UNCITRAL UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods

UNITED NATIONS

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods

UNITED NATIONS
Vienna, 2009

UNITED NATIONS PUBLICATION
Sales No. E.09.V.4
ISBN 978-92-1-133663-4

Foreword

In 2004, having completed its work on the Convention on the Use of Electronic Communications in International Contracts, Working Group IV (Electronic Commerce) of the United Nations Commission on International Trade Law (UNCITRAL) requested the Secretariat to continue monitoring various issues related to electronic commerce, including issues related to cross-border recognition of electronic signatures, and to publish the results of its research with a view to making recommendations to the Commission as to whether future work in those areas would be possible (see A/CN.9/571, para. 12).

In 2005, UNCITRAL took note of the work undertaken by other organizations in various areas related to electronic commerce and requested the Secretariat to prepare a more detailed study, which should include proposals as to the form and nature of a comprehensive reference document discussing the various elements required to establish a favourable legal framework for electronic commerce, which UNCITRAL might in the future consider preparing with a view to assisting legislators and policymakers around the world.[1]

In 2006, UNCITRAL considered a note prepared by its secretariat pursuant to that request (A/CN.9/604). The note identified the following areas as possible components of a comprehensive reference document: (*a*) authentication and cross-border recognition of electronic signatures; (*b*) liability and standards of conduct for information-services providers; (*c*) electronic invoicing and legal issues related to supply chains in electronic commerce; (*d*) transfer of rights in tangible goods and other rights through electronic communications; (*e*) unfair competition and deceptive trade practices in electronic commerce; and (*f*) privacy and data protection in electronic commerce. The note also identified other issues that, although in a more summary fashion, could be included in such a document: (*a*) protection of intellectual property rights; (*b*) unsolicited electronic communications (spam); and (*c*) cybercrime. At that session, there was support for the view that the task of legislators and policymakers, in particular in developing countries, might be greatly facilitated if UNCITRAL were to formulate a comprehensive reference document dealing with the topics identified by the Secretariat. Such a document, it was also said, might also assist UNCITRAL in identifying areas in which it might itself undertake future harmonization work. UNCITRAL asked the Secretariat to prepare a sample portion of the comprehensive reference document dealing specifically with issues related to authentication and cross-border recognition of electronic signatures, for review at its fortieth session, in 2007.[2]

[1] *Official Records of the General Assembly, Sixtieth Session, Supplement No. 17* (A/60/17), para. 214.

[2] Ibid., *Sixty-first Session, Supplement No. 17* (A/61/17), para. 216.

The sample chapter that the Secretariat prepared pursuant to that request (A/CN.9/630 and Add.1-5) was submitted for consideration by UNCITRAL at its fortieth session. UNCITRAL commended the Secretariat for the preparation of the sample chapter and requested the Secretariat to publish it as a stand-alone publication.[3]

The present publication analyses the main legal issues arising out of the use of electronic signatures and authentication methods in international transactions. Part one provides an overview of methods used for electronic signature and authentication and their legal treatment in various jurisdictions. Part two considers the use of electronic signature and authentication methods in international transactions and identifies the main legal issues related to cross-border recognition of such methods. It has been observed that, from an international perspective, legal difficulties are more likely to arise in connection with the cross-border use of electronic signature and authentication methods that require the involvement of third parties in the signature or authentication process. This is the case, for instance, of electronic signature and authentication methods supported by certificates issued by a trusted third-party certification services provider, in particular digital signatures under a public key infrastructure (PKI). For this reason, part two of this publication devotes special attention to international use of digital signatures under a PKI. This emphasis should not be understood as a preference or endorsement of this or any other particular type of authentication method or technology.

[3] Ibid., *Sixty-second Session, Supplement No. 17* (A/62/17), para. 195.

Contents

Page

Part one

Part two

Introduction

1. Information and computer technology have developed various means for linking information in electronic form to particular persons or entities, for ensuring the integrity of such information or for enabling persons to demonstrate their entitlement or authorization to obtain access to a certain service or repository of information. These functions are sometimes referred to generically either as electronic "authentication" or electronic "signature" methods. Sometimes, however, distinctions are made between electronic "authentication" and electronic "signature". The use of terminology is not only inconsistent, but is to some extent misleading. In a paper-based environment, the words "authentication" and "signature" and the related actions of "authenticating" and "signing" do not have exactly the same connotation in different legal systems and have functionalities that may not necessarily correspond to the purpose and function of the so-called electronic "authentication" and "signature" methods. Furthermore, the word "authentication" is sometimes generically used in connection with any assurance of both authorship and integrity of information, but some legal systems may distinguish between those elements. A short overview of differences in terminology and legal understanding is therefore necessary with a view to establishing the scope of the present document.

2. Under common law on civil evidence, a record or document is regarded as "authentic" if there is evidence that the document or record "is what its proponent claims".[1] The notion of "document" as such is fairly broad and generally encompasses "anything in which information of any description is recorded".[2] This would include, for example, such things as photographs of tombstones and houses,[3] account books[4] and drawings and plans.[5] The relevancy of a document as a piece of evidence is established by connecting it with a person, place or thing, a process which in some common law jurisdictions is known as "authentication".[6] Signing a document is a

[1] United States of America, Federal Rules of Evidence, rule 901, subdivision (*a*): "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

[2] United Kingdom of Great Britain and Northern Ireland, Civil Evidence Act 1995, chapter 38, section 13.

[3] *Lyell v. Kennedy* (No. 3) (1884) 27 Ch.D. 1 (United Kingdom, Chancery Division).

