International Chamber of Commerce

The world business organization

GUIDEC II

General Usage for International Digitally Ensured Commerce (version II)

October 2001

International Chamber of Commerce
38, Cours Albert 1er, 75008 Paris, France
Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59
Web site www.iccwbo.org E-mail icc@iccwbo.org

Published in October 2001 by
International Chamber of Commerce
The world business organization
38 Cours Albert 1er
75008 Paris, France

Foreword

by William Kennair
Scrivener Notary, John Venn & Sons, London, U.K.
Chairman, Information Security Working Party, ICC Electronic Commerce Project.

The first version of GUIDEC was published in November 1997 by the International Chamber of Commerce (ICC) Information Security Working Party, under the auspices of ICC's Electronic Commerce Project (ECP), with the title of General Usage for International Digitally Ensured Commerce. The Electronic Commerce Project itself is an international, multidisciplinary effort to study, facilitate and promote global electronic trading systems.
ICC Commissions participating in the Electronic Commerce Project include the commissions on Banking Technique and Practice, Air Transport, Maritime and Surface Transport, Telecommunications and Information Technologies, International Commercial Practice, Financial Services and Insurance, and together they aim to provide a globally comprehensive approach to electronic commerce.

The Electronic Commerce Project is chaired by Åke Nilson of Marinade Limited, London, U.K. and brings together leading corporations, lawyers, information technology specialists, government representatives and industry associations worldwide to focus on pivotal issues in electronic commerce. Electronic commerce working groups have been formed to examine specific critical issues in this context.

The proposal to develop international guidelines was raised at the ICC in November 1995 in the context of ICC work on the legal aspects of electronic commerce and on the establishment of an international chain of registration and certification authorities.

Upon examination, ICC and its Electronic Commerce Project determined that the issues involved in electronic commerce, including the use of digital signatures, and the role of certification authorities in enabling their use, were sufficiently complex to merit a distinct new group. The first version of the GUIDEC aimed to draw together the key elements involved in electronic commerce, to serve as an indicator of terms and an exposition of the general background to the issue. This second version carries on from the original work. It has retained most of the issues addressed in its predecessor, but attempts to go further in the field of application, as opposed to giving an historical overview. It also contains several new definitions and best practices, and reorders the way they are handled in the text itself.

Contents

Preface

I. Background

1. Objectives

This document is intended to provide the context and policy underpinnings of the GUIDEC, with the objective of promoting the world business community's understanding of the issues relating to the use of techniques in electronic commerce. The first edition of the GUIDEC aimed to balance different legal traditions and cover both the civil and common-law treatment of the subject, as well as pertinent international principles. By doing so, it presented both business and governments with a comprehensive statement of best practices for a global infrastructure. This second version builds on the foundation created by the previous document, and expands areas of direct relevance to the business community. It includes the potential of additional technologies such as biometrics in establishing trustworthy digital transactions as well as taking cognizance of policy developments such as the United Nations Commission on International Trade Law (UNCITRAL) model laws and the European Union Directives.

The principle objective of the GUIDEC is to establish a general framework for the authentication of digital messages, based upon existing law and practice in different legal systems. In so doing, the GUIDEC provides a detailed explanation of principles, particularly as they relate to information system security issues, public key cryptographic techniques and emerging biometric capabilities. It also provides succinct standard practices or recommendations relating to secure authentication and processing of digital information.

2. The aim of the GUIDEC

The GUIDEC framework attempts to allocate risk and liability equitably between transacting parties in accordance with existing business practice, and includes a clear description of the rights and responsibilities of subscribers, certifiers, and relying parties.

The aim of the GUIDEC is to enhance the ability of the international business community to execute trustworthy digital transactions utilizing legal principles that promote reliable digital authentication and certification practices.

The GUIDEC treats the core concepts, best practices and certification issues in the context of international commercial law and practice. In so doing, the document assumes practices in which transacting parties are expert commercial actors, operating under the lex mercatoria. The document does not attempt to define rights and responsibilities for transactions involving consumers. Nor is it intended to outline practices for transactions in which overriding national or other public interests may demand additional transactional security, such as notarial or other public intervention, although many notarial principles are enshrined in the document. In this regard, it is also important to note that the GUIDEC does not attempt to set out rules for certification of information relating to authority, legal competence, etc., which notaries are often called upon to certify.

Although the GUIDEC is organized primarily as an outline for parties involved in public key based systems (i.e. digital signatures), the fact that it draws upon existing law means most of its principles will apply for other technologies.

II. Electronic commercial transactions

The earliest international mode interchange agreement was published by ICC as long ago as 1987 in response to the need for harmonized principles promoting certainty in electronic commercial transactions conducted through Electronic Data Interchange, as well as the need to promote parity between trading partners. These Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission (UN-CID) have served as the basis for many of the model or standard trading agreements issued by national, regional and business organizations. These rules update the UN-CID principles, and apply them in the context of electronic commerce today.

As a common denominator, any model agreement should aim to address the common issues of technical requirements, acknowledgement or verification, third-party service providers, record storage and audit trails, digital security, confidentiality, and data protection. In doing so, model trading agreements will establish the foundation for a contractually based legal structure for electronic commerce.

III. Trustworthiness of electronic transactions

The movement to open network communications systems, such as the Internet, poses significant challenges to the implementation of a global electronic trading system. Among the most significant barriers to global electronic commerce over open networks are those pertaining to the security of the information involved (i.e. its integrity, availability and confidentiality). The application of security and reduction of the risk of fraud and unauthorized access is vital to the growth of the number and volume of international commercial transactions over networked computers.

Appropriate information security enables a level of trust and confidence to be present in the transfer of information between parties. Industry recognizes the need for a reliable framework for identifying and certifying parties to a transaction and authenticating the transaction itself. This should be industry-driven and enable some transactions to demonstrate a higher level of trust and confidence than others. Governments should provide support through legislation and international agreements. This document continues the process of enhancing legal predictability by providing a statement of commercial authentication and certification practices.

IV. Existing law and electronic transactions

1. General

The advent of electronic commerce has challenged, and will continue to challenge, the validity of formalities in personal and commercial documentation. Recently, there has been a steady movement throughout the world to address the issues pertaining to global electronic commerce through legislation.

The historical, and currently perceived, function of formalities has an important effect on their adaptability to electronic commerce. Virtually every nation has at least looked into the question, resulting in a variety of approaches. Amongst these are the work of UNCITRAL in its Model Laws on Electronic Commerce and Electronic Signatures rules, the European Union Directives on the subject, work done at the Organization for Economic Cooperation and Development (OECD), and legislation in the United States. All of these have had a profound influence on the direction taken.

2. UNCITRAL - Model laws on electronic commerce and electronic signatures

The most definitive treatment of the issues for international electronic commercial transactions is still that embodied in the United Nations Commission on International Trade Law Model Law on Electronic Commerce (the UNCITRAL Model Law), adopted by UNCITRAL during its 29th session, 28 May – 14 June 1996, in New York. The Model Law treats electronic signatures as they relate generally to problems deriving from form requirements in existing commercial laws of the major legal systems. Specifically, the Model Law provides that form requirements relating to signatures may be met in relation to data messages where a method is used that identifies the person and indicates that person's approval of the contents of the data message, and where the reliability of the method of signing is appropriate under the circumstances. Recognizing that signature requirements derive from fundamental commercial law and public policy issues relating to intent of contracting parties, the Model Law does not specify what method of signing a data message might be appropriate under what circumstances. The Guide to the Model Law does indicate, however, that it may be useful in the context of data messages, to "develop functional equivalents for the various types and levels of signature requirements in existence". The first GUIDEC attempted to build upon the Model Law in this regard, by defining requirements for signatures used in international commerce, in particular digital signatures, in which there is the additional requirement of certification.

The Model Law further treats signature requirements in the context of the evidential weight of data messages based upon the reliability of the manner in which the data message was generated, stored, communicated, and maintained, in general. In the context of storage and retention of data messages for evidentiary purposes, the Model Law provides that document retention provisions may be satisfied for data messages if the following conditions are met:

- the information contained in the data message is accessible so as to be subsequently usable;
- the data message is maintained in the same format in which it was generated and communicated, or in another format which demonstrably maintains the accuracy of the message's content, and;
- the information is retained in a fashion that enables the identification of the origin, destination, date, and time it was sent and received.

The Model Law recognises that data message retention will often be undertaken by intermediaries and other third parties which do not fall under the definition of "intermediary" in the Model Law, and provides that data messages may be retained by third parties as long as the above requirements are met. Although the Guide makes it clear that retention may be carried out by non-"intermediary" third parties, it does not distinguish whether responsibilities of these parties in the context of the Model Law would be regarded as the same or similar to those of intermediaries, or whether third party obligations fall outside the ambit of the Model Law.

The UNCITRAL Working Group on Electronic Commerce has subsequently developed a complementary Model Law on Electronic Signatures, accompanied as before by a Guide to Enactment. The new Model Law seeks to ensure equal treatment to users of paper-based documentation and computer-based documentation and to provide a level of confidence in the reliability of electronic signatures in legally significant transactions.

An electronic signature complies with the requirement for a signature if the following conditions are met:

- it is as reliable as was appropriate for the purpose for which the data message was generated or communicated;
- the signature creation data can only be attributed to the signatory;
- the signatory was the only person with control of the signature creation data at the time of signing;
- any alteration of the electronic signature is detectable;
- any alteration to the information whose integrity is required to be assured through a signature is detectable.

The Model Law is intended to promote international commerce through electronic transactions and, as such, excludes consideration of the geographic origin of the certificate or electronic signature or the place of business of the issuer or signatory in determining its legal effect. It also provides equal treatment for electronic signatures with substantially the same level of reliability created inside and outside of the enacting State. The Model Law on Electronic Signatures outlines specific rules for the conduct of the signatory, service provider, and the relying party and holds the parties liable for any failure to satisfy such requirements.

3. European directive

The European Union Directive on Electronic Signatures (Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures) provides a harmonized legal framework for electronic signatures in the European Union.

It is available at http://europa.eu.int/comm/internal_market/en/media/sign/index.htm.

The Directive is intended to (1) remove legal barriers to the use of electronic authentication in Europe, (2) restrain the Member States from enacting contradictory national legislation, and (3) provide a basis for international negotiations between the EU and third countries.

The Directive contains provisions in the following areas:

- *Legal recognition:* The Directive stipulates that an electronic signature cannot be legally discriminated against solely on the grounds that it is in electronic form. Certain types of signatures and certificates also receive enhanced legal recognition.
- *Free circulation:* All products and services related to electronic signatures can circulate freely and are only subject to legislation and control by the country of origin. Member States cannot make the provision of services related to electronic signatures subject to mandatory licensing.
- *Liability:* Minimum liability rules are established for service providers who are, in particular, liable for the validity of a certificate's content.

- *A technology-neutral framework:* The Directive provides for legal recognition of electronic signatures irrespective of the technology used.
- *Scope:* The Directive covers the supply of certificates aimed at identifying the sender of an electronic message. In accordance with the principles of party autonomy and contractual freedom, it generally avoids mandatory regulation and permits the operation of schemes governed by private law agreements such as corporate Intranets or banking systems.
- *International dimension:* To promote a global market in electronic commerce, the Directive includes mechanisms for cooperation with third countries on the basis of mutual recognition of certificates and bilateral and multilateral agreements.

4. OECD

There are a number of recent OECD work products that are relevant to digital signatures. First in 1998, in Ottawa, the OECD Ministers set forth a statement on Electronic Authentication. The Ministerial declaration recognized the importance of electronic authentication in developing consumer trust and urged Member States to promote the deployment of electronic authentication systems and to remove barriers to electronic authentication.
The text can be found at: http://www.olis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final

Further, as part of the review of electronic authentication, the Working Party on Information Security and Privacy (WPISP) undertook a survey of authentication laws across Member countries. This survey is updated on a periodic basis. Another project undertaken by the WPISP was to review the form-based barriers to electronic commerce. The review of barriers was undertaken across four main topic areas: Electronic Contracting, Financial Services, Transportation and Government.
[Document not yet released].

5. United States of America - E-SIGN Act

On 30 June 2000, President Clinton signed the "Electronic Signatures in Global and National Commerce Act" (Public Law 106-229), also known as the "E-SIGN Act". Simply put, E-SIGN states that electronic signatures are as legally binding as traditional paper signatures. E-SIGN also does not compel the use of electronic signatures nor does it deny anyone the right to determine the means for authenticating an electronic signature. It merely prohibits the denial of legal effect, validity or enforceability of a transaction solely because an electronic signature was used.

Under the E-SIGN Act, the validity and enforceability of an electronic contract is still evaluated under existing substantive contract law. Parties involved in a transaction are free to choose the authentication technologies they consider appropriate for their transactions. By ensuring that state laws do not require, or give greater legal status or effect to the use or application of a specific technology or technological specification, E-SIGN advances three legislative goals:

(i) to ensure a uniform nationwide standard of legal certainty for electronic signatures;
(ii) to give consumers and businesses the freedom to select the technology that is most appropriate for their particular needs, taking into account the importance of the transaction and its corresponding need for assurance; and

(iii) to encourage technological innovation by not granting a legal presumption of reliability to any one type of technology or software business, as many states did when they granted a legal presumption of authenticity to digital signature technology.

As of 1st October 2000, E-SIGN pre-empted all state laws governing electronic signatures except in those states, which enacted the Uniform Electronic Transactions Act (UETA), as drafted by the National Conference of Commissioners on Uniform State Law (NCCUSL). UETA will continue to govern electronic signatures in those states that have enacted it; provided that the state's e-signature law does not conflict with titles I and II of E-SIGN.

As of 2 April 2001, 27 states had enacted UETA in some form.

ESIGN also requires the Secretary of Commerce to promote the acceptance and use, on an international basis, of electronic signatures in accordance with the following principles:

(A) Remove paper-based obstacles to electronic transactions by adopting relevant principles from the Model Law on Electronic Commerce adopted in 1996 by UNCITRAL.

(B) Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced.

(C) Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.

(D) Take a non-discriminatory approach to electronic signatures and authentication methods from other jurisdictions.

6. Others

The Internet Law and Policy Forum had conducted an International Authentication Survey to ascertain the position worldwide as regards legislation in this field. The results can be found at http://www.ilpf.org/groups/analysis_IEDSII.htm and are also reproduced here as an annex.

Electronic contracting

V. Business context of electronic contracting

'Electronic contracting' is the automated process of entering into contracts via the parties' computers, whether networked or through electronic messaging. Because the parties can programme their computers to respond automatically to certain input (such as an offer or enquiry), the parties may not be aware in every case of precisely what their networked computers are doing, and they may not consciously participate in the contract formation process. Moreover, the errors that result from computers making contracts (probably due to the programming logic) are sometimes not the sort that human beings would make, and the legal rules relating to mistake, bad faith, misrepresentation, and the like may not quite fit the errors that result from computers processing transactions. In view of those facts, this document recommends best practices for businesses making contracts electronically.

The recommendations assume a business and economic context in which electronic contracting occurs. In light of electronic commerce as practiced as of this writing (2001), that context has come to be dominated by large-scale public networks of computers, networks which have become easy to use and practically ubiquitous in many commercial environments as the World Wide Web. These developments fundamentally affect the way business is done, even where it is already being done electronically. The greater power and reach of the new networks also offer opportunities to achieve greater efficiency in performing transactions. To consider how transactions work electronically, a look at basic business models is informative.

VI. Electronic business models

In most economic cultures, the basic model for doing business is the market. In a market model, those who have meet those who need, they bargain and agree, and they exchange. The market is assumed to operate among an open, broad community, and in that respect, it differs from a chain. This constitutes an open business model.

In a chain, the number of buyers and sellers is restricted due to obligations of exclusivity. If a chain has been imposed, a stranger can no longer simply go to the marketplace and sell what he has or buy what he needs. Instead, a seller is committed to sell only to a specified buyer or small group of buyers. Similarly, a buyer is also restricted to a defined set of sellers. This constitutes a closed business model. The exclusivity is a matter of degree, and depends, among other things, on:

- *Relative bargaining power of the parties:*
  The relative numbers and availability of alternatives are among the factors determining bargaining power. Bargaining power has often proven to be greater in the buying role, assuming that many potential suppliers exist or can be induced to exist.
- *Cost of building one-off relationships:*
  The stranger-to-stranger transactions of the market model can be expensive, depending on how the

transactions are carried out.

In the recent past, the cost of building relationships has increasingly led the parties with superior bargaining power to promote the building of chains. Factors that contribute to that cost are:

- *Need for specialized goods:*
  In the automotive, aerospace, and similar industries, the captive supply chain manufactures goods that are not standard, fungible commodities but rather are made to the buyer's specifications. The supplier may recover over time the costs of tooling-up to produce goods satisfying unique specifications, and may thus become economically dependent on a powerful buyer. In addition to specialized goods, distribution services are often established to support the chains and are dependent on the chains for their subsequent survival.
- *Technical set-up and integration:*
  Traditional electronic data interchange (EDI) is based on the chain model because of the difficulty and complexity of setting up interconnected databases and the means of reliably transferring information between them. The legal approach to EDI reinforced this dependence on chains: the legal basis for EDI was established bilaterally between 'trading partners' through an agreement that was intended to suffice for all transactions that the parties would carry out. EDI has thus greatly promoted the development of trade chains in recent years at the expense of free choice in the marketplace.

