digital signatures and digitally signed documents whilst Greece may accept any type of authentication technology.

Furthermore, this discussion does not consider the European 'voluntary' accreditation scheme of foreign certificates to be a good example of 'fair play' in the business world, when on the other side of the Atlantic a clear unbiased policy is established in respect to third countries certificates. In other words, any given European certificate will be fully recognised in the US but an American-originated certificate will be valid in the EU **only if** there is a link with the EU or a specific bilateral agreement. And what will happen if some Member States impose voluntary authentication schemes whereas others impose mandatory licensing? Easily guessing the businesses' preference and based on business world's axiom 'always balance cost against benefit' a CA's monopoly is going to flourish within the internal market and split the EU Member States into two camps: the innovative and legally flexible countries and the obsolete and legally sterilized ones. The time has come to think whether this European provision clears the way for businesses that want to convert rapidly and efficiently from paper-driven systems to an international online environment of transactions.
It is quite obvious that these inconsistencies can be effectively faced on a transnational level; not only US and EU government but also American and European business industries should, and in fact do, cooperate in order to create a uniform infrastructure that will spur the growth of a secure B2B and B2C e-commerce. The most illustrative examples of these initiatives are the TransAtlantic Business Dialogue (TABD) and the Identrus system.

4.3 EU-US Partnership on Governmental Level (TABD) (50)

In 1990, the USA and the EU (then the EC) and its Member States jointly declared their determination to strengthen their partnership further in order to 'promote market principles, reject protectionism, expand and further open the multilateral trading system **(51)**'. Due to the development of the Internet and the rapid expansion of e-commerce EU and US adopted the following guidelines**(52)** (in their Summits in 1997 and 2000): 1) e-commerce will be essentially market-led and driven by private initiative 2) government should just provide a clear, consistent and predictable legal framework, promote a pro-competitive environment in which e-commerce can flourish and ensure adequate consumer protection 3) industry self-regulation is important (e.g codes of conduct, model contracts, guidelines agreed between industry and other private sector bodies) in order to gain consumer confidence in e-commerce 4) unnecessary existing legal and regulatory barriers should be eliminated and the emergence of new ones should be prevented 5)…6) …and 7) interoperability, innovation and competition of e-authentication methods are important for the development of a global market place and, in this context, voluntary consensus-based standards, preferably at an international level, can play an important role.

Based on these principles, EU and US adopted a transatlantic agenda **(53)** in order to set up an action plan in respect to e-commerce, which will 'contribute to the creation of a New Transatlantic Marketplace by progressively eliminating barriers that hinder the flow of goods, services and capital between EU and US **(54)**'. This marketplace will be established on a confidence-building process as far as e-transactions are concerned and on

an agreement on mutual recognition of conformity assessment in respect to e-signatures. Furthermore, both EU and US, taking their own regulations and policies into consideration, cooperate in order to achieve the maximum technological transparency, regulatory harmonization, business participation and legal non-discrimination of authentication methods.

The TABD organisation attempts to bring EU and US governmental and legislative measures on e-signatures closer in order to standardise-at least on a transatlantic level- the legal requirements of validity of e-signatures. The most important role in this effort is played by the private sector and in particular by the Identrus.

4.4 Identrus (55)

In a move to reduce regulatory hurdles facing e-transactions, a global network for e-signature authentication was incorporated under US law in 1999. In fact, every financial institution that joins the Identrus system becomes an accredited CA that aims at enhancing a truly global and highly trusted B2B e-commerce. Although Identrus's international dimension is known, it is established on a joint European and American private-sector initiatives led by some financial institutions. The main goal of Identrus is to ensure authentication of the identity of the transacting parties, authorisation, confidentiality of communications, integrity of transmitted messages and non-repudiation of signatures over open networks and to guarantee an interoperable system of e-transacting based on uniform standards and beyond any legal divergences**(56)**.

At the beginning, the EU was unsure about this agreement but, a few months ago, it officially approved Identrus and laid the groundwork for the establishment of such services by granting financial institutions the right to operate as independent and competitive CA s with the intention to secure e-commerce transactions**(57)**. Currently, there are approximately 50 banks worldwide that have joined the Identrus.