[4] *Hayes v. Brown* [1920] 1 K.B. 250 (United Kingdom, Law Reports, King's Bench).

[5] *J. H. Tucker & Co., Ltd. v. Board of Trade* [1955] 2 All ER 522 (United Kingdom, All England Law Reports).

[6] *Farm Credit Bank of St. Paul v. William G. Huether*, 12 April 1990 (454 N.W.2d 710, 713) (United States, Supreme Court of North Dakota, North Western Reporter).

common—albeit not exclusive—means of "authentication", and, depending on the context, the terms "to sign" and "to authenticate" may be used as synonyms.[7]

3. A "signature", in turn, is "any name or symbol used by a party with the intention of constituting it his signature".[8] It is understood that the purpose of statutes that require a particular document to be signed by a particular person is to confirm the genuineness of the document.[9] The paradigm case of signature is the signatory's name, written in the signatory's own hand, on a paper document (a "handwritten" or "manuscript" signature).[10] However, the handwritten signature is not the only conceivable type of signature. Since courts regard signatures as "only a mark", unless the statute in question requires the signature to be an autograph, "the printed name of the party who is required to sign the document is enough", or the signature "may be impressed upon the document by a stamp engraved with a facsimile of the ordinary signature of the person signing", provided that proof in these cases is given "that the name printed on the stamp was affixed by the person signing", or that such signature "has been recognized and brought home to him as having been done by his authority so as to appropriate it to the particular instrument".[11]

4. Legal signature requirements as a condition for the validity of certain acts in common law jurisdictions are typically found in the British Statute of Frauds[12] and its versions in other countries.[13] With time, courts have tended to interpret the Statute of Frauds liberally, out of recognition that its strict form requirements were conceived against a particular background[14] and that strict adherence to its rules might unnecessarily

[7] In the context of the revised article 9 of the United States Uniform Commercial Code, for example, "authenticate" is defined as "(A) to sign; or (B) to execute or otherwise adopt a symbol, or encrypt or similarly process a record in whole or in part, with the present intent of the authenticating person to identify the person and adopt or accept a record".

[8] *Alfred E. Weber v. Dante De Cecco,* 14 October 1948 (1 N.J. Super. 353, 358) (United States, New Jersey Superior Court Reports).

[9] *Lobb v. Stanley* (1844), 5 QB 574, 114 E.R. 1366 (United Kingdom, Law Reports, Queen's Bench).

[10] Lord Denning in *Goodman v. Eban* [1954] QBD 550 at 56: "In modern English usage when a document is required to be signed by someone that means that he must write his name with his own hand upon it" (United Kingdom, Queen's Bench Division).

[11] *R. v. Moore: ex parte Myers* (1884) 10 V.L.R. 322 at 324 (United Kingdom, Victorian Law Reports).

[12] The Statute of Frauds was originally passed in Great Britain in 1677 "for the prevention of many fraudulent practices which are commonly endeavoured to be upheld by perjury and subordination of perjury". Most of its provisions were repealed in the United Kingdom during the twentieth century.

[13] For example, section 2-201, subsection 1, of the Uniform Commercial Code of the United States, which has expressed the Statute of Frauds as follows: "Except as otherwise provided in this section, a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by a party against whom enforcement is sought or by his authorized agent or broker."

[14] "The Statute of Frauds was passed at a period when the legislature was somewhat inclined to provide that cases should be decided according to fixed rules rather than to leave it to the jury to consider the effect of the evidence in each case. This, no doubt, arose to a certain extent from the fact that in those days the plaintiff and the defendant were not competent witnesses" (J. Roxborough in *Leeman v. Stocks* [1951] 1 Ch 941 at 947-8 (United Kingdom, Law Reports, Chancery Division) citing approval for the views of J. Cave in *Evans v. Hoare* [1892] 1 QB 593 at 597 (United Kingdom, Law Reports, Queen's Bench)).

deprive contracts of legal effect.[15] Thus, in the last 150 years, common law jurisdictions have seen an evolution of the concept of "signature" from an original emphasis on form to a focus on function.[16] Variations on this theme have been considered by the English courts from time to time, ranging from simple modifications such as crosses[17] or initials,[18] to pseudonyms[19] and identifying phrases,[20] to printed names,[21] signatures by third parties[22] and rubber stamps.[23] In all these cases the courts have been able to resolve the question as to whether a valid signature was made by drawing an analogy with a manuscript signature. Thus, it could be said that against a background of some rigid general form requirements, courts in common law jurisdictions have tended to develop a broad understanding of what the notions of "authentication" and "signature" mean, focusing on the intention of the parties, rather than on the form of their acts.

5. The approach to "authentication" and "signature" in civil law jurisdictions is not in all respects identical to the common law approach. Most civil law jurisdictions follow the rule of freedom of form for contractual engagements in private law matters, either expressly[24] or impliedly[25] subject, however, to a more or less extensive catalogue of exceptions depending on the jurisdiction concerned. This means that, as a general

[15] As explained by Lord Bingham of Cornhill, "it quickly became evident that if the seventeenth century solution addressed one mischief it was capable of giving rise to another: that a party, making and acting on what was thought to be a binding oral agreement, would find his commercial expectations defeated when the time for enforcement came and the other party successfully relied on the lack of a written memorandum or note of the agreement" (*Actionstrength Limited v. International Glass Engineering*, 3 April 2003, [2003] UKHL 17 (United Kingdom, House of Lords)).

[16] Chris Reed, "What is a signature?", *Journal of Information, Law and Technology*, vol. 3, 2000, and reference to case law therein, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/ (accessed on 5 June 2008).