A more recent model is the web portal whereby an intermediary establishes favourable pricing for purchases made through their portal. Generally they establish a closed user consumer/retail group and membership involves agreeing to certain rules. It is between a closed and open system, being less formally structured than EDI and is business-to-consumer focused rather than business-to-business as in EDI. The technical connectivity is much simpler and the relationship established contractually. Other forms of 'portal' are appearing aimed at providing an open marketplace or exchange of goods and services. This marketplace or exchange is itself a service and the growth of intermediaries is an indication of the major change from more traditional business models.

Although chains have become common in recent years, the market (open) model retains a great advantage over the chain (closed) model and a modest advantage over the semi-closed portal model: It is more economically efficient. The exclusivity of a chain causes the buyer to forego getting it cheaper elsewhere, and the seller to forego a better price elsewhere. A chain also burdens innovation by locking in a defined set of suppliers and locking out entrepreneurs with innovative products but no access to the locked-in sales channel. Further, a market is also highly responsive to changing circumstances, whereas the complexity and production integration of a chain can make it slow to realize that cars must now be more fuel-efficient, for example. Fundamentally, the economic attractiveness of the market model persists.

Early electronic commerce fostered the proliferation of chains into areas where they had not existed or had never been firmed up into legal commitments. EDI was so difficult and complex to set up that it required the cooperation of both buyer and seller. Securing that co-operation often involved a strong party compelling a weaker one to join in the interchange. However, the cost savings possible through EDI made the economic inefficiency of the chain model compared to the market model tolerable. However, as electronic commerce matures, it has become simpler, easier, and more standardized, as well as more powerful. It has also become nearly ubiquitous, more than widely enough distributed to support a market model of commerce. These subsequent developments create opportunities for increased economic

efficiency by re-evaluating where a chain is necessary and where a return to a market model can yield advantage.

It is important to remember, however, that whatever model is in use, the protocols or systems in use are fit for purpose and that the controls in place are appropriate to the value of the transaction.

VII. Developments affecting economic models

The developments since the early days (EDI era) of electronic commerce have reduced much of the technical complexity and interdependence required to engage in electronic commerce. Today, many parties without extraordinary technical sophistication buy and sell electronically at a cost of set-up unimaginable in the EDI days. In large measure, this change is a result of (1) more powerful yet user-friendly methods of information interchange, (2) the commercialization of trust, and (3) electronic contracting. This section examines each of those in turn.

1. More powerful messages

The information-carrying power and flexibility of electronic messages has increased dramatically in recent years. In early electronic commerce, messages consisted merely of unlabelled data fields in a prescribed form. Because development and set-up for utilizing those messages was laborious and expensive, software producers and system integrators insisted on widespread agreement on all aspects of the form, after which the form became inflexible. While this highly formalized approach to electronic commerce remains common in older systems, a new approach to message form has emerged from the World Wide Web. Experience with Hyper Text Markup Language (HTML), the format for Web documents derived from the Standard Generalized Markup Language (SGML), led to making SGML extensible, and the Extensible Markup Language (XML) was born. XML has since overtaken the earlier formalistic messages used in EDI, although EDI remains in use in legacy systems. The power and flexibility of newer message forms and their ability to integrate data with a documentary context sets the stage functionally for electronic contracting. Besides these functional capabilities, business-grade electronic commerce requires message security and assured authenticity.

2. Commercialization of trust

Trade in all forms requires an essential element of trust between the participants. As we move towards using the Internet for electronic trading (electronic commerce), this ability to trust must be maintained. A significant element of trading for centuries has been the ability to carry out transactions in a confidential manner and to be able to 'bind' the resultant deal. This may have been in the form of a handshake, or by signed and witnessed documents. Some transactions are anonymous, some only require the exchange of a token such as a bond or a Bill of Lading. Whatever the process, the electronic environment must enable it to continue.

Trust is an abstract quality that is generally derived over time between two (or more) parties. Within electronic contracting the parties may not have met and there is a desire to "fast-track" the establishment of an appropriate level of trust. Consequently, the ability to rely on an electronic message has become progressively commercialized as an industry increasingly known by the term 'trust services'. The value of trust services is a transfer of risk from the parties in a transaction to third-party service providers. For example, the following services are commonly used in business-grade electronic commerce:

- *Authenticity services* ensure that a message is genuine; in other words, that it is authenticated by an identified party, has remained intact, and that evidence can be produced to establish both of those facts, should the sender deny authenticity. A "certifier" as defined here in the GUIDEC is a species of authenticity service.

- *Payment and credit services* ensure that instructions or obligations to pay are properly approved by the payer and carried out in favour of the intended payee. Some of these services are electronic adaptations of transactions originally developed on paper such as bankcard charges and letters of credit. They also include experiments in new forms of electronic funds transfers.

- *Operational auditing or accreditation services* review the security, information flows, and other technical aspects of a system's operations to determine whether they accord with its obligations.

These commercial trust services supporting business-grade electronic commerce create a basis for conducting transactions at least as solid as the traditional paper one. Together with more powerful message capabilities, they make possible electronic contracting on a scale greater than previously envisaged.

3. Automated and agent-based electronic contracting

Networked computers make and perform contracts with increasing frequency using the various business models described above. They also take other actions that can greatly affect the rights and liabilities of the parties. The active, conscious participation of the parties in these processes can vary from a thorough deliberation about the legal significance of a transaction to complete unawareness. These new electronic contracting capabilities introduce a new dynamic into business and trade transactions. It is now easy to make contracts because parties can automate the contract formation process and manage it much like they manage their other critical information technology systems.

The ease of making contractual deals through automation may lead prevailing commercial structures back toward market economic models. Extensive networks such as the Internet and NASDAQ have demonstrated the vitality of markets when highly customized products are not the object. Markets, rather than chains, are the natural and more efficient economic model in the large networks when many who have are juxtaposed against many who need.

Besides enabling a return to market economics, automated (including agent-based) electronic contracting can also potentially be more flexible. It can facilitate better alignment with the real relationship between the parties as it evolves. Particularly in the thought underlying EDI and chains, contract formation was viewed as a manual process done once and for all when a link in the chain was forged. This front-loading of the contract formation process made the transactional rules incapable of evolving as the relationship evolved and incapable of responding to a new opportunity or transaction. Setting out ground rules at the start makes sense, but ground rules should leave room to work out contractual specifics later. It is more practical to have an initial enabling contract setting out ground rules and allow further contracts to draw in specific details opportunities, transactions, and relationships occur. Particularly those later, more specific contracts can perhaps most efficiently be made through automated electronic contracting. The e-Terms

project within the ICC Electronic Commerce Project specifically addresses this area.

VIII. Principles of fair electronic contracting (POFEC)

The first GUIDEC set the stage for a principled commercialization of trust in accordance with business needs, and now by incorporating principles of fair electronic contracting (POFEC), the current version seeks to do the same for electronic contracting. Although electronic contracting offers new possibilities for efficient transactions and economics, as well as greater flexibility and evolutionary capabilities, it also has new vulnerabilities to abuse and could face theoretical validity questions in some legal systems.

Abuse may arise because the capabilities of computers in processing documents have limitations different from those of people. A computer's ability to perceive the significance of the information depends entirely on what its programming anticipates and what the computer can recognize in its input. It would, for instance, have great difficulty in ascertaining a price from a simple, untagged expression that could be quite clear to a human reader, such as "for a price of ten pounds sterling per dozen".

Further, even if the input is tagged to make it recognizable by computers, a program may fail to properly interpret and process it. Usually, such shortsightedness in programming is inadvertent or simply a constraint to be accommodated, but failings can also result from pranks, or even more sinister reasons. However, although a computer's document processing capabilities are limited and susceptible to abuse, many business leaders are finding that the speed and cost savings of automation nevertheless justify the use of computers to process business documents.

Those documents can increasingly affect the obligations and rights of the computer users. Computers now perform transactions that cannot be seen as anything other than the making or extending of a contract. Sometimes those transactions are validated by an umbrella enabling agreement. However, contracts are also commonly made now between strangers via the Internet, without any ascertainable previous relationship between them at all, let alone a preparatory contract providing for subsequent electronic contracting. The increasing commercial significance of the transactions that computers perform, despite their limitations and vulnerabilities, demands practices that respect those limitations and vulnerabilities.

The POFEC contained herein examine the computer-to-computer processing of commercial documents, particularly documents that cause non-consumers to incur or increase their obligations. They do not and cannot establish legal requirements themselves, but rather state best practices in order to inform both policy and the practical conduct of international commerce as it proceeds to involve obligations incurred in ever more automated ways.

The main elements addressed contain guidance in the following areas:

Drafting for documents for document processing systems

- Avoid a battle of forms
- Incorporate external documents sparingly and carefully
- Avoid inclusion of inapplicable text
- Use document type when appropriate
- Avoid unrecognizable mark-up in a document
- Ensure authenticity adequately
- Permit manual intervention and override

Legal efficacy of electronic contracting

- Assent by a document processing system
- Mistakes and document processing systems
- Availability of the human readable form
- Evidence

It is anticipated that further projects within ICC's ECP will tackle in greater detail many of the issues raised herein. The ICC Model Electronic Sales Contract is a perfect example of the practical application of these guidelines in an easy-to-use form for business.

Best practices

IX. Authenticating a message

1. Authenticating a message as a factual matter

A message is authenticated, **as a factual matter**, if acceptable evidence indicates:
(a) the identity of the signatory, and
(b) that the message has not been altered since authenticated.

Clarification

- *"as a factual matter":* Distinct from legal significance or meaning, the factual question of authenticating a message is addressed simply to identifying the signatory and the authenticated message from the available and admissible evidence. Such a question seeks to discover simply the facts of who authenticated what.

Commentary

- ✓ Authenticating a message for evidential purposes in proceedings before tribunals is generally to authenticate a message as a factual matter. The focus of the inquiry is the genuineness of the proffered evidence and its factual linkage to the persons involved in the controversy. (For example, see the US Federal Rules of Evidence 901, providing that the evidential requirement is satisfied by "evidence sufficient to support a finding that the matter in question is what the proponent claims", and listing several examples).
- ✓ Authenticating a message can also serve as an indicator of origin, often in an evidential context, where the question is usually the fact of origin rather than any legal consequences of a signature.

2. Attribution and legal significance of authenticating a message

A person **must attribute** an **authenticated message** to the person who **actually authenticated** the message.

Clarification

- *"must":* Whether any consequence flows from a failure to attribute an authenticated message depends on the import of the message. If the message may painlessly be ignored, then a failure to attribute it is of no consequence.
- *"attribute":* The person having the authenticated message must consider it to be associated with the signatory in some significant way, which is often apparent from an accompanying expression of the signatory's intent, the facts and circumstances of the transaction, course of dealing, or usage of trade. In the same way, a properly attributed message prevents the signatory from subsequently denying the message (this is generally termed “non-repudiation”).

- *"authenticated message":* means a message which is
  1. intact and unaltered since authenticated, and
  2. identified with its signatory.
- *"actually authenticated":* In a case of forgery, the forger, rather than the ostensible signatory, is the actual signatory.

In this context, see also the UNCITRAL Model Law art. 11 (attribution of data messages) (1995).

Commentary

- ✓ The duty to attribute an authenticated message to its signatory presumes that the person having the authenticated message acts in good faith, exercises reasonable care in evaluating the authenticated message, and lacks timely knowledge or notice that the authenticated message is false or significantly questionable.
- ✓ In ascertaining who actually authenticated a message, a person is entitled to receive reasonable further assurances that the signatory has properly authenticated a message. In determining what is reasonable in a case, a tribunal should consider indications of the reliability or lack of reliability of the authenticated message, the availability of those indications to the person having the message, as well as the resources required to make further information available.
- ✓ If a person properly attributes a forged or improperly altered message erroneously and thereby incurs a loss, and if the forgery or improper alteration resulted from a failure by the purported signatory to safeguard an authenticating device or other fault by the purported signatory, then the purported signatory must indemnify or compensate the attributing person for the loss.
- ✓ The effect of attribution to a signatory depends on the content of the authenticated message, the other facts and circumstances of the transaction, applicable law, the course of dealing between the parties, and/or usage of trade. For example, authenticating the written expression of a contract is customarily taken to indicate assent to the contract, and may satisfy formal requirements for authenticating a message sufficient to give effect or enforceability to the contract. Authenticating a letter ordinarily indicates authorship. Authenticating a negotiable instrument in the manner of an endorsement has the effect of an endorsement.
- ✓ Attribution or legal enforceability of an otherwise attributable message may be limited by formal authentication and certification requirements.

3. Authentication of a message by an agent

If an agent authenticates a message and represents himself to do so by authority of a principal, the authenticated message is valid as that of the principal if, under applicable law, the agent had **sufficient authority to authenticate** the message.

Clarification

- *"sufficient authority to authenticate":* Legal systems differ in the processes commonly utilized for the granting of authority, and particularly in the degree to which implicit or apparent authorization is recognized and accorded legal effect (see comment (2) below). If, under applicable law, the existence of sufficiency of the would-be agent's authority is reasonably in doubt, the recipient of an authen-ticated message may well have reason to seek further assurances.

Commentary

- ✓ A person generally acts at his peril in relying on an agent's representation of authority. Rather than taking a purported agent's word for the effectiveness and scope of the agency, a person having an authenticated message should require a certificate or other, more reliable proof of agency.
- ✓ With regard to the use of software agents, it is important that the trustworthiness of the agent is established either by impartial review and testing or by the acceptance of liability by the software agent's vendor. This does not absolve the relying party of his need to ascertain the software agent's representation of authority.
- ✓ Legal systems differ in the extent to which one may rely on representations of agency by the purported principal, which fall short of a valid power of attorney, in cases where the principal later disputes the agency. At common law, "apparent authority" can arise from almost any manifestation of agency by a principal to third persons. Civil law legal systems have traditionally eschewed recognition of apparent authority, although jurisprudence in some has developed comparable doctrines in cases where the principal failed to dispel the appearance that the agent had authority or failed to stop the agent from acting in the principal's name.

4. Appropriate practices for authenticating a message

A signatory **must** authenticate a message by a means **appropriate under the circumstances**

Clarification

- *"must":* The consequence of a failure to authenticate a message properly is that the message may be disregarded. In general commercial practice and unless otherwise agreed, a message may be ignored if the manner of authenticating it either contravenes an agreement by the parties, is not suited to impart the legal efficacy intended by the parties for the message, or if reliance on the message as authenticated would not be reasonable under the circumstances.
- *"appropriate under the circumstances":* As the commentary below explains, the means should carry out the intent of the parties, or at least reasonably fit the transactional context. At least, signature requirements had the perhaps salutary effect of requiring a person to use minimal authentication methods. However, imposing sanctions for failure to comply with form requirements has proved to be problematic. In the common law, case law has tended to weaken formal requirements, perhaps because of difficulty in finding a fitting sanction for non-compliance. In the civil law, there are more rigid forms to be adhered to, especially in the areas where the state might take an interest, such as real property law, inheritance, or commercial registration of companies. Such matters require the intervention of a Notary, as a certifier.

The UNCITRAL Model Law (art. 6) would sweep aside formal requirements, and leave the recipient of the message to prove attribution. While this approach is sensible, one sticking point remains: the recipient bears the burden of proof on the attribution issue, but only the sender can authenticate the sender's message. The recipient may act at her peril in rejecting a message which, under various current definitions of "signature", could be treated as authentic. This article seeks to address that problem by establishing in the recipient a right to demand reasonable assurance of an authenticated message's authenticity.

Commentary

- ✓ The "means" may be determined by either the certification authority (CA) of application software vendor (if different). Consequently, the parties involved must have a level of trust and confidence in the means available for authenticating the message.
- ✓ The recipient of an authenticated message may request further assurances of its validity, such as a valid certificate attesting to a critical fact, or replacement or augmentation of the authenticated message using a more technologically reliable method, if authenticating the message either was not accomplished as agreed by the parties, or is not suited to impart the legal efficacy intended by the parties for the message. In the absence of an express agreement, the parties are assumed to have intended a reasonable outcome, and therefore to have intended to use only authentication practices that are reasonable under the circumstances.
- ✓ In determining what is reasonable under the circumstances, the recipient should consider:
  - facts that the recipient knows or of which the recipient has notice, including all facts listed in the certificate,
  - the value or importance of the authenticated message,
  - within the transaction in question, the course of performance between the relying person and subscriber and the available indices of reliability or unreliability corroborating the authenticated message,
  - in prior transactions, the course of dealing between the relying person and subscriber and the available indices of reliability or unreliability corroborating the authenticated message,
  - usage of trade conducted by technologically reliable information systems.

The factors are listed approximately in order of importance.

5. Scope of an authenticated message

The creator of an authenticated message must **clearly indicate** what is being authenticated.

Clarification

- ■ *"clearly indicate":* The signatory should both delimit precisely what the message is in order to distinguish it from other matter, and should create a clear link between the act of authenticating the message and the authenticated message itself.