In respect to these initiatives both on governmental and business level, which were actually launched before the adoption of the Directive on e-signatures and the E-Sign Act, it is quite surprising that European and American legislators did not cooperate in order to find a common way to deal with the legal challenges imposed by the online transactions. What is more inexplicable is the fact that both legislative bodies followed a different approach towards authentication methods. No matter how diverse the legal and the economic background of EU and USA is, there have been and still are in progress action plans led by both public and private sector in order to build a compatible-between EU and USA- legal environment. Still even in these initiatives the legislators were either unintentionally excluded or avoided any participation for reasons that are not really clear to all of us. It seems that the legislative power remains isolated from the real world and, whenever it decides to take the stand, it sets up regulations, which bewilder the market rather than smooth the way for a user-friendly and competitive e-commerce.

4.5 Deliberations Regarding EU and US E-signature Legislation Schemes

Even though the aforementioned initiatives attempt to solve the legal conundrum between EU and USA, lots of issues in relation to these e-signature statutes arise.

Political imperatives of catching cybercriminals and protecting consumers- connected with the fear of losing tax revenues online- push EU to over-regulate and thus stifle the growth of e-business. L.Davies comments:' A lot of consumer protection advocates want to regulate e-commerce out of all existence**(58)**'.

However, the 'laisser faire, laisser passer' approach of the USA-given the current state of authentication methods- puts consumers at risk and, according to M. Saunders, it contributes to the digital divide, the growing gap between those connected to the emerging e-commerce world and those disconnected or without the necessary skills to cope**(59)**. And the question remains: Who has the competitive advantage in e-commerce: the US companies or the EU consumers? Which approach is more effective and compatible with the needs of the Internet age?

Considering the lack of common international technical standards, the constant existence of security and fraud threat, the costs of implementation of e-signatures, the absence of a common legal base regarding cross-border transactions and the psychological pressure imposed on traditional consumers to be converted overnight into masters of online commerce, neither companies nor consumers are most benefited by the EU and US statutes. Still companies have to develop systems, which prove that their data has not been tampered with, that the signatures are accurate and that all parties are aware of the approved agreement. According to Kaplan opinion on the statue of e-signatures:' Businesses still have a significant responsibility to get their ducks in a row'**(60)**.

Nevertheless, as both EU Member States and US States have not yet adapted completely their national legislation to the provisions of the EU Directive (for the former) and of the 'E-Sign Act' (for the latter), there is an uncertainty concerning the legal status of e-signatures and of e-signed e-documents. Currently, most laws of evidence attribute fully legal power to the handwritten signatures on paper documents and most judges around the world are not that enthusiastic to change a well-established practice regarding the in court proof of any transaction. This means that, for the time being, in case of failure of the PC's system, of forgery of an e-authorization or of alteration of the context of an e-document, the legitimate consumer is liable to prove that he/she was victimised by fraudulent spending**(61)** or that his/her PC's software collapsed. As both the Directive and the Act do not limit the consumers liability in these cases, it is quite difficult for the user to prove the invalidity of a signature which is supported by a certificate issued by an accredited CA; and this is disturbing given the banks-which are usually the CA s- bad record on consumer disputes and the fallible e-commerce technological implementation (e.g bugs, Trojans etc)**(62)**. Besides technical failure and abuse of an e-signature, consumers still carry the burden to provide evidence in disputes over e-transactions in case of human error; with our 'misclick' on the mouse or-even worse- with our children's click on the mouse our annual or even lifetime budget can be vanished into thin air!**(63)**

Therefore, as far as future harmonization between the Directive and the Act is concerned, there is a lot of work to be done both on governmental and private sector. Further, results will be definitely achieved, if EU and USA continue their transnational dialogue and cooperate with other international bodies for the proliferation of a reliable and consistently standardised e-commerce.

The minimalist approach still seems to be the strongest asset for e-signature users; legislation and regulation with a low level of thoroughness would possibly allow courts to recognise at their discretion a signature user's choice of methodology and intent to be bound**(64)**. However, even a minimalist scheme like the 'E-Sign Act' should safeguard better the consumers' rights and establish a well-shielded legal environment in order to promote the enhancement of transactions over open networks.