[17] *Baker v. Dening* (1838) 8 A. & E. 94 (United Kingdom, Adolphus and Ellis' Queen's Bench Reports).

[18] *Hill v. Hill* [1947] Ch 231 (United Kingdom, Chancery Division).

[19] *Redding, in re* (1850) 14 Jur. 1052, 2 Rob.Ecc. 339 (United Kingdom, Jurist Reports and Robertson's Ecclesiastical Reports).

[20] *Cook, In the Estate of (Deceased) Murison v. Cook and Another* [1960] 1 All ER 689 (United Kingdom, All England Law Reports).

[21] *Brydges v. Dicks* (1891) 7 T.L.R. 215 (cited in Brennan v. Kinjella Pty Ltd., Supreme Court of New South Wales, 24 June 1993, 1993 NSW LEXIS 7543, 10). Typewriting has also been considered in *Newborne v. Sensolid* (Great Britain), Ltd. [1954] 1 QB 45 (United Kingdom, Law Reports, Queen's Bench).

[22] *France v. Dutton*, 24 April 1891 [1891] 2 QB 208 (United Kingdom, Law Reports, Queen's Bench).

[23] *Goodman v. J. Eban Ltd.*, [1954] 1 QB 550, cited in *Lazarus Estates, Ltd. v. Beasley*, Court of Appeal, 24 January 1956 ([1956] 1 QB 702); *London County Council v. Vitamins, Ltd.*, *London County Council v. Agricultural Food Products, Ltd.,* Court of Appeal, 31 March 1955 [1955] 2 QB 218 (United Kingdom, Law Reports, Queen's Bench).

[24] This is recognized, for instance, in article 11, paragraph 1, of the Code of Obligations of Switzerland. Similarly, section 215 of the Civil Code of Germany provides that agreements are only invalid where they failed to observe a form prescribed by law or agreed upon by the parties. Except for such specific instances, it is generally understood that private law contracts are not subject to specific form requirements. Where the law expressly prescribes a particular form, that requirement is to be interpreted strictly.

[25] In France, for instance, freedom of form is an implication within the basic rules on contract formation under the Civil Code. According to article 1108 of the Civil Code of France, the validity of a contract requires the consent of the promisor, his or her legal capacity, a certain object and a licit cause; once these have been met, the contract is "law between the parties" according to article 1134. This is also the rule in Spain under articles 1258 and 1278 of the Civil Code of Spain. Italy also follows the same rule, although less explicitly (see Civil Code of Italy, articles 1326 and 1350).

rule, contracts need not be in "writing" or "signed" in order to be valid and enforceable. However, there are civil law jurisdictions that generally require a writing to prove the contents of contracts, except in commercial matters.[26] In contrast to common law jurisdictions, civil law countries tend to interpret evidentiary rules rather strictly. Typically, rules on civil evidence establish a hierarchy of evidence for proving the content of civil and commercial contracts. Highest in such ranking are documents issued by public authorities, followed by authentic private documents. Often, such hierarchy is conceived in such a way that the notions of "document" and "signature", although formally distinct, may become nearly inseparable.[27] Other civil law jurisdictions, however, positively link the notion of "document" to the existence of a "signature".[28] This does not mean that a document that has not been signed is necessarily deprived of any value as evidence, but such a document would not enjoy any particular presumption and is generally regarded as a "beginning of evidence".[29] "Authentication" is in most civil law jurisdictions a concept that is rather narrowly understood to mean that the authenticity of a document has been verified and certified by a competent public authority or a notary public. In civil procedure it is common to refer instead to the notion of "originality" of documents.

6. As is the case under common law, the paradigm of a signature in civil law countries is the handwritten one. As regards the signature itself, some jurisdictions tend to admit various equivalents, including mechanical reproductions of signatures, despite a generally formalist approach to evidence.[30] Other jurisdictions, however, admit mechanical signatures for commercial transactions[31] but, until the advent of computer technologies, continued to require a handwritten signature for the proof of other types of contract.[32] It could therefore be said that against a general background of freedom of form for the conclusion of business contracts, civil law countries tend to apply strict

[26] Article 1341 of the Civil Code of France requires a writing for the proof of contracts exceeding a certain value, but article 109 of the Commercial Code admits various types of evidence, without a particular hierarchy. This led the Court of Cassation of France in 1892 to recognize the general principle of freedom of evidence in commercial matters (Cass. civ. 17 May 1892, DP 1892.1.604; cited in Luc Grynbaum, *Preuve, Répertoire de droit commercial Dalloz*, June 2002, sections 6 and 11).

[27] Thus, for instance, under German law a signature is not an essential element of the notion of "document" (Urkunde) (Gerhard Lüke and Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), section 415, No. 6). Nevertheless, the hierarchy of documentary evidence established by sections 415, 416 and 419 of the Code of Civil Procedure of Germany clearly links the signature to the document. Indeed, section 416, on the evidentiary value of private documents (*Privaturkunden*), provides that private documents constitute "full proof" for the information they contain as long as they are signed by the author or by a notarized signature. As nothing is provided for documents without a signature, it seems that they share the sort of defective documents (i.e. garbled, damaged), whose evidentiary value is "freely established" by the courts (Code of Civil Procedure of Germany, section 419).

[28] Thus, in France, a signature is an "essential element" of private documents (*actes sous seing privé*) (see *Recueil Dalloz, Preuve*, No. 638).

[29] This is the situation in France, for example see *Recueil Dalloz, Preuve*, Nos. 657-658.