Commentary

- ✓ Since authenticating a message does not apply to alterations of the message, a person receiving the authenticated message must determine whether the message arrives intact. Such a determination is only possible if the message has been clearly delimited and linked to when it was authenticated. On paper, the delimitation is accomplished by the spatial limits of paper, formatting conventions, and the custom of signing at the end of the message. The linkage between signature and message is often accomplished by including them both within the same paper message, with the signature generally following the message.
- ✓ Defining the message is complicated by the fact that different systems may present the message in varying human-readable forms. For example, a printer or fax machine may utilize a different size of paper than another. Variance in representations of the signed matter may or may not be significant. With electronic messages, variations are common, even when all relevant information systems are technologically reliable, simply because the capabilities and preferences of information systems vary. A signatory should express the authenticated message in a manner that enables a receiving information system to represent it properly, either in the manner required by law, agreed upon by the signatory and receiver, or in accordance with usage of trade, applicable technical standards, and/or common practices for messages of the kind. The parties should agree, in specifying the form for their messages, which variations are to be considered significant. In the absence of such an agreement, the signatory may specify the variations to be considered significant alterations of the message. Ordinarily, minor variations in the media size, font, spacing, margins, and similar features are inconsequential; however, a change significantly affecting meaning, including a change to the logical structure of the message, should generally be treated as a significant alteration. This is especially important in the electronic environment as some of the meaning may be "hidden" from the signatory.

6. Safeguarding an authentication device

If a person authenticates a message by means of a **device**, the person must exercise, at a minimum, **reasonable care** to prevent unauthorized use of the device.

Clarification

- *"device":* If the device consists of a system of interrelated components, the entire system need not be safeguarded. Rather, it suffices to safeguard one or more critical components of the system sufficient to prevent a falsely authenticated message.
- *"reasonable care":* "Reasonable care" is the degree of caution and prudence that a reasonable person would exercise under the circumstances. *(For comments on "reasonable", see ante.)*

Commentary

- ✓ The authentication device should be physically kept in a location where access is limited and carefully controlled. Access should be accorded only to trustworthy persons and ordinarily based on their need to utilize authentication services. Persons to whom access is granted should be identified by presentation of a password or pass phrase, by biometric information, or other secure means.

Those using the authentication device should satisfy themselves or be satisfied as to the correct operation of the device.

✓ Where remedial action is possible following a loss of control over an authentication device, the remedial action should be taken without delay. In a case in which a private key has been lost, the public key certificate should be revoked, or suspended immediately until it can be revoked.

7. Representations to a certifier

A subscriber must accurately **represent** to a certifier all facts material to the certificate.

Clarification

■ *"represent"* This can take many forms. It may simply be the statements of the subscriber, or the certifier may have taken extraneous evidence of the matters contained in the certificate. As the certifier will be responsible for the statements made in the certificate, it would be advisable for the certificate to be clear as to how the statement of facts has been arrived at.

Commentary

✓ See generally the definitions in *"Certification"*, post.

X. Certification

1. Effect of a valid certificate

A person may **rely** on a valid certificate as accurately representing the fact or facts set forth in it, if the person has no **notice** that the certifier has failed to satisfy a material requirement of authenticated message practice.

Clarification

■ *"rely":* The extent to which one may properly rely is limited to what is reasonable under the circumstances. In other words, one is not entitled to rely when a businessman of ordinary prudence would not do so from substantially the same informational and circumstantial vantage point. This implicit limitation on reliance finds expression in substantive law in limiting relief for deception to plaintiffs who are not excessively gullible or tainted; see, e.g., US Restatement Second of Torts § 548A (1977) ("A fraudulent mis-representation is a legal cause of a pecuniary loss resulting from action or inaction in reliance upon it if, but only if, the loss might reasonably be expected to result from the reliance").

■ *"notice":* The UNIDROIT Principles of International Commercial Contracts point out that "notice" "includes a declaration, demand, request or any other communication of intention". (International Institution For The Unification of Private Law (UNIDROIT), Principles of International Commercial Contracts, art. 1.9 (1994).)

Commentary

- ✓ Fundamentally, a certificate is simply evidence of the fact or facts it represents. As such, it is only as good as the certifier is worthy of belief. For commerce to function properly, a society must provide a trustworthy means of establishing critical facts, such as the identity of a signatory. Certifiers provide such a means, but only if the certifiers are trustworthy.
- ✓ Where trustworthy certification practices are generally known to be followed, certificates are customarily treated as establishing the facts represented in them. For each transaction, the parties may ordinarily determine whether a particular certificate or type of certificate is acceptable. In certain circumstances, and particularly in the absence of an agreement among the parties, applicable substantive law can often supply a rule determining validity, together with any supporting certification. Such substantive rules may relate to the legal system's supervision of certifiers.
- ✓ Although a certificate is fundamentally evidence, whether or not a certificate is admissible in a judicial or arbitration proceeding is determined according to the rules of the forum.
- ✓ All the foregoing presumes that the parties are acting in good faith and without deception or negligence in conducting their business.

2. Accuracy of representations in certificate

A certifier must confirm the accuracy of all material facts **set forth** in a valid certificate, unless it is evident from the certificate itself that **some of the information has not been verified**.

Clarification

- ■ *"set forth":* This applies both to facts explicitly stated in the certificate and to facts on which conclusions in the certificate are based.
- ■ *"some of the information has not been verified":* This has been termed "Non-Verified Subscriber Information". See commentary, post.

Commentary

- ✓ One school of thought holds that all of the information set out in a certificate must have been verified by the certifier. This would prove to be unnecessarily restricting in commercial practice, as circumstances may exist where it is required to authenticate a message, but the signatory is unable to provide satisfactory evidence, say, of his corporate authority to act. It should therefore be possible for the certificate to contain a statement to the fact that the signatory is purporting to act on behalf of a particular corporation, but that this has not been proved. The receiving party is then able to make a commercial risk assessment as to whether to accept the authenticated message as it stands, or to demand further proof.

3. Trustworthiness of a certifier

A **certifier** must:

(a) use only technologically reliable information systems and processes, and **trustworthy personnel** in issuing a certificate and in suspending or revoking a public key certificate and in safeguarding its private key, if any;

(b) have no **conflict of interest** which would make the certifier untrustworthy in issuing, suspending, and revoking a certificate;

(c) refrain from contributing to a breach of a duty by the subscriber;

(d) refrain from acts or omissions which significantly impair reasonable and foreseeable reliance on a valid certificate;

(e) act in a trustworthy manner towards a **subscriber** and persons who rely on a valid certificate.

Clarification

- *"certifier":* The certifier may be a first party (within the organization) or a third party (independent).
- *"trustworthy personnel":* A certifier must make reasonable efforts to screen, train, manage, and assure the loyalty of all employees performing functions significantly affecting the certification process.
- *"conflict of interest":* To be trusted by the parties to a transaction and serve as a trustworthy verifier of facts should a dispute arise, a certifier must not have a stake in the transaction that would compromise the certifier's trustworthiness.
- *"subscriber":* A certifier owes a duty to a subscriber for whom the certifier issues a certificate, and to successors to the subscriber's rights which are dependent on the certification.

Commentary

✓ The trustworthiness of a certifier is central to the whole concept of certification. This trust in turn is generally founded upon the liability that the certifier is willing to accept for its statements. The certifier may seek to limit its liability to a certain level through its "certification practice statement" (see ante), but in doing so should exercise care that this limitation of liability is permissible within its jurisdiction. The very nature of electronic commerce as an international medium then further complicates this matter, as the certifier may find that its certification is relied upon beyond its own borders. By the same token, a person relying upon a certificate should ascertain the level of reliance the certifier is expecting him to place on the same.

4. Notice of practices and problems

A certifier must make reasonable efforts to notify a **foreseeably affected person** of:

(a) any material certification practice statement, and

(b) any fact material to either the reliability of a certificate which it has issued or its ability to perform its services.

Clarification

- *"foreseeably affected person":* To assure that a certifier foresees an effect, a person who believes himself to be affected may notify the certifier of the person's position and interest, and request a certification practice statement or further information.

Commentary

✓ Foreseeability is a difficult concept, especially when a certificate may be freely circulated, though of course it is an inherent element in assessing a commercial risk.

5. Financial resources

A certifier must have financial resources **sufficient** to conduct its business and bear the **reasonable risks** resulting from the certificates it issues.

Clarification

- *"sufficient":* As between a certifier and its client, the subscriber, the sufficiency of the certifier's financial basis is apparent from their willingness to do business with each other in a setting where the subscriber could have retained the services of another. In relation to third parties, however, the sufficiency of a certifier's financial basis should be evaluated according to a reasonableness standard.
- *"reasonable risks":* The reasonableness of a risk should be evaluated in light of what is foreseeable from the certifier's informational vantage point, and what is likely.

Commentary

✓ It is under this heading that we must consider the impact of insurance, either by bonding or through indemnity insurance. Existing professional certifiers, such as Notaries, are required to carry sufficient professional indemnity insurance to cover such losses as are likely to be occasioned as a result of others relying upon their certifications. Such insurance can be considered as adding to the available financial resources of a certifier, though evidently he will not have access to such resources unless and until a claim is made against him.

6. Records

A certifier must keep records of all **facts material to a certificate**, which it has issued for a **reasonable period of time**.

Clarification

- *"facts material to a certificate":* The required records include evidence to support all representations made in a certificate.

- *"reasonable period of time":* The duration of the record retention period is difficult to pinpoint, and requires weighing the need for reference to the records against the burden of keeping them. The records could be needed at least as long as a transaction relying on a valid certificate can be questioned. For most transactions, statutes of limitation will eventually place a transaction beyond dispute. However, for some transactions such as real property conveyances, legal repose may not be realised until after a lengthy time elapses, if ever.

Commentary

✓ Most professions already have established rules for the keeping of records, depending upon their nature. There is no reason that these rules should be any different in an electronic world, though added care must be taken to assure the retrievability of the information stored, especially in view of the rapid advances in technology.

7. Termination of a certifier's business

In terminating its business, a certifier must:
(a) act in a manner that causes minimal disruption to subscribers and persons relying on issued valid, operational certificates; and
(b) turn over its records to a **qualified successor**.

Clarification

- *"qualified successor":* Another certifier is generally qualified to succeed a withdrawing certifier. A responsible, high-quality archiving service, a professional association, or regulatory agency may also be suitable. The successor need not issue new certificates, but must at least maintain suspension, revocation and retrieval services.

Commentary

✓ If no successor is willing to take over a certifier's business, it may be necessary to revoke all valid certificates outstanding, since the certifier will not be available to support them in the future.

8. Suspension of public key certificate by request

The **certifier which issued** a certificate must **suspend** it promptly **upon request** by a person identifying himself as the subscriber named in the public key certificate, or as a person in a position likely to know of a compromise of the security of a subscriber's private key, such as an agent, employee, business associate, or member of the immediate family of the subscriber.

Clarification

- *"certifier which issued":* Although the certifier need not confirm the identity or agency of the person making the request, the certifier which issued the certificate should ordinarily be the person to suspend it, because the issuing certifier is in the best position to screen out and ignore requests that are obviously not in the subscriber's interest, such as requests intended as pranks, for

harassment, or for improper interference.

- *"suspend":* Since, by definition, a suspension cuts short an otherwise applicable time period, it relates only to certificates whose validity is determined according to time. If validity is measured by some other criterion, such as the scope of an identified transaction, this paragraph may well not apply.
- *"upon request":* The certifier must act in good faith in responding to the request, but need not conclusively confirm the identity or agency of the person requesting suspension. The certifier may rely on the representations of the person requesting the suspension, though there will be an element of verification of identity made by the certifier.

Commentary

- ✓ Since suspension temporarily invalidates a public key certificate, it, in effect, temporarily severs the association of the subscriber to the public key listed in the certificate. Without such an association, digital signatures verifiable by that public key are not attributable to the subscriber. The subscriber has thus effectively put its digital signature capability on hold.
- ✓ Although the certifier is not required to identify the authority of the person making the request, it should have some form of procedure in place for the immediate confirmation of such a request. Failing this, the certifier may find itself in breach of its obligations to the subscriber, and liable for any loss arising out of the subscriber's inability to use its digital signature.
- ✓ The ability to temporarily preclude attribution of digital signatures through suspension of the critical public key certificate is one of the principal means for the subscriber to manage the risk of holding a private key.
- ✓ A contract between a certifier and subscriber may limit or preclude suspension, so long as a person in a position to rely on the certification has notice of the limitation or preclusion. Such a limitation or preclusion could be included in a certification practice statement.

9. Revocation of public key certificate by request

The **certifier which issued** a public key certificate must **revoke** it promptly after:

(a) receiving a request for revocation by the subscriber named in the certificate or that subscriber's authorised agent, and

(b) confirming that the person requesting revocation is that subscriber, or is an agent of that subscriber with authority to request the revocation.

Clarification

- *"certifier which issued":* The certifier which issued the certificate should be the person to suspend it, because the issuing certifier is in the best position to confirm the identity and agency of the person requesting the revocation.
- *"revoke":* Since, by definition, a revocation cuts short an otherwise applicable time period, it relates only to certificates whose validity is determined according to time. If validity is measured by some other criterion, such as the scope of an identified transaction, this paragraph may well not apply.

Commentary

✓ The same comments as apply to the *"Suspension of a public key certificate by request"* will apply to a revocation, though evidently, a revocation is permanent, and can be regarded as an ultimate step.

10. Suspension or revocation of public key certificate without consent

The certifier which issued a public key certificate **must revoke** it, if:

(a) the certifier confirms that a material fact represented in the certificate is false;

(b) the certifier confirms that the trustworthiness of certifier's information system was **compromised** in a manner materially affecting the certificate's reliability.

The certifier may suspend a reasonably questionable certificate for the time necessary to perform an investigation sufficient to confirm grounds for revocation pursuant to this article.

Clarification

- *"must revoke"* If the certifier does not revoke the certificate, or at least suspend it pending investigation, and can be proved to have notice of any of the grounds listed above, then it follows that the certifier may be held liable for any consequential loss. Such failure to act may even bring into question the "Trust-worthiness" of the certifier vis-à-vis third parties.
- *"compromised"* That the information which must be secret in order to safeguard the operation of the authenticated message, has been revealed to parties who do not have the right to access such information.

Commentary

✓ It is anticipated that the exact parameters whereby a certifier would be entitled to suspend or revoke a certificate without consent would be established through the contract between the certifier and the subscriber. In the absence of such provisions, any court proceedings brought as a result of a loss occasioned would have to establish if the certifier was entitled to act in this way.

11. Notice of revocation or suspension of a public key certificate

Immediately upon suspension or revocation of a public key certificate by a certifier, the certifier must **give appropriate notice** of the revocation or suspension.

Clarification

- *"give appropriate notice":* In determining what is appropriate, the certifier should evaluate the circumstances and make reasonable efforts to deliver notice to persons likely to be significantly affected by the suspension or revocation. Ordinarily for a certificate published in a digital certificate repository, the certifier should likewise publish notice of the suspension or revocation in the same repository, in the manner specified by a standard adopted by the repository or a statement of procedures which it has published. For an unpublished certificate, the notice should reach persons

whose reliance on the certificate is foreseeable from the vantage point of the certifier and the person requesting the suspension or revocation. It is also possible that local laws may set out the procedure which should be followed, and parties should verify that there are not already specific provisions which apply.

Commentary

✓ If the certifier fails to give notice, then it may find itself at least in breach of its contract with the subscriber, or at worst liable for any loss arising out of the subscribers subsequent use in good faith of an invalidated key.

Glossary

XI. The core concepts

1. Agent

One authorized to carry on business or affairs for another. Within the electronic commerce environment, this may be implemented in software and run as an automated transaction.

Commentary

- ✓ Examples of such agents are Enterprise Resource Packages such as SAP, BAAN or Peoplesoft. These packages often achieve industry acceptance through experience rather than by formal independent review.
- ✓ The trustworthiness of the agent should be established before reliance is made upon it.

2. Authenticate

To record or adopt a digital seal or symbol associated with a **message**, with the present **intention of identifying oneself with the message**.

Clarification

- *"Authenticate":* In American usage, the term "authenticate" is often used to denote the act of identifying oneself with a message, but in European usage "authenticate" is more associated with the verification of a signature (see post). The first version of GUIDEC attempted to offer a solution to the potential confusion in the use of the word "Ensure", however in the rapid growth of electronic commerce the term "authenticate" has become more widely used. Regrettably, therefore, this revised version of the GUIDEC bows to the forces of customary use, and acknowledges the American meaning of the word. Readers are nevertheless warned of the dichotomy of meanings, and advised to make sure of the meaning when the term is employed.
- *"message":* This means only the message that is authenticated. If the message is altered (other than by the signatory with ratification), then there is no intention of the signatory to be identified with the message, and the authentication around the message does not apply to the alteration.
- *"intention of identifying oneself with the message":* The act of authentication may be founded on additional intentions besides the minimal identification of the signatory with the message. Often, it further indicates the signatory's approval of, or intent to be legally bound by, the message. Based on the expression of these various intentions through authentication, the law and/or commercial usage give the message a certain effect as the formally recognized act of the signatory; (see ante at IX – 2.: "Attribution and legal significance of authenticating a message"). Certification addresses the need for

guaranteeing the effectiveness of authentication, and some legal systems require it for certain messages, particularly when public filing is required or permitted, or the risks of false identification affect some other interest protected under a legal system's policy.