In terms of technology, e-signature standards should be developed uniformly, transparently and objectively by abstaining from introducing new regulatory schemes for each and every authentication method and by recognising the same level of validity and enforceability to e-signatures, which meet the international requirements.

Moreover, both European and American government could bring the public closer to the use of e-signatures and provide warranties about the reliability and the security of e-transactions. Both statutes should increase CA s liability towards consumers and ensure users rights in case of fraud, abuse and even human error while keeping the alternative of conventional transactions available to reluctant or even unable- to-use e-signatures users. In addition, the principle of 'freedom of contract' between parties, regarding the use of authentication systems they trust, can be reassured by the private sector's initiative to establish voluntary accreditation schemes and issue trustworthy and interoperable certificates. Not only on transatlantic but also on international level a cross-border ADR must be clearly designed in order to build a solid and secure legal platform regarding the use of e-signatures on the Internet**(65)**.

5. Conclusion

In conclusion, e-signatures do play an important part in e-commerce by providing safety and reliability in e-transactions. Due to the significance of this emerged technology a lot of international initiatives have been launched and legislators around the world struggle to find the best regulatory scheme in order to legally equate e-signatures to the handwritten ones.
Regarding the EU Directive and the E-Sign Act, both of them are innovative statutes and their main goal is to set up a functional and well-defined legal environment of e-transactions. However, as e-signatures are in their infancy, many aspects of these two statutes should be worked out in conjunction with the users and the market's needs.

Finally, the partnership between the EU and the USA both on governmental and business level can gradually lead to a common minimalist legal framework on e-signatures, which will become the driving force for e-commerce to flourish. The same type of transatlantic consensus that has been successfully achieved in the 'Safe Harbor Agreement' on the protection of personal data of individuals can also be accomplished on the issue of electronic signatures.

Notes and References

1. US Department of Commerce, US Census Bureau:
<http://www.census.gov/eos/www/ebusiness614.htm>.

2. According to Jupiter Communications, spending on B2B will reach $6.3 trillion by 2005 in the US marketplace.

3. Electronic commerce 101: Signing on the Dotted Line Gets Easier Everyday, Melissa J. Kozlowski, Miami Daily Business Review, : www.law.com.

4. For further information about the technological functions of 'digital signature method' see: Report from ABA: <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>.

5. The key pair can be generated by the user herself or by running specific cryptographic software (e.g MS Internet Explorer, NetScape Communicator): Digital signatures-addressing the legal issues: <http://www.bmck.com/ecommerce/Digital%20Signatures%20-Addressing%20the%20Legal%20Issues.doc>.

6. See the website referred in note 4.

7. Angel, J (1999), Why use Digital Signatures for Electronic Commerce?, The Journal of Information Law and Technology (JILT) 1999 (2)
<http://elj.warwick.ac.uk/jilt/99-2/angel.html>.

8. ABA (1996), Digital Signatures Guidelines
<http://www.abanet.org/scitech/ec/isc/dsgfree.html>.

9. Froomkin, A. Michael (1996), The Essential Role of Trusted Third Parties to Electronic Commerce, <http://www.law.miami.edu/~froomkin/Articles/trusted1.htm>.

10. Examples of currently available CAs worldwide: Verisign, BaltimoreTech, RSA security, PGA, Valicert <http://www.valicert.com>, Hyper-send <http://www.hyper-send.com>, Omtool <http://www.omtool.com>, Valimation <http://www.valimation.com>, Ecertain, ArcotSystems, Digitalsignature Trust Co, EnTrust Technologies, Alpha-Trust Corp.
<http:// www.alpha-trust.com>, Ednetrust.

11. Due to digital signatures the banking and the insurance sector can simplify the access to banking systems and the claims application and submission and thus provide competitive and consumer-friendly services: <http://www.hat-hat.com/academia/digitalsignature.ppt>.

12. 'Federal Courts Sign On With E-Signatures', The Third Branch:
<http://www.uscourts.gov/ttb/sept00ttb/esign.htm>.

13. The international approaches towards e-signatures are worth mentioned because they have strongly influenced both EU's and USA's perception as far as e-signatures legislation is concerned.