[30] Commentators of the Code of Civil Procedure of Germany point out that requiring a handwritten signature would mean excluding all forms of mechanically made signs, a result that would run counter to ordinary practice and technological progress (see Gerhard Lüke and Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), section 416, No. 5).

[31] For example, France (see *Recueil Dalloz, Preuve*, No. 662).

[32] In France, for instance, the signature could not be replaced with a cross or other signs, by a seal or by fingerprints (see *Recueil Dalloz, Preuve*, No. 665).

standards to assess the evidentiary value of private documents and may be dismissive of documents whose authenticity is not immediately recognizable on the basis of a signature.

7. The above discussion shows not only that the notions of signature and authentication are not uniformly understood, but also that the functions they fulfil vary across legal systems. Despite these divergences, a few general common elements can be found. The notions of "authentication" and "authenticity" are generally understood in law to refer to the genuineness of a document or record, that is, that the document is the "original" support of the information it contains, in the form it was recorded and without any alteration. Signatures, in turn, perform three main functions in the paper-based environment: signatures make it possible to identify the signatory (identification function); signatures provide certainty as to the personal involvement of that person in the act of signing (evidentiary function); and signatures associate the signatory with the content of a document (attribution function). Signatures can be said to perform various other functions as well, depending on the nature of the document that was signed. For example, a signature might attest to the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text (thus displaying awareness of the fact that legal consequences might possibly flow from the act of signing); the intent of a person to associate him or herself with the content of a document written by someone else; and the fact that, and the time when, a person has been at a given place.[33, 34]

8. It should be noted, however, that even though authenticity is often presumed by the existence of a signature, a signature alone does not "authenticate" a document. The two elements may even be separable, depending on the circumstances. A signature may retain its "authenticity" even though the document to which it is affixed is subsequently altered. Likewise, a document may still be "authentic" even though a signature it contains was forged. Furthermore, the authority to intervene in a transaction and the actual identity of the person in question, while important elements to ensure the authenticity of a document or signature, are neither fully demonstrated by the signature alone, nor are they sufficient assurance of the authenticity of the document or of the signature.

9. This observation leads to another aspect of the issue presently discussed. Regardless of the particular legal tradition, a signature, with very few exceptions, is not self-standing. Its legal effect will depend on the link between the signature and the person to whom the signature is attributable. In practice, various steps may be taken to verify the identity of the signatory. When the parties are all present at the same place at the same time, they may simply recognize one another by their faces; if they negotiate

[33] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001* (United Nations publication, Sales No. E.02.V.8), part two, para. 29 (available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html, accessed on 6 June 2008).

[34] This analysis had already served as a basis for functional equivalence criteria in article 7 of the earlier *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5 bis as Adopted in 1998* (United Nations publication, Sales No. E.99.V.4), available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html (accessed on 6 June 2008).

over the telephone, they may recognize each other's voices and so on. Much of this happens as a matter of course and is not subject to specific legal rules. However, where the parties negotiate by correspondence, or where signed documents are forwarded along a contracting chain, there may be few means of establishing that the signs that appear on a given document were indeed made by the person to whose name they appear to be linked and whether indeed only the duly authorized person was the one who produced the signature supposed to bind a particular person.

10. Although a manual signature is a familiar form of "authentication" and serves well for transaction documents passing between known parties, in many commercial and administrative situations a signature is relatively insecure. The person relying on the document often has neither the names of persons authorized to sign nor specimen signatures available for comparison.[35] This is particularly true of many documents relied upon in foreign countries in international trade transactions. Even where a specimen of the authorized signature is available for comparison, only an expert may be able to detect a careful forgery. Where large numbers of documents are processed, signatures are sometimes not even compared except for the most important transactions. Trust is one of the basic foundations of international business relations.

11. Most legal systems have special procedures or requirements that are intended to enhance the reliability of handwritten signatures. Some procedures may be mandatory in order for certain documents to produce legal effects. They may also be optional and available to parties that wish to act to preclude possible arguments concerning the authenticity of certain documents. Typical examples include the following:

(*a*) *Notarization.* In certain circumstances, the act of signing has a particular formal significance due to the reinforced trust associated with a special ceremony. This is the case, for instance, with notarization, i.e. the certification by a notary public to establish the authenticity of a signature on a legal document, which often requires the physical appearance of the person before the notary;

(*b*) *Attestation.* Attestation is the act of watching someone sign a legal document and then signing one's name as a witness. The purpose of attestation is to preserve evidence of the signing. By attesting, the witness states and confirms that the person whom he or she watched sign the document in fact did so. Attesting does not extend to vouching for the accuracy or truthfulness of the document. The witness can be called on to testify as to the circumstances surrounding the signing;[36]

[35] Some areas of the law recognize both the inherent insecurity of handwritten signatures and the impracticability of insisting on strict form requirements for the validity of legal acts, and admit that in some instances even the forgery of a signature would not deprive a document of its legal effect. Thus, for example, article 7 of the Uniform Law on Bills of Exchange and Promissory Notes annexed to the Convention providing a Uniform Law for Bills of Exchange and Promissory Notes, done at Geneva on 7 June 1930, provides that "if a bill of exchange bears the signatures of persons incapable of binding themselves by a bill of exchange, or forged signatures, or signatures of fictitious persons, or signatures which for any other reason cannot bind the persons who signed the bill of exchange or on whose behalf it was signed, the obligations of the other persons who signed it are none the less valid" (League of Nations, *Treaty Series*, vol. CXLIII, No. 3313).

[36] Adrian McCullagh, Peter Little and William Caelli, "Electronic signatures: understand the past to develop the future", *University of New South Wales Law Journal*, vol. 21, No. 2 (1998; see chap. III, sect. D, on the concept of witnessing.