See UNCITRAL Model Law art. 6 (criteria for satisfaction of signature requirements), art. 11 (attribution of data messages) (1995); United Nations Convention on International Bills of Exchange and Promissory Notes art. 5(k) (1988) ("'Signature' means a hand-written signature, its facsimile or an equivalent authentication....").

Commentary

✓ Fundamentally and minimally, authenticating a message provides evidence that:
(a) the signatory had contact with the message; and
(b) the message has been preserved intact since it was authenticated.

Authentication may also indicate more, depending on the circumstances, or have legal significance deriving from an agreement or law. Further, most means of authentication provide only imperfect evidence of the signatory's contact and the message's integrity, and are vulnerable to forgery or tampering.

✓ A forged message that had been authenticated, altered without the signatory's authorization, creates no binding obligation on the signatory. It is void, or subject to being declared void at the instance of the purported signatory. In some legal systems, a spoilt message, one materially altered without its signatory's authorization, is traditionally considered void, and may not be enforced according to its original tenor. Preferably, and according to many other jurisdictions, tampering with a message is simply ignored, and the message may be enforced as originally authenticated.

3. Certificate

A **message authenticated** by a person, which message attests to the accuracy of **facts material to the legal efficacy of the act of another person**.

Clarification

- *"message authenticated":* A certificate is itself a message, and verifying its authenticity is ordinarily an important fact. In order for the certificate to be clearly reliable in commerce, the certifier creating it should exercise a degree of care exceeding the care for authenticated messages generally.
- *"fact material to the legal efficacy of the act of another person":* Examples of facts which may be the subject of certification include the identity of the person performing an act such as authenticating a message, circumstances affecting that person's existence as a valid legal entity, and/or the authority of a person to perform an act in question. A single certificate may attest to one or more such facts.

Commentary

- ✓ A variety of different types of certificates are recognized. Notaries of various legal systems issue certificates varying in form and effect, such as the public or authentic, and private forms of the civil law tradition, and the less rigorous "acknowledgement" of North American notaries. Technical computer standards typically envisage a certificate whose validity is measured according to a time period, whereas traditional certificates are valid on a per-transaction basis. Public key certificates as defined below are a specific type of certificate, but nevertheless fit within this general definition. This definition recognizes the often profound distinctions in the concept of a "certificate" but nevertheless seeks to focus on a common gist.
- ✓ A certificate does not, by definition, include an indication of the scope of its intended effect. A certificate valid for only one message or transaction fits this definition, as well as one valid for multiple transactions over a specified time. If a certificate is valid for only one message or transaction, it should so state and be clearly associated with that message or transaction. If a certificate is limited according to a time period, that time period should ordinarily be specified in the certificate.
- ✓ The content of a certificate depends on the type and purpose of the certificate, and is often prescribed by law or custom.

4. Certification practice statement

A **statement** of the practices which a certifier employs in issuing certificates generally, or employed in issuing a particular certificate.

Clarification

- ■ *"statement":* The statement may include a technical standard, rules of professional conduct or practice, laws applicable to the certifier, or a brand or mark representing other rules with which the certifier complies.

Commentary

- ✓ If a certification practice statement is not already well-known or agreed upon by the parties to a particular transaction, widely accepted by usage and generally well-known in the trade, or a matter of widely known custom and/or relevant national law, its form should be optimised to provide notice to relying parties and for efficient reference and utilisation. A certification practice statement need not necessarily be documentary in form; however, its expression should provide for a reasonably high degree of readability, accessibility, and efficiency. It should also make advantageous use of electronic means of delivery and presentation, if electronic means are contemplated for the transaction or material to it, in order to reasonably facilitate automated processing and/or computer-assisted look-up of important terms. A certification practice statement functions mainly as notice of a certifier's practices in issuing certificates, and a certifier acts untrustworthily and perhaps even in bad faith if an important portion of a certification practice statement is unreasonably obscure.
- ✓ The certification practice statement should not be confused with the certificate policy. The certificate policy (sometimes inaccurately and confusingly referred to as the certificate policy statement) is determined by the party who requires certification services of a third party. This is generally the organization that wishes to procure certification services. They would have determined

the level of controls required to provide appropriate protection for their transactions. A certification service provider would demonstrate their capability of providing services as required by the certificate policy through their certification practice statement. It is likely that each certification services provider would

only have one certification practice statement, but could demonstrably comply with multiple certificate policies. Essentially, the certificate policy is the statement of requirement of an organization, trade or other entity which requires to procure certification services; the certification practice statement is the public (or, in more detail, private) statement of practices followed by a provider of certification services.

✓ This document may serve as a guide for the contents and form of a certification practice statement.

5. Certificate policy

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Commentary

✓ For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range. Each digital certificate contains an identifier for the particular certificate policy applying to that certificate, and such identifier is a reference to a particular certificate policy definition. This method of including digital object identifiers in the certificate is the system by which those (including devices as well as humans and other entities) relying on the certificate will be able to determine which particular certificate policy definitions apply to and govern the technical and legal rules for use of the certificate.

✓ Not to be confused with certification practice statement.

6. Certificate revocation list

A list of revoked certificates, which is signed by the certifier and published.

7. Certifier

A **person** who issues a certificate, and thereby attests to the accuracy of a fact material to the legal efficacy of the act of another person.

Clarification

■ *"person":* is defined in this publication to include any physical being or legal entity capable of authenticating a message, and would therefore include corporations, partnerships, governmental agencies, and other legal entities. However, these non-physical entities have no human senses and cannot perceive certain facts, except through their human agents. Ultimately, therefore, the process of certification must be performed by human beings, although incorporeal legal entities may assist in providing facilities, services, and assistance.

Commentary

✓ Examples of certifiers include notaries, public key certification authorities (which may also include notaries and other trusted entities), and governmental officers and other persons.

8. Digital signature

A transformation of a message using an **asymmetric cryptosystem** such that a person having the authenticated message and **the signatory's** public key can accurately determine:

(a) whether the transformation was created using the **private key** that **corresponds** to the signatory's **public key**, and

(b) whether the signed message has been altered since the transformation was made.

Clarification

- *"cryptosystem":* This term signifies an information system employing cryptographic techniques to provide data security over communication channels that may not be secure. The data security thus provided includes the capability of associating a given message with a particular cryptographic key, and one or more operations for determining whether a given message is precisely the same as when the operation was previously performed.
- *"asymmetric cryptosystem":* An asymmetric cryptosystem, also often termed a "public key crypto-system", is an information system utilizing an algorithm or series of algorithms which provide a cryptographic key pair consisting of a private key and a corresponding public key. The keys of the pair have the properties that (1) the public key can verify a digital signature that the private key creates, and (2) it is computationally infeasible to discover or derive the private key from the public key. The public key can therefore be disclosed without significantly risking disclosure of the private key.
- *"the signatory's":* The signatory is the person employing the algorithm in order to be associated with the content of the message. This definition assumes that a cryptographic key pair has itself been associated with an identified person, so that the digital signatures created by that person can be reliably attributed to him by others. The association of a person with a key pair can be accomplished by a certificate identifying the person and including the person's public key. Such a certificate is termed a "public key certificate" in this document.
- *"correspond":* "Correspond", as used in this definition with regard to cryptographic keys, means to belong to the same key pair.
- *"private key":* In an asymmetric cryptosystem, the cryptographic keys are paired, as mentioned above. The private key is the one of the pair used to create a digital signature. It must therefore be available only to the signatory, and the signatory accordingly has a duty to maintain exclusive control over the private key; (see safeguarding an authentication device).
- *"public key":* In an asymmetric cryptosystem, at least one cryptographic key of a pair may be disclosed without making discovery of the private key possible. The key that may thus be disclosed is generally termed the "public key".

Commentary

- ✓ A digital signature differs from an electronic signature in that it is one type of electronic signature. The UNCITRAL Model Law on Electronic Signatures uses the following definition: "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message.
- ✓ Some methods of authenticating electronic messages do not employ an asymmetric cryptosystem. The results of such methods do not fall within the above definition of "digital signature". Thus, a digitally scanned image of a hand-written signature, a signature by means of a stylus and digitizing tablet, a name signed using the keyboard, the use of passwords or other techniques, such as biometrics, for controlling access, and similar procedures could be used for authenticating a message, but are not "digital signatures" as the term is used in this document.
- ✓ A digital signature should be securely and unambiguously linked to its message. As long as such a link is maintained, it is unimportant whether a digital signature is kept within the message, appended or prefixed to it, or retained in a separate electronic file or information system.

9. Hold a private key

To use or be able to use a private key.

Clarification

- ■ *"to use or be able to use":* The principal concept underlying this definition is availability or access as a matter of fact, rather than as a matter of right or legal entitlement. A person who obtains a key by theft, or who has access or use of the key subject to pre-emption by another, nevertheless "holds the key" as here defined.

Commentary

- ✓ Since the private key is essentially a device capable of creating a digital signature when used in an information system for the purpose, and since a digital signature can be considered as authenticating a message, the ability to use a private key for digital signature purposes must be limited to the signatory only. Holding a private key should therefore legally be the exclusive right of the signatory.
- ✓ Holding a private key may include an employment or other agency relation, or another legally recognised relation in which rights of custody and control (or ownership, if "property" is involved) are shared or divided in a manner recognised under applicable law. For example, a corporate employer may designate a private key for use by an employee in the name of the corporate employer. Digital signatures by that private key could well be attributable to the corporate employer by application of agency or authorisation principles, although the digital signatures would also be traceable to the employee. See also post *"authentication of a message by an agent"*.
- ✓ Ordinarily, a private key should have but one holder, unless holding is intentionally shared or divided. If an asymmetric cryptosystem is properly designed, implemented, and maintained, duplicate private keys occur rarely or not at all, unless a duplicate is obtained illicitly. If an unauthorized duplicate is

discovered, a holder should immediately suspend the certificate pending an investigation, and, depending on the outcome, revoke the certificate.

10. Human-readable form

A presentation of a **digital message** such that it can be perceived by human beings.

Clarification

- *"digital message":* The information processed by nearly all computer-based information systems is fundamentally variations in voltage, alternating magnetic polarities, pits on plastic, and similar approaches to representing digital bits in physical matter and electrical energy. As a practical matter, bits thus represented are imperceptible and unreadable by human beings, unless the information system presents them as symbols such as letters, numerals, punctuation marks and formatting.

Reference is made to the UNCITRAL Model Law art. 7 (1995) (satisfaction of requirements or preferences for the original).

Commentary

✓ A human-readable representation is not, by definition, rendered by a technologically reliable information system nor authenticated; in other words, this definition includes no assurance that the information system has accurately translated the message from its basic digital form into a human-readable form, or that that human-readable form is the same as another form perceived by a signatory of the message. Whether a message is represented the same as it was for its signatory generally depends on whether the signatory included parameters adequately specifying the human-readable representation within the authenticated message. See post *"in determining the scope of an authenticated message, variations in the form of the message may or may not be significant"*.

11. Issue a certificate

The process by which a certifier **creates** a certificate and gives **notice** to the **subscriber** listed in the certificate of its contents.

Clarification

- *"creates":* Creation of a new certificate does not imply formation of a new client relationship with the subscriber. For certificates whose validity is limited according to a time period, the new certificate may substitute for or "renew" an earlier one, which has expired or been revoked, or is about to expire or be revoked.
- *"notice"* and *"subscriber"* see post. Issuance of a certificate does not necessarily guarantee effective delivery.

Commentary

✓ Certain civil law legal systems or national customs may prescribe the manner in which a certificate may be issued, particularly for specific transactions. Civil law legal systems generally require that a notary officiate at certain types of transactions in which certificates are issued. Civil law notarial

practices often include detailed inquiry into the parties' intent and the transactional context, in order to be certain that the parties are fully informed about the consequences of their transaction.

12. Notice

To communicate **information** to another person in a manner **likely under the circumstances to impart knowledge** thereof to the other person.

Clarification

- *"information":* Notice could occasion a claim for intentional or negligent misrepresentation, should the information prove to be inaccurate. Care by the notifier in drawing conclusions may be appropriate. A notifier may inform the recipient of relevant evidence or of an uncertain event, and leave the recipient to determine whether to rely on the notice as accurate. The recipient is often in the best position to weigh the indications and uncertainty in light of its risks.
- *"likely under the circumstances to impart knowledge":* A duty to notify may be satisfied, even though the intended recipient of the notice fails to become aware of its contents, provided that the notifier acts in good faith and takes action which, in the ordinary course of business, should suffice to cause the notice to be delivered to the intended recipient and come to its attention.

  The International Institution for the Unification of Private Law (UNIDROIT) Principles of International Commercial Contracts art. 1.9 (1994) note:

  > Where notice is required it may be given by any means appropriate to the circumstances.
  > (1) ……
  > (2) A notice is effective when it reaches the person to whom it is given.
  > (3) For the purpose of paragraph (2) a notice "reaches" a person when given to that person orally or delivered at that person's place of business or mailing address.
  > (4) For the purpose of this article "notice" includes a declaration, demand, request or any other communication of intention.

  Comment 4 of the same article states in defining "reach" that notice reaches the addressee

  > as soon as [it is] delivered...to [the addressee's] place of business or mailing address. The particular communication in question need not come into the hands of the addressee. It is sufficient that it be ... received by the addressee's fax, telex or computer.

  In an electronic setting, dispatching a reliably authenticated message addressed to the intended recipient through a technologically reliable system, without apparent error, should suffice as a means of notification, unless the parties agree otherwise.

Commentary

- ✓ If the parties have formed a contract, it or a general contractual duty of good faith may well include a notice requirement, and perhaps an agreed-upon definition better tailored to the parties. However, the parties may also find themselves in a pre-contractual state, and the authentication of a message or certification which is the subject of the notice is part of an effort to form a contract or satisfy the form requirements for a contract. In such a pre-contractual setting, a duty to refrain from misrepresentation or to bargain in good faith, or the doctrine of culpa in contrahendo supply and define a basic require-ment of notice.

13. Person

A human being or any **entity** which is either:
(a) recognized by applicable law as capable of authenticating a message; or
(b) capable of authenticating a message as a matter of fact.

Clarification

- *"entity":* Information systems and other devices are not "entities" as the word is used in this definition. Rather, such systems and devices are the instruments of the persons who own and operate them.

14. Public key certificate

A certificate **identifying** a **public key** to its subscriber, corresponding to a private key held by that subscriber.

Clarification

- *"public key":* Public keys can be used by a person having a digital signature to determine which private key created the digital signature and whether the signed message was altered since it was signed. See ante "digital signature" and post "verify a digital signature".
- *"identifying":* The process whereby the certifier ascertains the veracity of the statements made in the certificate.

15. Relying Party

A recipient of a certificate who acts in reliance on those certificate and/or digital signatures verified using that certificate.

16. Repository

A computer-based system for storing and retrieving certificates and other messages relevant to authenticating a message.

Commentary

- ✓ A digital certificate repository may be provided by a firm specialized for such a business, in conjunction with services as a certifier or other person involved in electronic commerce. A digital repository is distinct from a repository of messages on paper.

17. Revoke a public key certificate

The act of a certifier in **declaring** a public key certificate permanently invalid from a specified **time** forward.

Clarification

- *"declaring":* Revocation is a mere declaration, and does not include destruction of the invalidated certificate. The invalidated certificate remains available for verification of digital signatures effected while the certificate was still valid.
- *"time":* This definition presumes that the validity of the public key certificate is limited to a specified period of time, which revocation cuts short. Public key certificates whose validity is limited to a particular transaction or by other criteria could perhaps be invalidated after issuance, but this document would not term such invalidation "revocation".

Commentary

- ✓ Although not an element of this definition, notice (see ante for definition) is required for a revocation.
- ✓ The declaration is often made using a certificate revocation list, which is posted to the same directory as the certificate. Other mechanisms for declaring revocation include the On-line Certificate Status Protocol (OCSP).

18. Signatory

The person who authenticates a message.

Commentary

- ✓ This is the issuer of the message, who, by authenticating it, has evidenced his intention of identifying himself with it. In this context, see the definition of *"Person"* (post). In the case of a digital signature, the signatory is the person employing the algorithm in order to be associated with the content of the message.

19. Subscriber

A person who is the **subject of a certificate**.

Clarification

- *"subject of a certificate":* Not every signatory is a subscriber, since not every authenticated message has an associated certification. "Subscriber" may well refer to a signatory, but as the subject of a certificate, rather than as a signatory per se.

Commentary

- ✓ For example, if a public key certificate states, either explicitly or by some form of incorporation:

  > I hereby certify on this 15th day of May 2001, that John William Thompson of 38 Cours Albert 1er, 75008 Paris, France, personally appeared before me and was identified by .... Further, the same John William Thompson demonstrated to me that he held the private key corresponding to the following public key ....

  then John William Thompson is the subscriber of that certificate.