14. This is achieved by ensuring that e-signatures are as legally binding as the tangible signatures.

15. Model Law on Electronic Commerce (1996)-enacted in 1998: <http://www.uncitral.org>.

16. OECD Guidelines for Cryptography Policy (1997): <http://www.oecd.org>.

17. Declaration on Authentication for Electronic Commerce (Annex 3 of Conference Conclusions)-1998, Ottawa: <http://www.oecd.org>.

18. Joint OECD-Private Sector Workshop on Electronic Authentication, 1999: <http://www1.oecd.org/dsti/sti/index.htm>.

19. <http://www.abanet.org/scitech/ec/isc/dsgfree.html>.

20. <http://www.ict.etsi.org/eessi/final-Report.pdf>.

21. Approaches in electronic authentication legislation: <http://rechten.kub.nl/simone/DS-art4.htm>.

22. An Analysis of International Electronic and Digital Signature Implementation Initiatives: <http://www.ilpf.org/groups/analysis_IEDSII.htm>.

23. Model Law on Electronic Signatures, 2001: <http://www.uncitral.org>.

24. See note 19.

25. Directive 1999/93 EC, OJ L013, 19.1.2000,p.0012-0020, <http://europa.eu.int>..

26. COM (97) 157: <http://www/cordis.lu/esprit/src/ecomcom.htm>.

27. See note 23.

28. Frank D (2000), 'Europe Takes Lead on E-signatures', <http://www.fcw.com/fcw/Articles/2000/1016/tec-esigns-10-16-00.asp>.

29. 'Whereas rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically': See note 23.

30. Joint Keidanren-ILPF Workshop on Electronic Signatures and Authentication (1999): <http://www.ilpf.org/events/keidanren/summary.htm>.

31. Commission welcomes new legal framework to guarantee security of electronic signatures: <http://europa.eu.int/comm./internal_market/en/media/sign/99-915.htm>.

32. Idem.

33. <http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html>.

34. Signature Directive Consultation Compilation :
<http://www.fipr.org/publications/sigdirecon.html>.

35. See note 23.

36. <http://www.eema.org/isse/press/news-detail2.asp?item=41>.#

37. Special report: Sign us up:
<http://www.dabs.com/news/news-Articles.asp?atype=newsfeed&Article=261>.

38. E-Sign Act (2000):
<http://thomas.loc.gov/cgi-bin/query/D?c106:6:./temp/~c106Nii0hw>.

39. <http://www.ecommerce.gov/framewrk/htm>.

40. Uniform Electronic Transactions Act:
<http://www.nccus/org/uniformact_summaries/uniformacts-s-s-ueta.htm>.

41. Alston and Bird (2000), How the New E-Sign Act Will Affect E-Commerce, LLP:
<http://www.gigalaw.com/Articles/alston-2000-06-p2.htm>.
42. The Act contains a well-defined list of UETA and non-UETA based exemptions from its scope. See note 36.

43. Johnston M (2000), Digital Signatures Take Effect in US,
<http://www.nwfusion.com/news/2000/1002siglaw.htm>.

44. See note 36.

45. Bruce, W, Electronic Signatures in the Real World, Alpha Trust Corp.
<http://www. messageq.com/security/brice_1html>.

46. Summary of E-Commerce Legislation, McBride Baker & Coles:
<http://www.mbc.com/ecommerce/fedsummary.asp?federal=Enacted&PubID=
19124510520>.

47. See note 39.

48. A state that enacts UETA may exempt from UETA specific transactions governed by particular laws identified by the estate when it enacts UETA.

49. R. Gates is a managing partner of risk consulting for A. Andersen LLP: See note 41.

50. <http://www.tabd.org>.

51. Transatlantic Declaration: www.eurunion.org/partner/transatldec.htm

52. Electronic Commerce:
<http://www.eurunion.org/partner/summit/Summit9712/electrst.htm>, EU/US Summit, Washington, DC, December 18, 2000, Conclusions:
<http://www.eurunion.org/partner/summit/Summit/0012/Ecommerce.htm>.

53. Transatlantic agenda: <http://www.eurunion.org/partner/agenda/htm>.

54. Joint EU-US Action Plan: <http://www.eurunion.org/partner/actplan/htm>.

55. <http://www.identrus.com>.