(*c*) *Seals.* The practice of using seals in addition to, or in substitution of, signatures is not uncommon, especially in certain regions of the world.[37] Signing or sealing may, for example, provide evidence of the identity of the signatory; that the signatory agreed to be bound by the agreement and did so voluntarily; that the document is final and complete; or that the information has not been altered after signing.[38] It may also caution the signatory and indicate the intent to act in a legally binding manner.

12. Apart from these special situations, handwritten signatures have been used in commercial transactions, both domestic and international, for centuries without any particularly designed legislative or operational framework. The addressees or holders of the signed documents have assessed the reliability of signatures on a case-by-case basis depending on the level of trust enjoyed by the signatory. In fact, the vast majority of international written contracts—if there is "writing" at all—are not necessarily accompanied by any special formality or authentication procedure.

13. Cross-border use of signed documents becomes more complicated when public authorities are involved, as receiving authorities in a foreign country typically require some evidence of the identity and authority of the signatory. These requirements are traditionally satisfied by so-called "legalization" procedures, where the signatures are contained in domestic documents, authenticated by diplomatic authorities for use abroad. Conversely, consular or diplomatic representatives of the country where the documents are intended to be used may also authenticate signatures of foreign public authorities in the country of origin. Often consular and diplomatic authorities only authenticate signatures of certain high-ranking authorities in the issuing countries, thus requiring several layers of recognition of signatures where the document was originally issued by a lower-ranking official, or require prior notarization of signatures by a notary in the issuing country. Legalization is in most cases a cumbersome, time-consuming and expensive procedure. The Convention Abolishing the Requirement of Legalisation for Foreign Public Documents,[39] done at The Hague on 5 October 1961, was therefore negotiated to replace existing requirements with a simplified and standardized form (the "apostille"), which is used for providing a certification of certain public documents in the States parties to the Convention.[40] Only a competent authority designated by the State from which the public document emanates may issue an apostille. Apostilles certify the authenticity of the signature, the capacity in which the person signing the document has acted and, where appropriate, the identity of the seal or stamp that the document bears, but do not relate to the content of the underlying document itself.

[37] Seals are used in several countries in eastern Asia, such as China and Japan.

[38] Mark Sneddon, "Legislating to facilitate electronic signatures and records: exceptions, standards and the impact of the statute book", *University of New South Wales Law Journal*, vol. 21, No. 2 (1998); see part 2, Chap. II, "Policy objectives of writing and signature requirements".

[39] United Nations, *Treaty Series*, vol. 527, No. 7625.

[40] Those documents include documents emanating from an authority or official connected with a court or tribunal of the State (including documents issued by an administrative, constitutional or ecclesiastical court or tribunal, a public prosecutor, a clerk or a process-server); administrative documents; notarial acts; and official certificates that are placed on documents signed by persons in their private capacity.

14. As has been indicated above, in many legal systems, commercial contracts need not always to be contained in a document or evidenced by a writing to be valid. Even where a writing exists, a signature is not necessarily mandatory in order for the contract to be binding on the parties. Of course, where the law requires contracts to be in writing or to be signed, failure to meet those requirements would render the contract invalid. Perhaps more significant than form requirements for purposes of validity of contracts are form requirements for evidentiary purposes. The difficulty of proving oral agreements is one of the main reasons why commercial contracts are reflected in written documents or documented by correspondence, even if an oral agreement would be otherwise valid. Parties whose obligations are documented in signed writings are unlikely to succeed in attempts to negate the content of their obligations. Strict rules on documentary evidence typically aim at affording a high degree of reliability on the documents that meet them, which is generally believed to raise legal certainty. At the same time, however, the more elaborate the evidentiary requirements, the greater the opportunity a party has to invoke formal defects with a view to invalidating or denying enforceability to obligations they no longer intend to perform, for instance because the contract has become commercially disadvantageous. The interest for promoting security in the exchange of electronic communications needs therefore to be balanced against the risk of providing an easy way for traders in bad faith to repudiate their freely assumed legal obligations. Achieving this balance through rules and standards that are internationally recognized and operable across national borders is a major task of policymaking in the area of electronic commerce. The purpose of the present document is to help legislators and policymakers to identify the main legal issues involved in international use of electronic authentication and signature methods and consider possible solutions for them.

Part one

Electronic signature and authentication methods

Contents

Page

I. Definition and methods of electronic signature and authentication

A. General remarks on terminology

15. The terms "electronic authentication" and "electronic signature" are used to refer to various techniques currently available on the market or still under development for the purpose of replicating in an electronic environment some or all of the functions identified as characteristic of handwritten signatures or other traditional authentication methods.

16. A number of different electronic signature techniques have been developed over the years. Each technique aims at satisfying different needs and providing different levels of security, and entails different technical requirements. Electronic authentication and signature methods may be classified in three categories: those based on the knowledge of the user or the recipient (e.g. passwords, personal identification numbers (PINs)), those based on the physical features of the user (e.g. biometrics) and those based on the possession of an object by the user (e.g. codes or other information stored on a magnetic card).[41] A fourth category might include various types of authentication and signature methods that, without falling under any of the above categories, might also be used to indicate the originator of an electronic communication (such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message). Technologies currently in use include digital signatures within a public key infrastructure (PKI), biometric devices, PINs, user-defined or assigned passwords, scanned handwritten signatures, signature by means of a digital pen, and clickable "OK" or "I accept" boxes.[42] Hybrid solutions based on a combination of different technologies are becoming increasingly popular, such as, for instance, in the case of the combined use of passwords and transport layer security/secure sockets layer (TLS/SSL), which is a technology using a mix of public and symmetric key encryptions. The features of the main techniques currently used are described below (see paras. 25-66).