- ✓ In some instances, a subscriber may consist of a person acting by the authority of another. Thus, the above example could include the following:

  > The same John William Thompson also produced a resolution of the XYZ Corporation SA, which I authenticated by .... Said resolution, a copy of which is attached hereto, authorizes the said John William Thompson,, to act in certain matters on behalf of XYZ Corporation SA as its authorized signatory.

  Authenticating a message by the private key corresponding to the public key listed in the certificate would, by application of domestic agency law, be legally recognized as authenticating a message of the principal through an act of the agent.

- ✓ A subscriber is generally also a client of, or under contract with, a certifier.

20. Suspend a public key certificate

The act of a certifier in declaring a public key certificate temporarily **invalid** for a specified **time** period.

Clarification

- *"invalid":* If the certificate is invalid, then it cannot be relied upon by a third party, though this does not preclude the legal concept that if the relying party has acted reasonably (see *"clarification"* post) or in good faith in relying upon the certificate, then the fact that it is suspended does not prejudice that reliance.
- *"time":* This definition presumes that the validity of the public key certificate is limited to a specified period of time, which suspension cuts short. Public key certificates whose validity is limited to a particular transaction or by other criteria could perhaps be invalidated after issuance, but this document would not term such invalidation "suspension".

21. Technologically reliable

Having the qualities of:

(a) being **reasonably** secure from intrusion and misuse;

(b) providing a **reasonable** level of availability, reliability, and **correct operation**.

Clarification

- *"reasonably ... reasonable":* The reasonableness standard of this definition reflects the fact that security exists in varying degrees, and should ordinarily be evaluated in light of the circumstances. A greater or lesser degree of security is possible in nearly all situations, much like public streets can always be made safer or airports more secure. In a case, therefore, the question should be, not whether the defendant could have done more, but rather whether the defendant exercised an appropriate degree of care in the design, maintenance, and operation of the system in question, taking into account the feasibility and cost of additional measures and the benefits they would have provided under the relevant circumstances. It should be noted that the use of the concept of *"reasonable"* can be problematic in Civil Law jurisdictions, although *de facto* the standards of a *bonus pater familias* or an *orderly businessman* can be used to adhere more closely to the concept.
- *"correct operation":* What sort of operation is "correct" for a system depends on design specifications of the system. The expectations of a user of the system should be considered in light of what can reasonably be expected from the system, given the limits in its design and production, to the extent that those limits are made known to the user.

Commentary

✓ The objectives of a technological reliability are, in essence:
- *Confidentiality:* Securing information so that it is not disclosed or revealed to unauthorised persons.
- *Integrity:* Securing the consistency of data; in particular, preventing unauthorised creation, alteration, or destruction of data.
- *Availability:* Securing access to information and resources so that legitimate users are not unduly denied it.
- *Legitimate use:* Securing resources so that they are used only by authorised persons in authorised ways.

22. Trustworthy

Conducting business in a manner that warrants the trust of a reasonable person active in commerce, and having capabilities, competence, and other resources which are **sufficient** to enable performance of one's legal duties, and assure unbiased action.

Clarification

- *"sufficient":* The sufficiency of a person's capabilities, competence, and resources and the sufficiency of one's disinterest should both be tested according to standards of reasonableness. In any case, greater effort and investment will have been possible, but the question is whether a reasonable person under the circumstances would have expended the additional effort and investment to obtain greater capabilities, competence, or absence of bias.

Commentary

✓ Trustworthiness is a central concept to all business relationships, and is not a concept that can be closely defined. The commercial assessment of the risk involved in a certain transaction will always

have a central role to play. Of course, there exist professions, such as that of a notary, which remove much of the element of risk in establishing the legal bona fides of a signature by issuing a certification which takes the responsibility for the accuracy of the facts contained therein out of the hands of the receiving party. Indeed, a notary will remain liable for any statements made in a certificate notwithstanding the fact that there is no contractual relationship between him and the party relying on the statements made.

✓ It will be a matter of commercial risk assessment whether or not a person will rely upon a certification where the signatory, subscriber and even certifier all lie within the same group. Paper-based examples such as the credit card industry have historically provided examples of unbiased performance of legal duties, despite acting in several roles in a transaction.

23. Valid certificate

A certificate which its certifier has issued or disclosed to another person in circumstances where that person's reliance on the certificate is foreseeable, unless the certifier **gives** timely **notice** that the certificate is unreliable, or unless the certificate is a public key certificate which has been revoked or is, at the time in question, suspended.

Clarification

■ *"gives notice":* The notice must reach all persons who are in a position to rely on the certificate.

Commentary

✓ A certifier may seek to restrict liability for the contents of a certificate issued either through the contractual relationship with the subscriber, or by means of a general disclaimer in the practice statement, or even in the certificate itself. Care should be taken, however, of restrictions on such disclaimers that some jurisdictions regard as unfair or invalid contract terms. This is especially the case in transactions that are deemed to be "consumer".

24. Verify a digital signature

In relation to authenticating a given message (digital signature, message, and public key), to determine accurately that:

(a) the digital signature was created by the private key corresponding to the public key; and

(b) the message has not been altered since its digital signature was created.

Clarification

■ *"Verify":* If a recipient person does not verify the said information, then reliance cannot be made upon the infrastructure mechanisms which have been created for just that purpose, and for securing the security of the message.

Commentary

- ✓ This is, of course, the central element in relying upon an authenticated message with a digital signature.

Conclusion

It is intended that the GUIDEC serve as a foundation document in the application of digitally authenticated electronic commerce, but it is freely acknowledged that we cannot hope to have addressed all of the issues at once. The whole field of electronic commerce is evolving at a rapid rate, and it is necessary that the concepts and definitions inherent thereto also evolve at an equivalent pace. ICC's ECP will therefore seek to apply the definitions and principles as set out in the GUIDEC through further studies into the subject as it is enumerated here, and address itself to additional problems in the field as they continue to be identified. As technology develops, and the commercial world attempts to embrace such technological developments, further revisions and enhancements of this document will be made available, in order that the inevitably complex concepts can be readily understood by the business community, and put to the best use.

Appendix

1. What is public key cryptography?

Public key encryption assures two things for commercial actors:
a) that their messages are secure, and
b) that other transacting parties are authenticated.

Using this technology, senders and receivers of electronic messages each possess two keys – a public key and a private key – one of which is never shared with anybody, and the other of which is shared with everyone. These two keys correspond to each other, so that whatever is encoded with one key can only be decoded by the other. In the encrypting process, the sender of the message encodes it with the recipient's public key (which has been shared with him and all other parties), making it impossible for any party other than the one holding the private key to decrypt the message. Encryption protects the message from all parties other than the recipient, without the recipient having to divulge his private key to the sender.

By reversing the process described above, public key cryptography also provides a highly dependable mechanism, known in the GUIDEC as "authenticating a message", or within a public key infrastructure as a "digital signature". This authentication, or digital signature, is an attachment to a set of data which is composed by taking the output of a hash function, or digest, of the original data that is encrypted with the sender's private key. The hash function puts the original data through an algorithm, resulting in a data sequence unique to a particular message but much shorter than the message itself. The resulting digital signature can only be decrypted if the recipient has the correct public key, thereby permitting a recipient to verify the identity of the sender. In a given transaction, therefore, the sender encrypts the message with the public key of the recipient, and digitally signs or authenticates the message with his own private key, and the recipient uses his private key to decrypt the message, and the public key of the sender to verify the message authenticated.

Because an authenticated message is difficult to forge, its use binds the signatory, precluding a later repudiation of the message. Digital signature technology also forms the basis for forming legally binding contracts in the course of electronic commercial transactions since it can provide electronically the same forensic effect a signed paper message provides.

Authentication and Certification Authorities
The use of public key cryptography for digital signature purposes require that a trusted third party establish that holders of public keys are indeed who they purport to be. Without a trusted third party certifying that a given individual is in fact the holder of a public key, it is impossible for other transacting parties on the network to know for certain that the holder of the public key is not an impostor. This third party, known in the GUIDEC as a certifier, will form the trust backbone for all types of commercial and non-commercial transactions taking place over open networks. Certifiers will certify the identity of the public key holder, and publish and update public keys, in a process referred to as certificate issuance. The effectiveness of the

authentication process depends upon establishing certifiers to provide parties with a means for reliably associating the public and private key pair with an identified person, and a trustworthy means of ascertaining the public key needed for verification. Given the importance of the accuracy of the information provided by the third party institution (i.e. the public key of the sender), the certifier should be sufficiently trustworthy to assure a high level of trust in electronic commercial transactions. In communications among different organizations, a certification authority must be an institution trusted by all parties relying on its information. To provide further assurance of actual trustworthiness, a hierarchy of certification authorities may need to be established to ensure that individuals comply with rules, such as those articulated in the GUIDEC. In a hierarchy of multiple certifiers, each certifier has an authenticated text certified by the certificate authority above it, forming a certificate chain to assure that sub-certifiers are identifiable.

Because certificates issued by certifiers will essentially be guarantees of the certificate holder's commercial identity, laws are currently being developed which prescribe clear rules and liabilities for certifiers. This document outlines the general set of international rules that govern authentication and certification for commercial applications. The GUIDEC is designed to restate and harmonize existing law and practice relating to the particulars of the authentication, certification, and verification process.

2. XML development

The causes of this development lie in relative advantages of XML messages:

· **Flexibility and extensibility**:
XML message forms can be as standardized as users want them to be. There is no general insistence that a myriad of different forms be exhaustively and finally standardized in every detail. Rather, XML defines the minimal form requirements necessary to parse[1] the message, including elements within it that the parsing computer may not be set up to recognize. When the parsing computer encounters an unrecognized element, it can take a variety of actions depending on the nature of the transaction.[2] The result is a message form that can be standardized to the extent standardization is useful, while remaining as flexible and extensible as possible.

· **Readily available commercial software:**
EDI systems required extensive engineering, including customization, before they were useful; however, XML applications work using off-the-shelf software. World Wide Web browsers can display XML documents, and parsing scripts can process them in background applications that update databases and other information stores. The know-how that has emerged from the Web for processing XML documents is widespread, in contrast to the more arcane and specialized world of EDI. XML thus brings electronic commerce into the mainstream and makes it as ubiquitous as the Web itself.

1 'Parsing' refers to the process by which a computer scans a message and determines its structure and components. The components may be textual elements such as headings, paragraphs, emphasised text, etc., or data elements such as a stock number, quantity, price, and description. XML prescribes a flexible methodology for specifying how elements are to be arranged in relation to each other. The limits of that flexibility are set by the bounds of what software can be made to parse, in other words, by what is said to be 'well formed' in XML jargon.

2 For example, if the parties have agreed that a receiving party need not treat unrecognised elements as significant, the receiving party may ignore element outside a specified set. A sending party then remains at liberty, however, to invent elements for it's own or another party's use. Groups of users may also upgrade to improved functionality without making older applications incompatible with the evolving state of the art.

- **Ease of use:**

Human eyes have difficulty making sense out of older messages. Their contents are not labelled, and the reader must know the standardized sequence prescribed for the given message type to know the significance of the information in the message. XML, on the other hand, tags the beginning and end of every element in the message, and the tags are ordinarily mnemonic. Because XML is based on the same technology as the familiar HTML, it is easy to learn.

· **Robust information-carrying structures:**

Older message forms were quite linear in their logical structure, but XML messages can also be logically tabular (repeated sequences of the fields), nested (fields encapsulated in other data objects), or fully documentary, or a mixture of logical structures. For example, data fields that can readily be input into or drawn from a database can be embedded within the text of a document easily read by human beings. They can also be embedded into a form that people can fill in, and the filled-in data can be similarly labelled and manipulated.

3. ILPF analysis of international electronic and digital signature implementation initiatives

A study prepared for the Internet Law and Policy Forum (ILPF)
September, 2000
by

The Brussels office of
Morrison & Foerster LLP
Chris Kuner (ckuner@mofo.com)
Rosa Barcelo (rbarcelo@mofo.com)

The Washington, D.C. office of
Steptoe & Johnson LLP
Stewart Baker (sbaker@steptoe.com)
Eric Greenwald (egreenwald@steptoe.com)

ILPF and the authors seek public comment on this analysis and welcome additional information and corrections concerning the initiatives discussed in this report. We particularly encourage readers to submit information about new implementation initiatives that are not discussed in this analysis. Any comments should be sent to the ILPF (implementation@ilpf.org) and to the authors, Stewart Baker and Chris Kuner.

Executive summary

Many jurisdictions have been setting up implementation schemes designed to provide technical guidance to allow the general legal framework for electronic authentication to work in practice. Such schemes may include (1) national and international standards for electronic authentication products and services; (2) regulatory schemes for the supervision, accreditation, and certification of particular authentication products and services; and (3) guidelines, best practices, and similar documentation for the operation of electronic authentication systems. Such schemes may be set forth in national legislation, international or regional regulatory principles, guidelines drafted by commercial or policy organizations, or other initiatives.

When one looks more closely at such schemes, a number of trends emerge:

- Information about them is often difficult to come by.
- The majority of countries with laws on electronic authentication have not yet developed detailed standards, although a number are working on them.
- In those countries where accreditation or certification schemes for electronic authentication exist, the vast majority at least purport to be "voluntary". On the other hand, many laws require the use of accredited Certification Service Providers ("CSPs") in transactions with the government, which can have a powerful effect in forcing a particular standard or accreditation procedure on the market.
- While almost all the laws give basic legal effect to electronic signatures independent of the technology used, very often the most important legal effects are only recognized when the certificate is issued by a service provider that is accredited or certified in some way, or that meets certain standards.
- A number of countries are currently struggling with the issue of whether to establish a supervisory body for all authentication products and services.
- Many countries also require CSPs to register in some way before starting their activities.
- In countries where standards are adopted or in the process of being adopted, it is often difficult to ascertain the extent to which they are truly international in nature.
- It seems that the evolving definition of "accreditation," "certification," and "standardization" in the context of electronic authentication is a flexible one, which should be implemented in national systems in a way which furthers truly international and interoperable electronic commerce.

However, the evidence so far is that both the plethora of such initiatives, and the way they are being implemented, is not developing in a way which would optimize the use of electronic signature technologies. Nearly every country has at least initiated a national accreditation, certification, or standardization scheme for electronic signature products and services, which could lead to a Babel that imperils international legal interoperability. There is also evidence that some of them are not as "international" as they purport to be, and that there is sometimes more governmental involvement in what are supposedly "private sector" standards than is warranted. In part, of course, this reflects a determination on the part of some governments to seize the initiative in this field even before a strong private-sector market has emerged.

Table of contents

Table of contents *(continued)*

PART I . Introduction

1. Background

Over the past few years, changes in law and advances in technology have dramatically altered the landscape of electronic authentication. Although use of the technology is not yet widespread, electronic authentication holds the promise of fostering, at a minimum, a modest transformation in online commerce to, at a maximum, a radical shift in the way business is conducted. Digital signatures and the operation of public key infrastructures ("PKIs") promise drastically-reduced transaction costs in virtually every sector of business. Companies and consumers alike welcome the day when the click of a button can complete high-value transactions that previously required hours of deliberation and hundreds of documents.

While the benefits of authentication technologies have long been apparent, the method of achieving these commercial gains has been decidedly less obvious. Legislatures and regulatory agencies around the world have taken various and divergent approaches in their effort to take advantage of these emerging technologies. Much of this divergence stems from the simple fact that these technologies have yet to fully evolve. Electronic signatures currently claim only limited acceptance in the marketplace; thus, policy-makers are left with the task of predicting how e-signatures will be used, rather than reacting to how they are used. Differing policies reflect differing assumptions about the future of these technologies and how best to influence them.

A review of legislative and regulatory activity reveals three basic approaches. [1] The first, a minimalist approach, aims to facilitate the use of electronic signatures generally, rather than advocate a specific protocol or technology. The primary motivation is to remove existing legal obstacles to the recognition and enforceability of electronic signatures and records. This is ordinarily done by ensuring that electronic signatures and records fulfill existing legal requirements for tangible signatures. To the extent that there are any legislative or regulatory judgments involved in this approach, they are generally limited to defining the circumstances under which an electronic signature will fulfill any such requirements, with a goal of establishing a standard of proof. To this end, the minimalist approach focuses on verifying the intent of the signing party rather than on developing particularized forms and guidelines.

The second approach tends to be more prescriptive. Here the motivation often stems from a desire to establish a legal framework for the operation of PKIs - whether or not other forms of secure authentication are included or permitted - as well as a reflection of form and handwriting requirements that apply in the offline world. Legislation and regulations enacted under this approach often share the following characteristics: adoption of asymmetric cryptography as the approved means of creating a digital signature; imposition of certain operational and financial requirements on certificate authorities ("CAs"); prescription of the duties of key holders; and definition of the circumstances under which reliance on an electronic signature is justified. This prescriptive approach allows legislatures and regulatory agencies to play a direct role in setting standards for and influencing the direction of new technologies.