56. Further information on 'Identrus' is available on: <http://www.identrus.com> and in'32000Y0811(02) Commission notice',OJ C231,11/8/2000,p. 0005-0008:
<http://europa.eu.int>.

57. European Commission Approves Network for E-Signature Authentication:
<http://www.devicelink.com/emdm/archive/01/01/013e.htm>.

58. L Davies is a researcher in Internet law at University of London. European E-Business Review, Managing Europe, Regulation: Red tape may weigh down web:
<http://specials.ft.com/ln/specials/q338606.htm>.

59. M. Saunders is a managing attorney of NCLC's DC office: Consumers at Risk, A ligitation Nightmare with Electronic Signature Law: <http://law.about.com>.

60. G.L.Kaplan, partner at Pittsburgh's Reed Smith Show &McClay. E-Sign: A Nudge, Not a Revolution, Oct. 1 is big for E-signature implementation, but states, business have work to do, M.Ballard, The National Law Journal: <http://www.law.com>.

61. [Random Bits], CPT Statement on E-Sign Bill: lists.
<http://essentials.org/pipermail/random-bits/2000-July/000184.htm>.

62. See note 32.

63. Robert Longley, an About's US Gov Info Guide, shares the same point of view. See note 57.

64. An Analysis of International Electronic and Digital Signature Implementation Initiatives: <http://www.ilpf.org/groups/report_IEDSII.htm>.

65. <http://www.itu.ch/osg/spu/ni/esca/meetingdec9-101999/shima.ppt>.

Bibliography

Legislation, Research Papers, Reports

American Association Bar (ABA), Digital Signature Guidelines (1996): <http://www.abanet.org/scitech/ec/isc/dsgfree.html>.

Commission Welcomes New Legal Framework to Guarantee Security of Electronic Signatures: <http://europa.eu.int/comm./internal_market/en/media/sign/99-915.html>.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L013,19.1.2000,p. 0012-0020: <http://europa.eu.int>.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L178.
2000/709/EC: Commission Decision of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/ec of the European Parliament and of the Council on a Community framework for electronic signatures (notified under document number C (2000) 3179) (Text with EEA relevance), OJ L289, 16.11.2000,p. 0042-0043: <http://europa.eu.int>.

Commission notice pursuant to Article 19(3) of Council Regulation No 17 concerning case COMP/37.462- Identrus (Text with EEA relevance), OJ C231, 11.08.2000,p.0005-0008: <http://europa.eu.int>.

Declaration on Authentication for Electronic Commerce (Annex 3 of Conference Conclusions)-1998, Ottawa: <http://www.oecd.org/>.

Electronic Signatures in Global and National Commerce Act 2000,(E-SignAct): <http://thomas.loc.gov/cgi-bin/query/D?c106:6:./temp/~c106Nii0hw>.
A European Initiative in Electronic Commerce COM (97) 157: <http://www.cordis.lu/esprit/src/ecomcom.htm>.

European Electronic Signature Standardisation Initiative (EESSI), Final Report of the EESSI Expert Team, July 20, 1999: <http://www.ict.etsi.org/eessi/final-Report.pdf>.
A Framework for Global Electronic Commerce, White House Paper: <http://www.ecommerce.gov/framewrk.htm>.

McBride Baker & Coles, Summary of E-Commerce Legislation (E-Sign Act).
OECD Guidelines on Cryptography Policy (1997): <http://www.oecd.org>.

TABD, Electronic Commerce, Joint Statement released in conjunction with the EU-US Summit in Washington, DC, December, 1997:

<http://www.eurunion.org/partner/summit/Summit9712/electrst.htm>.

TABD, EU/US Summit, Washington, DC, December 18, 2000, Conclusions: <http://www.eurunion.org/partner/summit/Summit0012?Ecommerce.htm>.

TABD,TransatlanticAgenda: <http://www.eurunion.org/partner/agenda.htm>.

TABD, Joint EU-US Action Plan: <http://www.eurunion.org/partner/actplan.htm>.

TransAtlantic Business Dialogue (TABD), Transatlantic Declaration (1990): <http://www.eurunion.org/partner/transatldec.htm>.