17. As is often the case, technology developed long before the law entered this area. The resulting gap between law and technology leads not only to varying levels of expert knowledge, but also to inconsistent use of terminology. Expressions that were traditionally used with a particular connotation under national laws started to be used

[41] See the report of the Working Group on Electronic Commerce on the work of its thirty-second session, held in Vienna from 19 to 30 January 1998 (A/CN.9/446, paras. 91 ff.).

[42] *UNCITRAL Model Law on Electronic Signatures ...* , part two, para. 33.

to describe electronic techniques whose functionality did not necessarily coincide with the functions or characteristics of the corresponding concept in legal usage. As has been seen above (see paras. 7-10), the notions of "authentication", "authenticity", "signature" and "identity", although in certain contexts closely related, are not identical or interchangeable. The usage in the information technology industry, which evolved essentially around concerns over network security, however, does not necessarily apply the same categories as legal writings.

18. In some cases, the expression "electronic authentication" is used to refer to techniques that, depending on the context in which they are used, may involve various elements, such as identification of individuals, confirmation of a person's authority (typically to act on behalf of another person or entity) or prerogatives (for example, membership in an institution or subscription to a service) or assurance as to the integrity of information. In some cases, the focus is on identity only,[43] but sometimes it extends to authority,[44] or a combination of any or all of those elements.[45]

19. Neither the UNCITRAL Model Law on Electronic Commerce,[46] nor the UNCITRAL Model Law on Electronic Signatures[47] uses the term "electronic authentication", in view of the different meaning of "authentication" in various legal systems and the possible confusion with particular procedures or form requirements. The Model Law on Electronic Commerce uses instead the notion of "original form" to provide the criteria for the functional equivalence of "authentic" electronic information. According to article 8 of the Model Law, where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(*a*) There exists "a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise;" and

[43] The Technology Administration of the United States Department of Commerce, for example, defines electronic authentication as "the process of establishing confidence in user identities electronically presented to an information system" (United States, Department of Commerce, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-63, version 1.0.2 (Gaithersburg, Maryland, April 2006), available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf (accessed on 5 June 2008)).

[44] For example, the Government of Australia developed an electronic authentication framework that defines electronic authentication as "the process of establishing a level of confidence in whether a statement is genuine or valid when conducting a transaction online or by phone. It helps build trust in an online transaction by giving the parties involved some assurance that their dealings are legitimate. These statements might include: identity details; professional qualifications; or the delegated authority to conduct transactions" (Australia, Department of Finance and Administration, *Australian Government e-Authentication Framework: An Overview* (Commonwealth of Australia, 2005), available at http://www.agimo.gov.au/infrastructure/authentication/agaf_b/overview/introduction#e-authentication (accessed on 5 June 2008)).

[45] The Principles for Electronic Authentication prepared by the Government of Canada, for instance, define authentication as "a process that attests to the attributes of participants in an electronic communication or to the integrity of the communication". Attributes, in turn, are defined as "information concerning the identity privilege or rights of a participant or other authenticated entity" (Canada, Industry Canada, *Principles for Electronic Authentication: a Canadian Framework* (Ottawa, May 2004), available at http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html (accessed on 5 June 2008).

[46] *UNCITRAL Model Law on Electronic Commerce* ... .

[47] *UNCITRAL Model Law on Electronic Signatures* ... .

(*b*) Where it is required that information be presented, that information “is capable of being displayed to the person to whom it is to be presented.”

20. In keeping with the distinction made in most legal systems between signature (or seals, where they are used instead) as a means of “authentication”, on the one hand, and “authenticity” as the quality of a document or record on the other, both model laws complement the notion of “originality” with the notion of “signature”. Article 2, subparagraph (*a*), of the UNCITRAL Model Law on Electronic Signatures defines electronic signature as 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 to “indicate the signatory’s approval of the information contained in the data message”.

21. The definition of “electronic signature” in UNCITRAL texts is deliberately broad, so as to encompass all existing or future “electronic signature” methods. As long as the methods used are “as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement”,[48] they should be regarded as meeting legal signature requirements. UNCITRAL texts relating to electronic commerce, as well as a large number of other legislative texts, are based on the principle of technological neutrality and therefore aim at accommodating all forms of electronic signature. Thus the UNCITRAL definition of electronic signature would cover the entire spectrum of “electronic signature” techniques, from higher-level security, such as cryptographically based signature assurance schemes associated with a PKI scheme (a common form of “digital signature” (see paras. 25-53)), to lower levels of security, such as unencrypted codes or passwords. The simple typing of the author’s name at the end of an e-mail message, which is the most common form of electronic “signature”, would, for instance, fulfil the function of correctly identifying the author of the message whenever it was not unreasonable to use such a low level of security.