The record on adoption of these approaches falls closely in line with the systems of law in which each has evolved. Traditional common law countries – e.g., Canada, the United States, the United Kingdom, Australia, and New Zealand - have tended toward a minimalist approach. The United States, despite initial contrasting approaches among individual states, has largely resolved the tension by opting for the minimalist approach on a national level. The recently adopted Electronic Signatures in Global and National

Commerce Act ("E-SIGN") represents an affirmation of the minimalist approach. The law gives electronic signatures the same legal validity as traditional paper signatures and explicitly forbids the denial of an electronic agreement simply because it is not in "writing". To prevent conflicting state level approaches, the law further forbids any state statute or regulation that limits, modifies, or supersedes E-SIGN in a manner that would discriminate for or against a particular technology. Of course, states can preserve (or adopt) laws that offer an approach slightly different from that of the new federal law, but only where that variance is consistent with the overall terms of E-SIGN.

In contrast, civil law countries have tended to opt for the prescriptive approach. For example, the original German Digital Signature Law established stringent technical standards for what types of digital signatures are to be deemed "secure". Italy took this a step further by conveying legal effect only to signatures that have been authenticated by a licensed CA. Other nations including Argentina and Malaysia have enacted similar legislation outlining the circumstances in which digital signatures may be used.

Some jurisdictions have also begun to realize that the first two approaches are not necessarily mutually exclusive, and so have adopted a third approach. The result has been a "two-tier" approach representing a convergence and synthesis of the two approaches. This consolidated approach generally takes the form of enacting laws that prescribe standards for the operation of PKIs, and concomitantly take a broad view of what constitutes a valid electronic signature for legal purposes. The virtue of this approach is that it achieves legal neutrality by granting at least minimum recognition to most authentication technologies, while at the same time creating a better-defined, more predictable legal environment by incorporating provisions for an authentication technology of choice.

This "two-tier" approach has found increasing support, most notably in the European Union. At the minimalist level, the EU Digital Signatures Directive prohibits EU Member States from denying legal effect to an electronic signature solely on the grounds that it is in electronic form, or on the grounds that it does not satisfy the standards set forth elsewhere in the directive for "advanced" electronic signatures. At the prescriptive level, the Directive affirmatively requires the Member States to give legal effect to "advanced electronic signatures" that are based on "qualified certificates" and that are created by "secure signature creation devices". Singapore's Electronic Transactions Bill takes a similar approach, and distinguishes between technologies based on levels of security by establishing one legal treatment for "electronic signatures," and another for "secure electronic signatures". The "electronic signatures" are generally given minimum legal effect, while the "secure electronic signatures" are entitled to an additional presumption of integrity, a presumption that the signature is that of the person with whom it is associated, and a presumption that the user affixed the signature with the intent of signing or approving the document.

Despite increasing reliance on the "two-tier" or "hybrid" method, there remains a wide divergence between the minimalist and prescriptive approaches. This international - and in some cases even domestic - policy divergence could severely limit the recognition and interoperability of electronic signatures and certificates across borders, with far-reaching consequences. For instance, as the Organization for Economic Cooperation and Development has recognized in its own work to identify the barriers to electronic authentication, the growth of competing legal and technical frameworks could result in an intricate and unworkable maze of conflicting standards; divergent legal requirements could effectively erect barriers to international trade; and a system in which each country prescribes its own standards could inhibit mutual recognition and cross-certification requirements.

2. The ILPF International Consensus Principles

Motivated by the belief that "legal interoperability" is essential to realizing the potential gains of electronic commerce, the ILPF has devised a set of International Consensus Principles on Electronic Authentication[2] designed to create a predictable legal environment. Based on a "crystallization" of salient policy principles from electronic authentication regulations around the world, the Principles attempt to cut a middle ground between the divergent approaches. Since many of the considerations articulated in the Principles are relevant when analyzing implementation initiatives for digital and electronic signatures, the Principles are quoted here:

- **Remove legal barriers to electronic authentication**
  Governments should identify and remove legal barriers that hinder the recognition of electronic authentication. An electronic authentication should not be denied legal effect solely because of its electronic form.
- **Respect freedom of contract and parties' ability to set provisions by agreement**
  To the fullest extent possible, national laws and jurisdictions should recognize and give full legal effect to contractual agreements concerning the use and recognition of electronic authentication techniques.
- **Harmonization: making laws governing electronic authentication consistent across jurisdictions**
  Legal rules relating to electronic authentication should be made to operate collaboratively and provide consistent results across jurisdictions to promote the growth of electronic transactions and establish a predictable legal environment for the use and recognition of electronic authentication methods.
- **Avoid discrimination and erection of non-tariff barriers**
  Governments should recognize that their actions with respect to electronic authentication can create barriers to trade. Governments should not unreasonably discriminate against electronic authentication methods or providers from other jurisdictions or erect improper non-tariff barriers to trade.
- **Allow for use of current or future means of electronic authentication**
  Governments should not require or unduly promote the use of particular electronic authentication means or technologies.
- **Promote market-driven standards**
  Standards for use of electronic authentication methods or technologies should be market-driven to meet user needs.

3. Goals of this paper

The above discussion has centered on the broad policy framework for electronic authentication, which has now been set up in many jurisdictions by the myriad electronic and digital signature laws and regulations in force or planned around the world. However, perhaps the more difficult exercise will be to make these policy schemes work in practice, i.e., to further the creation of a global, seamless, legal framework for electronic authentication, while at the same time ensuring that they work at the local level as well. Since much of the relevant legislation and regulation is so broadly formulated, many jurisdictions have been

setting up various implementation schemes designed to provide the detailed technical guidance to allow the general legal framework for electronic authentication to work in practice. Such schemes may include, for example:

- National and international standards for electronic authentication products and services;
- Regulatory schemes for the supervision, accreditation, and certification of particular authentication products and services (e.g., for accreditation of certification service providers); and
- Guidelines, best practices, and similar documentation for the operation of electronic authentication systems.

Such schemes may be set forth in national legislation, international or regional regulatory principles, guidelines drafted by commercial or policy organizations, or other initiatives.

The remainder of this paper will continue to build upon the above discussion, in order to provide an overview of the direction in which such implementation schemes are proceeding, to analyze the similarities and the differences between the various approaches, and to provide further insight into not simply the content, but also the effectiveness of current legislative and regulatory efforts. This paper concludes with a table containing a brief description of major implementation initiatives in the area of electronic authentication currently going on around the globe.

What follows is not a set of answers, but rather an effort to narrow the subject into a workable framework for readers to identify and analyze a set of useful questions. A primary goal is to help readers organize a coherent view of how various approaches toward accreditation, certification, and standardization both do and should operate and interact. The classification of approaches reflects an attempt to create for the reader a system of organizing principles out of a vast array of approaches. By pushing readers to formulate a sense of how various approaches help achieve legal interoperability on either a local, national, regional, or global scale, it is hoped that conclusions can be reached on the effectiveness of the various schemes themselves.

To this end, readers are encouraged to reflect not only on the adequacy of the minimalist and prescriptive approaches, but also on the adequacy of various efforts to set standards or set up certification or accreditation schemes within each of the approaches. Such standards or regulatory schemes generally develop in three ways. Often a national or regional legislature sets forth the standards, either by mandating specific methods or by explicitly clarifying that no specific standard will be adopted. Alternatively, standard setting bodies - trade groups, regulators, non-governmental organizations - may develop their own sets of standards. Finally, commercial organizations frequently play a crucial role in setting standards, not through formal policymaking but through the development and application of the products or services to be standardized and the systems in which they will operate - in this case, electronic signatures and public key infrastructures.

It is important to note that these three methods of standard-setting/accreditation/certification act in conjunction with one another. Readers are thus encouraged to compare and evaluate their effectiveness, based on criteria such as:

- the extent to which the market is flourishing; the ease of successfully establishing regional or international interoperability;
- the prevalence of a particular standard or accreditation/certification scheme within a region; and
- the growth of a particular standard or scheme outside of the region in which it was established.

PART II. Analysis

Following passage of the Utah Digital Signature Law in 1995, the last few years have seen an explosion of legislative and regulatory work by governments in the field of electronic authentication. As detailed in the first section of this report, the ILPF, in its previous work, has examined and categorized the basic legislative approaches being used around the world. However, now that several years have gone by, it is easier both to categorize the types of approaches used and to understand the way in which accreditation, certification, and standardization regimes are being constructed to implement them.[3]

As is usually the case when dealing with the subject of electronic signatures, it is important to define the terminology used. As noted in the preface to the table (Part III of this paper), there is a great deal of confusion about the meaning of terms such as "technology neutral," "international standards," and "mandatory," which makes it difficult to apply clear and consistent criteria to the various implementation schemes that exist. This paper takes a pragmatic approach and uses terminology, which, hopefully, is both understandable and precise enough to allow meaningful discussion about the issues. Thus, for example, in describing whether an initiative is based on "international standards," use has been made both of long descriptive phrases, short responses such as "yes" and "no" (when this seemed clear), and more subtle responses such as "ostensibly" (when the standards are purported to be "international" by those in charge of the scheme, but there is evidence that this may not be fully the case).

The basic legislative approaches to electronic authentication currently in use are much the same as detailed in previous ILPF studies (and described in Part I), but the following points are worthy of emphasis:

- Some electronic authentication laws are focused uniquely on electronic signatures (for example, some of those that derive from the EU Electronic Signatures Directive), while others also cover contract formation and related issues. Of the latter category, many are based on the UNCITRAL Model Law on Electronic Commerce (e.g., the laws and draft laws of Argentina, Colombia, Ecuador, and Hong Kong). Almost all of the laws give basic legal effect to electronic documents and signatures (i.e., they exclude the possibility of not legally recognizing electronic signatures and documents merely because they are in electronic form), with the exception of certain types of documents or acts (e.g., wills).

- Most of the initiatives are, or at least purport to be, "technologically neutral," although the underlying methodology clearly involves PKI technology (e.g., the EU Directive, and the laws of Denmark, Spain, and Sweden). A few of the laws are openly PKI-based, such as the Italian law. Some countries have a general law on authentication that purports to be technologically neutral, and a more specific law applying only to communications with the government that is PKI-based (e.g., Belgium, France, and Luxembourg).

When one looks more closely at the accreditation, certification, and standardization initiatives described in Part III, a number of trends emerge:

- To begin with, there is often a general lack of transparency surrounding such schemes. Information about them is often difficult to come by, may only be available in the respective national language, and tends to be less than accessible to parties outside the country. These factors increase the risk that the scheme may be overly shaped by national or local interests, rather than by a desire to further international legal interoperability.

- The majority of countries with laws on electronic authentication have not developed detailed standards, although a number are working on them. It appears that many countries are adopting a "wait and see" attitude as they wait for either regional standards (for example many European countries are awaiting finalization of the EESSI project) or market standards (as seems to be the case in many South American countries) to emerge before finalizing their own.

- In those countries where accreditation or certification schemes for electronic authentication exist, the vast majority at least purport to be "voluntary"; very few have been found which are openly mandatory (Ecuador seems to be one). On the other hand, many laws require the use of accredited CSPs in transactions with the government, which can have a powerful effect in forcing a particular standard or accreditation procedure on the market.

- Many implementation schemes may have a greater effect in practice than might be supposed from their voluntary nature. In particular, while almost all the laws give basic legal effect to electronic signatures independent of the technology used, very often the most important legal effects are only recognized when the certificate is issued by a service provider that is accredited or certified in some way, or that meets certain standards. An example is provided by the EU Directive, which grants enhanced legal effect to electronic signatures that satisfy certain technical criteria (i.e., signatures that are based on "qualified certificates" and created by "secure signature creation devices," as defined in a set of annexes). While under this scheme all signatures and certificates are admissible in court, in practice the evidentiary hurdles for signatures that meet the criteria for enhanced legal effect will be lower, which could create a powerful de facto incentive to use them instead of other procedures.

- The use of accreditation and certification implies the existence of a mechanism to certify compliance. A number of such bodies are contemplated in various national schemes, with the EU scheme under the EU Directive providing a microcosm. Under the Directive, the Member States are supposed to designate their own "bodies" to certify compliance with the Annexes, under the general rules set forth by a committee composed of the Member States and the European Commission. So far, it seems that some Member States will leave the task of certifying compliance to a voluntary, industry-led body (e.g., Ireland, The Netherlands, and the UK), while others (e.g., Germany) will rely on a government agency.

- An issue related to certifying compliance with accreditation and certification schemes is that of supervision of signature products and services; i.e., by what means (if at all) those offering such services should be subject to oversight, whether by the government or by a private body. A number of countries (such as those in the EU) are currently struggling with the issue of whether to establish a supervisory body for all authentication products and services, and, if so, what form it should take. Anecdotal evidence suggests that several European governments are reluctant to go to the expense and trouble of establishing a government body for supervision, until it has become clear what direction the market is moving, and whether there is a need for such a body.

- Many countries also require CSPs to register in some way before starting their activities (e.g., Luxembourg and Spain); in some cases, this almost rises to the level of a licensing requirement. Furthermore, some countries have enacted legislation regarding additional functions of a CSP, such as time stamping functions (e.g., Austria).

- In countries where standards have been adopted or are in the process of being adopted, it is often difficult to ascertain the extent to which they are truly international in nature. While nearly every standardization scheme purports to be based on "international standards," a closer look at anecdotal evidence often reveals that they are not fully compliant with standards drawn up by international groups, and that they often incorporate national variants.

The latest iteration of the UNCITRAL Draft Uniform Rules on Electronic Signatures (as set forth in the "Draft Guide to Enactment")[4] demonstrates an emerging international consensus on the use of accreditation/certification/standardization schemes to determine enhanced legal effect. The draft includes an Article (Article 6) which defines criteria to determine when an electronic signature may be considered "reliable," and further provides that any such determination of reliability must be consistent with "international standards" (Article 7). The commentary in the Draft Guide to Enactment goes on to define "standards" as follows:

- With respect to paragraph (2), the notion of "standard" should not be limited to official standards developed, for example, by the International Standards Organization (ISO) and the Internet Engineering Task Force (IETF), or to other technical standards. The word "standards" should be interpreted in a broad sense, which would include industry practices and trade usages, texts emanating from such international organizations as the International Chamber of Commerce, as well as the work of UNCITRAL itself (including these Rules and the Model Law). The possible lack of relevant standards should not prevent the competent persons or authorities from making the determination referred to in paragraph (1). As to the reference to "recognized" standards, a question might be raised as to what constitutes "recognition" and of whom such recognition is required (see A/CN.9/465, para. 94).

  It thus seems that the evolving definition of "accreditation," "certification," and "standardization" in the context of electronic authentication is a flexible one, which should be implemented in national systems in a way which furthers truly international, and, hopefully, interoperable electronic commerce. Unfortunately, the evidence so far is that both the plethora of such initiatives, and the way they are being implemented, is not developing in a way that would optimize the use of electronic signature technologies.

- With regard to the number of such implementation schemes, it can be seen from the table (Part III of this paper) that nearly all of the industrialized nations have at least initiated a national accreditation, certification, or standardization scheme for electronic signature products and services. One must ask why so many, nationally-based schemes are necessary, and why there is not more reliance on a few, larger-scale schemes that could be tailored for a region, or a particular legal system. One could argue that competition will result among the schemes, leading to a "survival of the fittest," which may well be true to some extent. But, at the same time, having nearly every country adopt its own implemen-tation scheme for electronic signatures carries the risk of leading to a patchwork of inconsistent national systems that may well imperil international legal interoperability.

- With regard to the way in which these myriad schemes are presently being implemented, there is evidence that at least some of them are not as "international" as they purport to be. There is also some-times more governmental involvement in what are supposedly "private sector" standards than one would think was warranted.

These concerns suggest that vigilance is called for in ensuring that national or regional implementation

schemes do not stifle potential growth in the use of signature technologies. On the positive side, the existence of several large-scale, international schemes based on system rules agreed to among the parties can act de facto as a restraining factor on more parochial implementation schemes.

PART III. Table of digital and electronic signature implementation initatives

The following is a table of current accreditation, certification, standardization, and similar initiatives around the world in the area of electronic authentication. It is not intended to be exhaustive, but to provide the most important information about a representative selection of initiatives.

It has been exceedingly difficult to formulate standard terminology in some areas (e.g., in describing the technology used, or whether an initiative is based on international standards), but the authors have gone to great pains to devise descriptive, easily-understandable terms, and to use the same terminology for similar initiatives. Even if the results are not perfectly uniform, they should be descriptive enough to give a reasonably clear sense of what is meant.

Finally, readers will note that the table includes certain policy initiatives (such as the UNCITRAL Model Law and Model Rules, the ILPF papers, and the ABA Digital Signature Guidelines) and electronic authentication legislation (such as the U.S. E-SIGN Act). Although these initiatives do not contain standardization, accreditation, or certification programs for electronic signature products or services, it was decided that such initiatives and legislation should be included because of their underlying importance for many of the implementation initiatives described herein.

The authors wish to thank their correspondents around the world who kindly provided information, without which this table would not have been possible.