UNCITRAL Model Law on Electronic Commerce (1996): <http://www.uncitral.org>.

UNCITRAL Uniform Rules on Electronic signatures with guide toenactment(2001): <http://www.uncitral.org/english/sessions/wg_ec/wp-86.pdf>.

UNCITRAL Model Law on Electronic Signatures (2001): <http://www.uncitral.org>.
Uniform Electronic Transactions Act (UETA): <http://www.nccusl.org/uniformact_summaries/uniformacts-s-ueta.htm>.

Research papers, reports

Alliance for Global Business (AGB), Global Action Plan For Electronic Commerce: <http://www.intug.net/agb>.

American Bar Association (ABA) Report: <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>.

GBDe, 'Tokyo Recommendations', September 14, 2001: <http://www.gbd.org/acrobat/recommendations01.pdf>.

Global Business Dialogue on Electronic Commerce (GBDe), 'The Paris Recommendations', Authentication and Security, September 13, 1999: <http://www.gbd.org/acrobat/paris99.pdf>.

Global Information Infrastructure Commission (GIIC), Electronic Commerce: A Comparison of US, EU, MITI and GIIC Reports on Electronic Commerce, March 27,1998: <http://www.giic.org/focus/ecommerce/eccompares.htm>.

ICC, Creating trust in e-business -ICC guidelines updated, 2001: <http://www.iccwbo.org/home/news/archives/2001/guidec_two.asp>.
International Chamber of Commerce (ICC), General Usage for International Digitally Ensured Commerce-GUIDEC (version II): <http://www.iccwbo.org/home/guidec_two/contents.asp>.

Internet Law and Policy Forum (ILPF), REPORT: An Analysis of International Electronic

and Digital Signature Implementation Initiatives, Presentation and international discussion, September 10, 2000: <http://www.ilpf.org/groups/report_IEDSII.htm>.

Kuner, C, Barcelo, R, Baker, S and Greenwald, E (2000), An Analysis of International Electronic and Digital Signature Implementation Initiatives, A Study prepared for the ILPF by The Brussels office of Morrison & Foerster LLP and the Washington, DC office of Steptoe & Johnston LLP, September, 2000: <http://www.ilpf.org/groups/analysis_IEDSII.htm>.

Books

Edwards, L and Waelde, C, (2000) Law and the Internet: a framework for electronic commerce, Oxford, Portland Oregon, 2000.

European Commission, The legal aspects of digital signatures, ICRI.

Grant, L. G (1997), Understanding Digital Signatures: Establishing Trust over the Internet and Other Networks, McGraw-Hill Book Company.

Lloyd, (2000) J. Ian, Information Technology Law, 3rd edition, Butterworth.

Journal Articles

Approaches in Electronic Authentication Legislation: <http://rechten.kub.nl/simone/DS-art4.htm>.

Akdeniz, Y, Clarke, O, Kelman, A, Oram, A (1997), 'Can the Trusted Third Parties be Trusted? A Critique of the Recent UK Proposals', The Journal of Information, Law and Technology (JILT), 1997 (2): <http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/akdeniz.html>.

Angel, J (1999), Why use Digital Signatures for Electronic Commerce? The Journal of Information, Law and Technology (JILT) 1999 (2): <http://elj.warwick.ac.uk/jilt/99-2/angel.htm>.

Alston & Bird LLP (2000), How the New E-Sign Act Will affect E-Commerce: <http://www.gigalaw.com/Articles/alston-2000-06-p2.htm>.

Ballard, M (2000), E-Sign: A Nudge, Not a Revolution: Oct.1 is big day for E-signature implementation, but states, business have work to do, The National Law Journal, September 19, 2000: <http://www.law.com>.

B L, European Commission Approves Network for E-Signature Authentication, EMDM (Web Watch), October 2001: <http://www.devicelink.com/emdm/archive/01/10/013e.htm>.

Brice, W, Electronic Signatures in the Real World: <http://www.messageq.com/security/brice_1html>.

Downing, Robbie, and McKean, Ross, Digital Signatures: Addressing the Legal Issues, Baker & McKenzie's London Office, <http://www.bmck.com/> <http://www.bmck.com/ecommerce/Digital Signatures-Addressing the Legal Issues.doc>.