22. The UNCITRAL model laws do not deal otherwise with issues related to access control or identity verification. This was also in keeping with the fact that, in a paper-based environment, signatures may be signs of identity but are necessarily attributive of identity. The UNCITRAL Model Law on Electronic Commerce deals, however, with the conditions under which the addressee of a data message is entitled to assume that the message actually originated from its purported originator. Indeed, article 13 of the Model Law provides that as between the originator and the addressee, a data message is deemed to be that of the originator if it was sent by a person “who had the authority to act on behalf of the originator in respect of that data message” or by “an information system programmed by, or on behalf of, the originator to operate automatically”. As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator and to act on that assumption, if (*a*) in order to ascertain whether the data message was that of the originator, “the addressee properly applied a procedure previously agreed to by the originator for that purpose” or (*b*) the data message as received by the addressee resulted from the actions

[48] *UNCITRAL Model Law on Electronic Commerce* ..., art. 7, para. 1 (*b*).

of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own. As a whole, these rules allow a party to infer someone else's identity, whether or not the message was electronically "signed" and whether or not the method used for attributing the message to the originator could be validly used for "signature" purposes. This conforms to current practice in the paper-based environment. Checking someone else's voice, physical appearance or identity papers (for example, a national passport) may suffice to conclude that the person is who he or she purports to be for the purpose of communicating with the person concerned, but would not qualify as a "signature" of such person under most legal systems.

23. Besides the confusion that has been caused by the fact that technical and legal usage of terms in the paper-based and electronic environments do not coincide, the various techniques mentioned earlier (see para. 16 above and the more detailed discussion in paras. 24-66 below) can be used for different purposes and provide a different functionality, depending on the context. Passwords or codes, for example, may be used to "sign" an electronic document, but they may also be used to gain access to a network, a database or another electronic service in much the same way as a key may be used to unlock a safe or open a door. However, while in the first instance the password is a proof of identity, in the second instance it is a credential or sign of authority, which, while ordinarily linked to a particular person, is also capable of being transferred to another. In the case of digital signatures, the inappropriateness of the current terminology is even more patent. The digital signature is widely regarded as a particular technology for "signing" electronic documents. However, it is at least questionable whether, from a legal point of view, the application of asymmetric cryptography for authentication purposes should be referred to as a digital "signature", as its functions go beyond the typical functions of a handwritten signature. The digital signature offers means both to "verify the authenticity of electronic messages" and to "guarantee the integrity of the contents." Furthermore, digital signature technology does not merely establish origin or integrity with respect to individuals as is required for signing purposes, but it can also authenticate, for instance, servers, websites, computer software or any other data that is distributed or stored digitally, which gives digital signatures much broader use than an electronic alternative for handwritten signatures.[49]

B. Main methods of electronic signature and authentication

24. For the purposes of this discussion, four main signature and authentication methods will be discussed: digital signatures; biometric methods; passwords and hybrid methods; and scanned or typed signatures.

[49] Babette Aalberts and Simone van der Hof, Digital Signature Blindness: *Analysis of Legislative Approaches toward Electronic Authentication* (November 1999), p. 8, available at http://rechten.uvt.nl/simone/Digsigbl.pdf (accessed on 5 June 2008).

1. Digital signatures relying on public key cryptography

25. "Digital signature" is a name for technological applications using asymmetric cryptography, also referred to as public key encryption systems, to ensure the authenticity of electronic messages and guarantee the integrity of the contents of these messages. The digital signature has many different appearances, such as fail stop digital signatures, blind signatures and undeniable digital signatures.

(a) Technical notions and terminology

(i) *Cryptography*

26. Digital signatures are created and verified by using cryptography, the branch of applied mathematics that is concerned with transforming messages into a seemingly unintelligible form and then back into their original form. Digital signatures use what is known as public key cryptography, which is often based on the use of algorithmic functions to generate two different but mathematically related "keys" (i.e. large numbers produced using a series of mathematical formulae applied to prime numbers).[50] One key is used for creating a digital signature or transforming data into a seemingly unintelligible form, and the other key is used for verifying a digital signature or returning the message to its original form.[51] Computer equipment and software utilizing two such keys are often collectively referred to as "cryptosystems" or, more specifically, "asymmetric cryptosystems" where they rely on the use of asymmetric algorithms.

(ii) *Public and private keys*

27. A complementary key used for digital signatures is named the "private key", which is used only by the signatory to create the digital signature and should be kept secret, while the "public key" is ordinarily more widely known and is used by a relying party to verify the digital signature. The private key is likely to be kept on a smart card or to be accessible through a personal identification number (PIN) or a biometric

[50] It should be noted, however, that the concept of public key cryptography, as discussed here, does not necessarily imply the use of algorithms based on prime numbers. Other mathematical techniques are currently used or under development, such as cryptosystems relying on elliptic curves, which are often described as offering a high degree of security through the use of significantly reduced key lengths.

[51] While the use of cryptography is one of the main features of digital signatures, the mere fact that a digital signature is used to authenticate a message containing information in digital form should not be confused with a more general use of cryptography for purposes of confidentiality. Confidentiality encryption is a method used for encoding an electronic communication so that only the originator and the addressee of the message will be able to read it. In a number of countries, the use of cryptography for confidentiality purposes is limited by law for reasons of public policy that may involve considerations of national defence. However, the use of cryptography for authentication purposes by producing a digital signature does not necessarily imply the use of cryptography to make any information confidential in the communication process, since the encrypted digital signature may be merely appended to a non-encrypted message.

identification device, such as thumbprint recognition. If many people need to verify the signatory's digital signature, the public key must be available or distributed to all of them, for example by attaching the certificates to the signature or by other means that ensure that the relying parties, and only those who have to verify the signatures, can obtain the related certificates. Although the keys of the pair are mathematically related, if an asymmetric cryptosystem has been designed and implemented securely it is virtually impossible to derive the private key from knowledge of the public key. The most common algorithms for encryption through the use of public and private keys are based on an important feature of large prime numbers: once they are multiplied together to produce a new number, it is particularly difficult and time-consuming to determine which two prime numbers created that new, larger number.[52] Thus, although many people may know the public key of a given signatory and use it to verify that signatory's signature, they cannot discover that signatory's private key and use it to forge digital signatures.