1. International organizations and business entities

i) IDENTRUS

URL	http://www.identrus.com
Project	Bank certification network for financial and e-commerce transactions.
Technology	PKI.
Based on international standards?	Yes.
Status	Ongoing project.
Application	Global.
Mandatory?	No.
Summary of provisions	The network offers a standard for B2B transactions between financial institutions.
Relevant supervisory body	Identrus, though its system rules. Initial members include ABN AMRO, Bank of America, Barclays Bank, Canadian Imperial Bank of Commerce (CIBC), Chase Manhattan Bank, Citigroup, Commerzbank, Deutsche Bank, HSBC Group, Hypo Vereinsbank, The Industrial Bank of Japan Limited (IBJ), Royal Bank of Scotland Group, Sanwa Bank, Scotiabank, and Wells Fargo Wholesale Internet Services.

ii) International Chamber of Commerce (ICC)

URL	http://www.iccwbo.org
Project	General Usage in International Digitally Ensured Commerce (GUIDEC).
Technology	Neutral formulation.
Based on international standards?	Yes.
Status	Issued November 6, 1997. Under revision this year
Application	Global.
Mandatory?	No.
Summary of provisions	Addressing specifically the use of digital signatures, the GUIDEC specifies core concepts, best practices and certification issues in the context of international commercial law and practice.
Relevant supervisory body	The ICC Information Security Working Party.

iii) International Telecommunication Union (ITU)

URL	http://www.itu.int/
Project	Development of global digital signature standards.
Technology	Primarily PKI X.509, though the ITU has developed (and continues to work on) other related standards.
Based on international standards?	Yes.
Status	Ongoing.
Application	Global.
Mandatory?	No.
Summary of objectives	Headquartered in Geneva, Switzerland, the ITU is an international organization within which governments and the private sector coordinate global telecommunication networks and services. The ITU Telecommunication Standardization Center (ITU-T) studies technical, operating, and tariff questions and adopts Recommendations with a view to standardizing telecommunications on a worldwide basis. ITU-T is comprised of over twenty Study Groups and Telecommunication Standardization Advisory Groups. The ITU-T Study Group 7 (SG 7) focuses on data communications, data networks, and open system communication, which work includes the development of standards for electronic signatures and certification authorities. Through the efforts of SG 7, the ITU-T hopes to play a central role in the development of the global infrastructure used for electronic commerce, notably PKI X.509. The ITU also promotes the transfer of technologies to developing countries, largely through its Electronic Commerce for Developing Countries (EC-DC) project.
Relevant supervisory body	ITU-T, primarily Study Group 7.

iv) Internet Engineering Task Force (IETF)

URL	http://www.ietf.org/
Project	Development of global digital signature standards.
Technology	PKI X.509
Based on international standards?	Yes.
Status	Ongoing.
Application	Global.
Mandatory?	No.
Summary of objectives	The IETF is a large international community of network designers, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas. The Public-Key Infrastructure K.509 (PKIX) Working Group was established in the Fall of 1995 to develop Internet standards to support an X.509-based PKI. The Working Group is now developing additional protocols that are either integral to PKI management, or that are otherwise closely related to PKI use. The Group also continues to examine alternative certificate revocation methods, conventions for certificate name forms and extension usage for certificates designed for use in (legally-binding) non-repudiation contexts, and protocols for time stamping and data certification.
Relevant supervisory body	Public Key Infrastructure (PKIX) Working Group.

v) Internet Law and Policy Forum (ILPF)

URL	http://www.ilpf.org
Project	Various projects to address specific legal issues that arise from the cross-border nature of electronic commerce.
Technology	Neutral formulation.
Based on international standards?	Yes.
Status	Ongoing.
Application	Global.
Mandatory?	No.
Summary of objectives	The ILPF is comprised of about 15 North American, Asian and European companies involved in technology and telecommu-nications, though it solicits information and advice from a wide range or experts, including legal and technical experts its member companies and other businesses, governments and intergovern-mental organizations, academia, and the private practice of law around the world.

v) Internet Law and Policy Forum (ILPF) *(continued)*

Summary of objectives *(continued)*	The Forum's Digital Signature and Certificate Authorities Working Groups have conducted studies on topics ranging from the promotion of model U.S. digital signature legislation to best practices for certificate authorities. Current goals of the Electronic Authentication Working Group include the removal of legal and tariff barriers to electronic authentication, and the harmonization of laws governing electronic authentication across jurisdictions.
Relevant Supervisory Body	Electronic Authentication, Digital Signature, and Certificate Authorities Working Groups.

vi) UNCITRAL Model Law on Electronic Commerce

URL	http://www.uncitral.org
Project	Model international law.
Technology	Neutral formulation.
Status	Enacted.
Application	United Nations Member States (upon implementation by Member States).
Mandatory?	No.
Summary of provisions	Defines electronic signatures and provides for legal effect of electronic signatures, by offering a baseline for presumptions of validity. In four Chapters, the Model Law addresses: • general provisions related to the definition of electronic commerce; • the recognition of specific qualities of digitally-produced and signed documents that can be used to establish their full legal validity; • crucial factors in the communication of data messages, including contract formation, recognition by all involved parties, attribution, and receipt and acknowledgement of receipt; and • the application of the Model Law's general provisions to contracts related to the carriage of goods. Included with the Model Law is a guide to its enactment, designed to provide in-depth explanations of the purposes of the Law's provisions, so that officials in Member States may better understand why specific provisions have been included and determine which, if any, of the provisions might have to be varied to take into account particular national circumstances.
Relevant supervisory body	United Nations Commission on International Trade Law.

vii) UNCITRAL Model Rules on Electronic Signatures

URL	http://www.uncitral.org
Project	Model international rules.
Technology	Neutral formulation.

vii) UNCITRAL Model Rules on Electronic Signatures *(continued)*

Status	Draft.
Application	United Nations Member States (upon implementation by Member States).
Mandatory?	No.
Summary of provisions	Provides for legal effect of electronic signatures which varies depending of the level of technical reliability. According to the drafters, the Uniform Rules are meant to provide a basic "framework" to be supplemented by technical and/or contractual regulations (determined by Member States and/or the parties to a transaction facilitated through the use of electronic signatures). For this reason, the Rules offer general provisions to establish the legal validity of electronic signatures, and specify basic rules of conduct for the parties involved in a digital signature transaction. As with the Model Law, the Uniform Rules will be accompanied by guide to enactment, to explain why specific provisions were included as essential basic features of a statutory device designed to achieve the objectives of the Rules.
Relevant supervisory body	United Nations Commission on International Trade Law.

2. European Union

i) EESSI (EU-wide standardization initiative)

URL	http://www.ict.etsi.org/eessi/EESSI-homepage.htm
Technology	PKI x. 509
Based on international standards?	Ostensibly. Profile for qualified certificates: Standard for the use of X. 509 public key certificates as qualified certificates; European profile based on current IETF PKIX draft. Standards for CSPs issuing qualified certificates: Based on BS 7799. Electronic signature formats: ES 201 733.
Status	Ongoing project.
Application	European Union.
Mandatory?	No.
Summary of provisions	Voluntary, EU-wide standards and accreditation for signature creation devices, signature verification, and other areas. Supervision of the CSPs issuing qualified certificates to the public (registration/notification; self-declaration for fulfilling QC policy). The standards-related work is carried out by CEN and ETSI (EU-wide standardization bodies). ETSI is responsible for defining standards for qualified certificates, security management and certificate policy for CSPs issuing qualified certificates; electronic signature syntax and encoding formats (Annexes I and II of the EU Directive).

i) EESSI (EU-wide standardization initiative) *(continued)*

Summary of provisions *(continued)*	CEN is responsible for creating standards for signature creation and verification products and functional standards for certification service providers (Annexes III and IV of the EU Directive and also Annex II (f)). The work of ETSI/CEN is carried out in various working groups: *Area D* defines the CSP which includes a certification, registration authority, repositories and querying capabilities. The current definition contains the following functional areas: certificate issuance, revocation issuance, certificate revocation status, certificate dissemination and registration. Optional areas include time stamping and subscriber key generation and SSCD preparation. *Area F* defines secure signature creation devices. The device may or may not contain the ability to generate the key pair. While this device is sometimes thought of only as a smart card, the working group is also considering the use of other devices. *Area G1* is in charge of the signature creation environment. Signing is to be done in one of three environments: (a) Trusted, where the user completely trusts the environment; (b) Partially Trusted, where the user has partial trust (e.g., such as using an employer's computer for personal use at the office); and (c) Untrusted (e.g., such as using a public kiosk). The environment has three interfaces: user interface, SSCD interface and input/output interface. *Area G2* works in the signature validation environment. Area G2 does not require the SSCD to create a signature, but only the user's public certificate. *Area V* works on validation.
Relevant supervisory body	To be determined, depending on the Member State. Some Member States will have voluntary, self-certification schemes, while others will have governmental schemes.

3. Europe (EU Member States)

i) AUSTRIA

URL	http://www.a-sit.at/Englishch/documents.htm
Technology	Neutral formulation.
Based on international standards?	Ostensibly (ITSEC E3 high/E2 high).
Status	Enacted.
Application	Austria (both public and private sector).
Mandatory?	No.
Summary of provisions	Generally follows EU Directive. Secure electronic signature meets handwriting requirements. Supervisory body has broad powers to ensure compliance by CSPs. CSPs must notify supervisory body when they start operations.
Relevant supervisory body	Telekom-Control-Kommission (government agency, under Art. 110 of the Telecommunications Law).

ii) BELGIUM

URL	None.
Technology	PKI.
Based on international standards?	No national standards.
Status	Draft being considered in parliament.
Application	Belgium.
Mandatory?	No.
Summary of provisions	It follows the EU Directive. Provides for legal effect of electronic signatures.
Relevant supervisory body	Unknown.

iii) DENMARK

URL	http://www.fsk.dk/cgi-bin/intranet/doc-show.cgi?doc_id=34226
Technology	Technology neutral but PKI-based.
Based on international standards?	The law is silent on the standards issue; although regarding secure signature creation devices there is a reference to generally recognized standards (approved and published by the Commission).
Status	Enacted (entered into force on October 2000).
Application	Denmark (excluded when the laws calls for formal requirements).
Mandatory?	No.
Summary of provisions	It follows the EU Directive. Accreditation is not required but CSPs must declare commencement of activities. Private or public bodies will be set up for testing compliance. Under extraordinary circumstances, the National Telecom Agency might deprive CSPs of the right to issue advanced electronic signatures. Advanced electronic signatures satisfy any signature requirement stipulated by law.
Relevant supervisory body	National Telecom Agency.

iv) FINLAND

URL	None.
Technology	Neutral formulation.
Based on international standards?	Yes.
Status	Draft (it seems unlikely that the Act will be adopted in the year 2000).
Application	Finland.
Mandatory?	No.
Summary of provisions	Draft law follows Directive.
Relevant supervisory body	Telecommunications Administration Centre (Telehallintokeskus) and Mittatekniikan keskus.

v) FRANCE

URL	http://www.justice.gouv.fr
Technology	Neutral formulation.
Based on international standards?	International standards (EN 45 xxx, ISO 9000, BS 7799). National ITSEC/CCevaluation / certification scheme.
Status	Draft.
Application	France.
Mandatory?	No.
Summary of provisions	Voluntary accreditation. Must declare commencement of activities. Provides for legal effect of electronic signatures.
Relevant supervisory body	French Accreditation Body (COFRAC).

vi) GERMANY

a) Statutory scheme

URL	www.iukdg.de
Technology	PKI
Based on international standards?	National standard ostensibly based on international norms, but with national variations.
Status	Enacted, ongoing action to implement EU Directive
Application	Germany.
Mandatory?	No.
Summary of provisions	Sets security standard for qualified certificates. No notification necessary for unaccredited CSPs. Wide-ranging civil penalties for violations by accredited CSPs.
Relevant supervisory body	Regulierungsbehörde (government agency under Federal Economics Ministry).

b) ISIS

Name	ISIS (Industrial Signature Interoperability Specification)
URL	None.
Technology	PKI.
Based on international standards?	Ostensibly.
Status	Version 1.2 published on December 3, 1999.
Application	Germany.
Mandatory?	No.
Summary of provisions	Sets forth uniform standards for data and messages for services provided under the German Digital Signature Law. Defines formats for certificates and directory services.
Relevant supervisory body	Designed as a specification for companies offering certification services under the German Digital Signature Law. Companies presently participating include: German Federal Printer, CCC Competence Center Informatik GmbH, Debis Systemhaus Information Security Services GmbH, Deutsche Post AG, D-Trust GmbH, Gieseke + Devrient GmbH, TC Trust Center, TeleCash, Telesec Deutsche Telekom AG.

vii) GREECE

URL	None.
Technology	PKI.
Based on international standards?	It is uncertain whether the national standardization body (ELOT) will adopt national standards.
Status	Draft presidential decree that transposes literal text of EU Electronic Signatures Directive.
Application	Greece.
Mandatory?	No.
Summary of provisions	Mandatory accreditation of CSP.
Relevant supervisory body	Unknown.

viii) IRELAND

URL	None.
Technology	Neutral.
Based on international standards?	Yes.
Status	Discussions underway between business and government on accreditation/certification scheme under the EU Directive, but no clear timetable for completion.
Application	Ireland.
Mandatory?	No.
Summary of provisions	No draft provisions yet, but any scheme is likely to be business-led and based on a system of voluntary accreditation/certification.
Relevant supervisory body	Likely to be under the auspices of the Irish National Accreditation Board (NAB).

ix) ITALY

URL	http://www.aipa.it/attivita
Technology	PKI.
Based on international standards?	Ostensibly (X. 509v3, RSA PKCS#1, ISO 10118-3 (SHA-1), PKCS#7 (rfc 2321)).
Status	Enacted.
Application	Italy.
Mandatory?	No.
Summary of provisions	Electronic signatures must be interoperable with government. CSP must be accredited for signature to be equivalent to handwritten signature. Provides for legal effect of electronic documents if they comply with the technical requirements laid out by the law. It also gives full force and effects to hard copies and excerpts of electronic documents and authorizes compliance with all mandatory provisions on the keeping of documents with electronic media.

ix) ITALY *(continued)*

Summary of provisions *(continued)*	It contains rules which govern the transmission of an electronic document by virtue of which an electronic document is deemed to have been dispatched and received if sent to the e-mail address of the recipient. Despite purporting to follow the EU Directive on Electronic Signatures, several provisions might need to be modified to fully incorporate the Directive, in particular, (a) becoming registered as a CSP in effect requires a government license, and (b) the fact that legal effect is limited to certificates from registered CSPs.
Relevant supervisory body	AIPA (Autorita' per l'informatica nella Publica Amministrazione/ Authority for Information Technology).

x) LUXEMBOURG

URL	http://www.etat.lu/
Technology	Technology neutral but PKI-based.
Based on international standards?	Yes (ISO/EN).
Status	Enacted although it has not entered into force yet.
Application	Luxembourg.
Mandatory?	No.
Summary of provisions	Technology neutral but PKI-based. Secure electronic signature based on qualified certificate meets handwriting requirements. Voluntary accreditation system although prior to the commencement of their activities, CSPs (non certified) offering qualified certificates must provide the National Registry of Accreditation with sufficient evidence of compliance with minimum technical requirements. This agency is structured as a "monitoring body", which might be assisted by private bodies. Forthcoming regulation will detail how the Agency works.
Relevant supervisory body	National Registry of Accreditation (Ministry of Economy).

xi) THE NETHERLANDS

URL	http://www.minvenw.nl/hdtp/factsheets/trust1.html
Technology	PKI.
Based on international standards?	ANSI ABA/X9 and national standards.
Status	Ongoing project (carried out by Governments and business) which intents to become the "market standard". Non-published draft is being prepared by the Ministry of Justice to modify the Civil code to adopt a functional-equivalence definition of electronic document and electronic signature.
Application	The Netherlands.
Mandatory?	No.
Summary of provisions	Voluntary accreditation scheme (TTP. NL Scheme). Registration of any CSP that issues qualified certificates. Public registry establishes whether CSP is accredited. Requirements for CSP follow EU Directive.
Relevant supervisory body	Ministry of Transport and Communications.

xii) PORTUGAL

URL	http://www.missao-si.mct.pt/assinatura_digital.html
Technology	PKI.
Based on international standards?	Standards to be defined by forthcoming regulation.
Status	Enacted.
Application	Portugal.
Mandatory?	No.
Summary of provisions	Voluntary accreditation. Accredited CSP must comply with additional security measures. Provides for legal effect of electronic signatures.
Relevant supervisory body	To be designated by forthcoming regulation.

xiii) SPAIN

URL	http://www.sgc.mfom.es/legisla/top_leg.htm
Technology	Neutral, but PKI-based.
Based on international standards?	No national standards yet, awaiting EU standards.
Status	Enacted.
Application	Spain. Does not apply to communications involving the government (special national standards for this).
Mandatory?	No, although electronic communication with government requires the use of specific type of signatures and certificates.
Summary of provisions	Follows very closely EU Directive. Voluntary accreditation. Accredited CSP must comply with additional security measures. Provides for legal effect of electronic signatures. Additional legal effects are provided to electronic signatures issued by licensed CSP.
Relevant supervisory body	Accreditation is carried out jointly by ENAC (Entidad Nacinal de Acreditacion) & Ministry of Science and Technology.

xiv) SWEDEN

URL	http://www.swedac.se
Technology	Technology neutral but PKI-based.
Based on international standards?	No national standards. Reference to EN 45012, BS 7799, ISO TR 13335.
Status	Adopted in late October 2000.
Application	Sweden.
Mandatory?	No.
Summary of provisions	The proposal follows the Directive on most important points. Accreditation is not mandatory. The use of standards is not mandatory. Provides for legal effect of electronic signatures.
Relevant supervisory body	National Post and Telecom Agency.

xv) UNITED KINGDOM

a) Cloud cover

Name	Cloud cover
URL	http://www.cesg.gov.uk/cloudcover/
Technology	PKI solutions.
Based on international standards?	Ostensibly (X. 509 v3 certificates & X. 509 v2 certificate revocation list, RSA PKCS, others).
Status	Ongoing project.
Application	UK government communications and government Intranet (including, potentially, communications with citizens).
Mandatory?	Yes (for UK government).
Summary of provisions	Government scheme to develop minimum PKI interoperability standards for the UK government. Run by CESG (root authority which certifies CSPs for the government), a part of the UK Civil Service.
Relevant supervisory body	CESG's certification body of the UK IT Security Evaluation and Certification Scheme is accredited by the UK Accreditation Service.

b) T-Scheme

Name	T-Scheme.
URL	None.
Technology	PKI.
Based on international standards?	Yes.
Status	Ongoing project with participation by business and government.
Application	UK companies and government agencies that self-certify under the scheme.
Mandatory?	No.
Summary of provisions	The T-Scheme is designed to be a scheme for CSPs in the UK (including, possibly, the UK government) to issue certificates that have met certain industry-defined standards for trustworthiness. The status of such certificates under the EU Directive (i.e., whether they would be considered per se to be "qualified certificates") is presently uncertain.
Relevant supervisory body	Self-regulation. Government supervision may be established for authentication procedures that do not participate in T-Scheme.