Eaglesham, J, Hargreaves, D (2000), REGULATION: Red tape may weigh down web, Managing Europe, February 1, 2000, European e-Business Review: <http://specials.ft.com/ln/specials/q338606.htm>.

Federal Courts Sign On With E-Signatures, The Third Branch: <http://www.uscourts.gov/ttb/sept00ttb/esign.htm>.

Foundation for Information Policy Research (FIPR), Signature Directive Consultation Compilation: <http://www.fipr.org/publications/sigdirecon.htm>.

Frank, D (2000), Europe Takes Lead on E-signs, Federal Computer Week, October 16, 2000: <http://www.fcw.com/>.

Froomkin, M (1996), The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregon L. Rev. 49 (1996), October 14, 1996: <http://www.law.miami.edu/~froomkin/Articles/trusted1.htm>.

Ghosh, K. Anup, Securing E-Commerce: A Systematic Approach, Journal of Internet Banking and Commerce (JIBC): <http://www.arraydev.com/commerce/JIBC/9704-04.htm>.

Johnston, M (2000), Digital Signatures Take Effect in US, NetworkWorldFusion News, October 2, 2000: <http://www.nwfusion.com>.

Love, J (2000), [Random-bits] CPT Statement on E-Sign Bill. June 30, 2000: <http://lists.essential.org/pipermail/random-bits/2000-July/000184.htm>.

Kozlowski, J. M, (1999), Electronic Commerce 101: Signing on the Dotted Line Gets Easier Everyday, Miami Daily Business Review, May 18, 1999: <http://www.law.com>.

Reed, P (2000), Consumers at Risk: A Litigation Nightmare with Electronic Signature Laws, October 24,2000: <http://law.about.com>.

Special Report: Sign us up, September 12, 2001: <http://www.dabs.com/news/news-Article.asp?atype=newsfeed&Article=261>.

Swindells, C, Henderson, K, Legal Regulation of Electronic Commerce, The Journal of Information, Law and Technology (JILT), 1998 (3): <http://elj.warwick.ac.uk/jilt/98-3/swindells.html>.

Timmers, P (1999), European Commission, Directorate General XIII, Van der Veer, Joep, Directorate General XV, Electronic Commerce: A Challenge for Europe, CommerceNet, October 18,1999: <http://www.commerce.net/>.

Workshops

Joint Keidanren-ILPF workshop on Electronic Signatures and Authentication, Tokyo, November19, 1999: <http://www.ilpf.org/events/keidanren/summary.htm>.

Joint OECD-Private Sector Workshop on Electronic Authentication, 1999: <http://www1.oecd.org/dsti/sti/index.htm>.

Links

<http://www.alpha-trust.com>.

Business and Industry Advisory Committee to the OECD(BIAC): <http://www.biac.org>.

Erik Tan Chong Meng, Hatsue Ogawa, Low Kerk Long, Ong Tong San, Tang Jia Jing, Li Wei, Wang Hong Liang, Wang Qian, Digital Signature (presentation), MBA 7503_A, MANAGEMENT OF INFORMATION TECHNOLOGY: <http://www.hat-hat.com/academia/digitalsignature.ppt>.

Global Business Dialogue on Electronic Commerce (GBDe): <http://www.gbd.org>.

Global Information Infrastructure Commission(GIIC): <http://www.giic.org>.

<http://www.hyper-send.com>.

<http://www.identrus.com>.

International Chamber of Commerce (ICC): <http://www.iccwbo.org>.

International Telecommunications User Group (INTUG): <http://www.intug.net>.
<http://www.omtool.com>.

Shima, Naoshi (NEC Corporation), The Needs of The Business Community: Towards a Global Framework for Authentication and Security (presentation), December 9-10, 1999: <http://www.itu.ch/osg/spu/ni/esca/meetingdec9-101999/shima.ppt>.

Transatlantic Business Dialogue (TABD): <http://www.tabd.org>.

US Census Bureau (US Department of Commerce): <http://www.census.gov/eos/www/ebusiness614.htm>.

<http://www.valicert.com>.

<http://www.valimation.com>.

World Information Technology and Services Association (WITSA):
<http://www.witsa.org>.