4. Europe (non-EU)

i) CZECH REPUBLIC

URL	http://www.park.cz/commerce/
Technology	Neutral formulation.
Based on international standards?	Unclear.
Status	Enacted.
Application	Czech Republic (covers both private and public communications).
Mandatory?	No.

i) CZECH REPUBLIC *(continued)*

Summary of provisions	Follows EU Directive on electronic signatures. Certification authorities must be authorized by the Office for electronic signatures.
Relevant supervisory body	Office for electronic signatures (Ministry of transport and communications).

ii) SLOVAKIA

URL	http://www.economy.gov.sk
Technology	Neutral formulation.
Based on international standards?	Unclear.
Status	Draft.
Application	Slovakia.
Mandatory?	No.
Summary of provisions	Certification authorities must be accredited. Certification authority can function only in the form of stock company (with a capital of 10 000 000 SK). National office for Electronic Signatures establishes Registrar Bodies that are responsible for correctness of identity of applicants for certificates.
Relevant supervisory body	Office for Electronic Signatures.

iii) SWITZERLAND

URL	http://www.bakom.ch/eng/subpage/?category_104.html
Technology	PKI.
Based on international standards?	The implementation of the provisions is to be based on international standards. At the present and absent international standards, accredited CSPs must ensure compliance with EN 45012.
Status	Enacted, ongoing action to implement the provisions of this Decree.
Application	Switzerland.
Mandatory?	No.
Summary of provisions	Voluntary accreditation scheme. Compliance with the requirements is ensured by accredited certification bodies. Such bodies must supervise the accredited CSP. CSP must be registered before starting activities.
Relevant supervisory body	Swiss Accreditation Service of the Federal Office of Metrology (http://www.sas.admin.ch), which is responsible for authorizing accredited certification bodies.

5. North America

i) CANADA

a) Uniform Electronic Commerce Act (UECA)

URL	http://www.law.ualberta.ca/alri/ulc/current/euecafin.htm (an annotated version can be found at http://www.law.ualberta.ca/alri/ulc/current/euecafa.htm)
Project	Model provincial law.
Technology	Neutral.
Status	Model law only.
Application	Canada (where adopted).
Mandatory?	Yes (where adopted).
Summary of provisions	Follows the specifications set out in UNCITRAL Model Law on Electronic Commerce. Provides legal effect to electronic signatures.
Relevant supervisory body	To be determined by each adopting jurisdiction.

b) Personal Information Protection and Electronic Documents Act

URL	http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052b-3E.html#17
Project	Federal legislation.
Technology	Neutral.
Status	Came into force May 1 2000.
Application	Canada.
Mandatory?	Yes.
Summary of Provisions	Part 2 of the Act provides for legal effect of electronic signatures, but does not prescribe the use of any specific technology or procedure; introduces the concept of "secure electronic signature" to be defined through regulations.
Relevant supervisory body	Canadian government.

c) Ontario Electronic Commerce Act (ECA)

URL	http://www.ontla.on.ca/Documents/documentsindex.htm (see Bill # 88)
Project	Provincial law.
Technology	Neutral.
Status	Received Royal Assent October 16 2000.
Application	Ontario.
Mandatory?	Yes.
Summary of provisions	Follows the specifications set out in the UNCITRAL Model Law on Electronic Commerce (and the Canada Uniform Electronic Commerce Act). Provides legal effect to electronic signatures.
Relevant supervisory body	Ministry of the Attorney General.

d) Saskatchewan Electronic Information and Documents Act

URL	http://www.legassembly.sk.ca/bills/html/bill038.htm
Project	Provincial law.
Technology	Neutral.
Status	Received Royal Assent June 21 2000.
Application	Saskatchewan.
Mandatory?	Yes.
Summary of provisions	Very similar to the Uniform Electronic Commerce Act.
Relevant supervisory body	Ministry of the Attorney General.

ii) UNITED STATES

a) Electronic Signatures in Global and National Commerce (E-SIGN) Act

URL	http://thomas.loc.gov/cgi-bin/query/D?c106:6:./temp/~c106Nii0hw::
Project	National law.
Technology	Neutral.
Status	Signed into law on June 30, 2000.
Application	United States
Mandatory?	Yes.
Summary of provisions	Provides for legal effect of electronic signatures but does not prescribe the use of any specific technology or procedure.
Relevant supervisory body	None.

b) Uniform Electronic Transactions Act (UETA)

URL	http://www.nccusl.org/uniformact_summaries/uniformacts-s-ueta.htm
Project	Model state law.
Technology	Neutral.
Status	Adopted in twenty-two (?) states.
Application	United States (where adopted).
Mandatory?	Yes (where adopted).
Summary of provisions	Provides for legal effect of electronic signatures but does not prescribe the use of any specific technology or procedure.
Relevant supervisory body	To be determined by each adopting state.

c) RSA Data Security, Inc.

URL	http://www.rsasecurity.com
Project	The Public Key Cryptography Standards (PKCS)
Technology	Various formal and de facto standards, including ANSI X9 documents, PKIX, SET, S/MIME, and SSL.
Based on international standards?	No.
Status	RSA is not a standards-setting body, but a US-based supplier of software components for data security. However the PKCS, which are produced by the company's research and development

	division, RSA Laboratories, have become widely referenced and implemented by national standards organizations.

c) RSA Data Security, Inc. (continued)

Application	United States.
Mandatory?	No, though the PKCS have been integrated into a number of formal standards.
Summary of objectives	Develop technical solutions for the secure transfer of electronic data.
Relevant supervisory body	RSA Laboratories.

d) National Institute of Standards and Technology (NIST)

URL	http://www.nist.gov
Project	Development and application of technology, measurements, and standards for the protection of government information.
Technology	DSA ANSI X9.31 ANSI X9.62 (ECDSA)
Based on international standards?	No.
Status	Ongoing.
Application	U.S. Government.
Mandatory?	No.
Summary of accomplishments	Developed the Digital Signature Standard (DSS).
Relevant supervisory body	Federal Public Key Infrastructure (FPKI) Steering Committee and the PKI Technical Working Group (PKI-TWG).

e) Federal Public Key Infrastructure (FPKI) Steering Committee

URL	http://www.gits -sec.treas.gov/index.shtml
Project	Various initiatives to identify and resolve federal PKI technical and business issues, and find solutions to policy and interoperability issues. Current project involves the creation of the Federal Bridge Certification Authority (FBCA) to allow the interoperation of federal agencies (and ultimately external organizations) that employ their own PKIs.
Technology	Neutral.
Based on international standards?	No.
Status	Projects are ongoing; FBCA expected to be operational by the end of 2000.
Application	United States.
Mandatory?	No.
Summary of objectives	The FBCA would act as a trusted third party, to cross-certify individual governmental CAs so that a user from any participating agency who is presented with a certificate could trust that certificate, regardless of which CA issued it.
Relevant supervisory body	The Government Information Technology Services (GITS) Board Champion for Security.

f) National Automated Clearinghouse Association (NACHA)

URL	http://www.nacha.org
Project	Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates.
Technology	Neutral.
Based on international standards?	No.
Status	Published in 1999, along with results of NACHA study on Certification Authority Interoperability.
Application	United States.
Mandatory?	No.
Summary of provisions	Promotes and facilitates the standardization of policies and procedures related to electronic payments. NACHA's PKI work is specifically designed to encourage uniformity in states' e-commerce policies and practices, and to advance the security of interstate electronic transactions.
Project development body	The Internet Council's Certification Authority Rating and Trust Task Force (CARAT).

g) American Bar Association (ABA)

URL	http://www.abanet.org/scitech/ec/isc/dsgfree.html
Project	Digital Signature Guidelines.
Technology	The guidelines are specific to digital signatures, certificates and PKIs
Based on international standards?	No. The Guidelines have influenced standards outside the U.S. to varying degrees.
Status	Issued in August 1996.
Application	Proposed for United States.
Mandatory?	No.
Summary of provisions	The Guidelines provide a detailed examination of the legal principles applicable to the use of digital certificates and PKIs..
Relevant supervisory body	The Information Security Committee of the ABA's Section of Science & Technology, Electronic Commerce Division.

h) American Bar Association (ABA)

URL	http://www.abanet.org/scitech/ec/isc/home.html
Project	PKI Assessment Guidelines (PAG)
Technology	Digital signatures, certificates and PKIs
Based on international standards?	Yes, including BS 7799, X.509, PKIX RFC 2527 and other standards.
Status	Draft
Application	Anticipated to be in the U.S. and of considerable influence globally
Mandatory?	No.
Summary of provisions	Section A (Introduction) provides an introduction to the PAG. Section B (PKI Overview) includes a broad overview of PKI and PKI assessment, a list of important PKI-related terms, and

	references to significant related documents. (A more detailed tutorial on PKI technology is included in a PAG Appendix.

h) American Bar Association (ABA) (continued)

Summary of provisions *(continued)*	Section C (Legal Preface) presents important legal issues and principles that generally affect PKI. Section D (PAG Provisions) contains the PAG's substantive assessment provisions, following generally the format of RFC 2527.
Relevant supervisory body	The Information Security Committee of the ABA's Section of Science & Technology, Electronic Commerce Division.

6. South America

i) ARGENTINA

URL	www.cnv.gov.ar
Technology	PKI.
Based on international standards?	Not defined yet; although the Secretaria de la Funcion Publica publishes draft standards.
Status	Draft.
Application	Argentina (it does not cover relationships involving the government).
Mandatory?	No.
Summary of provisions	Accreditation is voluntary. Provides for legal effect of electronic signatures.
Relevant supervisory body	Secretaria de la Funcion Publica (Jefatura de Gabinete de Ministros).

ii) COLOMBIA

URL	http://natlaw.com/ecommerce/materials.htm
Technology	PKI.
Based on international standards?	Not addressed (waiting for implementing regulations).
Status	Enacted.
Application	General.
Mandatory?	No.
Summary of provisions	Follows the proposed UNCITRAL Model Law. Provides for legal effect of electronic signatures. CA must be licensed.
Relevant supervisory body	Colombian Superintendent of Industry and Trade.

iii) CHILE

URL	http://www.modernizacion.cl/
Technology	Technology neutral but PKI-based.
Based on international standards?	Yes. Projects are ongoing to define market standards regarding communications with the government.
Status	Draft.
Application	Private communications. There is an additional law on the use of

	digital signatures for electronic communications carried out by government.

iii) CHILE *(continued)*

Mandatory?	No.
Summary of provisions	Provides legal effects of electronic documents and signatures.
Relevant supervisory body	Unidad de Tecnologías de la Información y Comunicaciones.

iv) ECUADOR

URL	http://natlaw.com/ecommerce/materials.htm
Technology	Technology neutral but PKI-based.
Based on international standards?	Unclear.
Status	Draft.
Application	Ecuador.
Mandatory?	Yes.
Summary of provisions	Mandatory licensing scheme. Provides for legal effect of electronic signatures.
Relevant supervisory body	Ecuadorian Superintendent of Telecommunications.

v) PERU

URL	http://www.corpece.net/servicios/proyectos/ley_comercio_electronico.htm
Technology	Technology neutral but PKI-based.
Based on international standards?	Yes, although specific standards still need to be defined.
Status	Enacted.
Application	Peru.
Mandatory?	No.
Summary of provisions	CSP must be registered prior to starting activities. Unclear whether accreditation is voluntary or mandatory. Provides for legal effect of electronic signatures.
Relevant supervisory body	To be defined.

7. ASIA

i) AUSTRALIA

URL	http://www.law.gov.au/ecommerce
Technology	Neutral formulation.
Based on international standards?	Standards Australia Committee IT/12/4/1 is responsible for the development of PKAF related Standards. Australian Standard 4539 deals with the Public Key Authentication Framework (PKAF). There are existing standards for protection of PINs in financial transactions. Where possible the laws are based on ISO or IETF standards http://www.standards.com.au There is a private sector body, the Certification Forum of Australia, which is developing a voluntary standards based accreditation process. Limited details on the Forum can be found at http://www.aeema.asn.au

i) AUSTRALIA *(continued)*

Based on international standards? *(continued)*	There is also a National Electronic Authentication Council which is looking at policy and standards requirements. Information is at http://www.noie.gov.au/projects/consult/NEAC/index.htm
Status	Enacted. The States and territories have agreed to mirror the federal legislation and the two largest states, New South Wales and Victoria have already passed their versions.
Application	Australia.
Mandatory?	No.
Summary of provisions	Accreditation is not mandatory. The Australian Government has an accreditation scheme for CAs issuing certificates for dealings with the Federal Government. The states and territories are looking at also adopting the scheme which is called Gatekeeper. Information on the scheme is available at http://www.ogo.gov.au/projects/publickey/Gatekeeper.htm
Relevant supervisory body	Various (see above).

ii) HONG KONG

URL	http://www.info.gov.hk/itbb/english/it/eto.htm
Technology	PKI.
Based on international standards?	Presumably yes although technical specifications are not adopted yet.
Status	Enacted, although some parts have not entered into force yet.
Application	Hong Kong (it applies to both for private and also Administrative communications).
Mandatory?	No.
Summary of provisions	Voluntary accreditation scheme. Equates electronic documents and signatures to paper documents with handwritten signatures although it excepts from this rule certain documents (such as wills, trusts, powers of attorney, documents required to be stamped, documents concerning land, oaths, statutory declarations, judgements, court warrants and negotiable instruments). The legal effects of electronic signatures are only provided if the signature is supported by a recognized certificate issued by a recognized certification authority. Security criteria for the management, systems and operations of CSPs in the areas of identification and authentication of registration, suspension and revocation requests; generation, issuance, suspension and revocation of certificates; and publication and archiving of certificates and their suspension or revocation information. Licensed CSPs will enjoy the benefits of trustworthiness, consumer confidence, and an evidentiary presumption for digital signatures.
Relevant supervisory body	Hong Kong Government.

iii) JAPAN

URL	http://www.mpt.go.jp/eng/
Technology	Neutral formulation.
Based on international standards?	Ostensibly.
Status	General law has been adopted and is to enter into force in April 2001. Awaiting implementation of regulations regarding technical requirements.
Application	It does not apply to the government (another initiative is underway). Governmental PKI system or electronic government project will take effect by 2003.
Mandatory?	No.
Summary of provisions	Voluntary accreditation scheme which require CSP to issue certificates with encryption keys with more than a certain number of bits, and to use certain facilities and equipment. Provides for legal effect of electronic signatures (presumption of the authenticity of an electronic document if a specific person has applied an electronic signature).
Relevant supervisory body	Ministry of International Trade and Industry and Ministry of Posts and Telecommunications.

iv) SINGAPORE

URL	http://www.cca.gov.sg/
Technology	PKI
Based on international standards?	Ostensibly
Status	Regulations are in effect; no licensed CAs as of December 3, 1999
Application	Singapore
Mandatory?	No
Summary of provisions	Security criteria for the management, systems and operations of CSPs in the areas of identification and authentication of registration, suspension and revocation requests; generation, issuance, suspension and revocation of certificates; and publication and archival of certificates and their suspension or revocation information. Licensed CSP will enjoy the benefits of trustworthiness, consumer confidence and evidentiary presumption for digital signatures.
Relevant supervisory body	Singapore CCA (Controller of Certification Authorities) and National Computer Board