(iii) *Hash function*

28. In addition to the generation of key pairs, another fundamental process, generally referred to as a "hash function", is used in both creating and verifying a digital signature. A hash function is a mathematical process, based on an algorithm that creates a digital representation or compressed form of the message (often referred to as a "message digest" or "fingerprint" of the message), in the form of a "hash value" or "hash result" of a standard length that is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used. In the case of a secure hash function, sometimes called a "one-way hash function", it is virtually impossible to derive the original message from knowledge of its hash value. Another basic feature of hash functions is that it is also virtually impossible to find another binary object (i.e. different from the one from which the digest was originally derived) producing the same digest. Hash functions therefore enable the software for creating digital signatures to operate on smaller and more predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed.

[52] Certain existing standards refer to the notion of "computational unfeasibility" to describe the expected irreversibility of the process, that is, the hope that it will be impossible to derive a user's secret private key from that user's public key. "'Computationally unfeasible' is a relative concept based on the value of the data protected, the computing overhead required to protect it, the length of time it needs to be protected, and the cost and time required to attack the data, with such factors assessed both currently and in the light of future technological advance." (American Bar Association, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (Chicago, American Bar Association, 1 August 1996), p. 9, note 23, available at http://www.abanet.org/scitech/ec/isc/dsgfree.html (accessed on 4 June 2008)).

(iv) *Generation of a digital signature*

29. To sign a document or any other item of information, the signatory first delimits precisely the borders of what is to be signed. Then a hash function in the signatory's software computes a hash result unique (for all practical purposes) to the information to be signed. The signatory's software then transforms the hash result into a digital signature using the signatory's private key. The resulting digital signature is thus unique to both the information being signed and the private key used to create the digital signature. Typically, a digital signature (the encryption with the signer's private key of the hash result of the message) is attached to the message and stored or transmitted with that message. However, it may also be sent or stored as a separate data element, as long as it maintains a reliable association with the corresponding message. Since a digital signature is unique to its message, it is inoperable if permanently disassociated from the message.

(v) *Verification of digital signature*

30. Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key. Verification of a digital signature is accomplished by computing a new hash result for the original message, by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks whether the digital signature was created using the corresponding private key and whether the newly computed hash result matches the original hash result that was transformed into the digital signature during the signing process.

31. The verification software will confirm the digital signature as "verified" from a cryptographic viewpoint if (*a*) the signatory's private key was used to sign digitally the message, which is known to be the case if the signatory's public key was used to verify the signature because the signatory's public key will verify only a digital signature created with the signatory's private key; and (*b*) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

(vi) *Other uses of digital signature technology*

32. Digital signature technology has a much broader use than merely to "sign" electronic communications in the same manner that handwritten signatures are used to sign documents. Indeed, digitally signed certificates are often used, for instance, to "authenticate" servers or websites, for example in order to guarantee to their users that the server or website is the one it purports to be or is genuinely attached to the company that claims to run the server or website. Digital signature technology can

also be used to "authenticate" computer software, for example in order to guarantee the authenticity of software downloaded from a website, or to guarantee that a particular server uses a technology that is widely recognized as providing a certain level of connection security, or to "authenticate" any other data that are distributed or stored digitally.

(b) Public key infrastructure and certification services providers

33. To verify a digital signature, the verifier must have access to the signatory's public key and be assured that it corresponds to the signatory's private key. However, a public-key and private-key pair has no intrinsic association with any person; it is simply a pair of numbers. An additional mechanism is necessary to associate reliably a particular person or entity to the key pair. This is particularly important as there may be no pre-existing relationship of trust between the signatory and the recipients of digitally signed communications. To that effect, the parties involved must have a degree of confidence in the public and private keys being issued.

34. The required level of confidence may exist between parties who trust each other, who have dealt with each other over a period of time, who communicate on closed systems, who operate within a closed group or who are able to govern their dealings contractually, for example in a trading partner agreement. In a transaction involving only two parties, each party can simply communicate (by a relatively secure channel such as by courier or telephone) the public key of the key pair each party will use. However, the same level of confidence may not be present when the parties deal infrequently with each other, communicate over open systems (e.g. the World Wide Web on the Internet), are not in a closed group or do not have trading partner agreements or other laws governing their relationships. Moreover, it should be taken into account that, if disputes need be settled in court or by arbitration, it might be difficult to demonstrate that a certain public key had or had not actually been given to the recipient by its legitimate owner.

35. A prospective signatory might issue a public statement indicating that signatures verifiable by a given public key should be treated as originating from that signatory. The law of the enacting State would govern the form and the legal effectiveness of such a statement. For example, a presumption of attribution of electronic signatures to a particular signatory could be established through publication of the statement in an official gazette or in a document recognized as "authentic" by public authorities. However, other parties might be unwilling to accept the statement, especially where there is no prior contract establishing the legal effect of that published statement with certainty. A party relying upon such an unsupported published statement in an open system would run a great risk of inadvertently trusting an impostor or of having to disprove a false denial of a digital signature (an issue often referred to in the context of "non-repudiation" of digital signatures) if a transaction should turn out to prove disadvantageous for the purported signatory.

36. One solution to some of these problems is the use of one or more third parties to associate an identified signatory or the signatory's name with a specific public key. That third party is generally referred to as a "certification authority", "certification services provider" or "supplier of certification services" in most technical standards and guidelines (in the UNCITRAL Model Law on Electronic Signatures, the term "certification service provider" has been chosen). In a number of countries, such certification authorities are being organized hierarchically into what is often referred to as a "public key infrastructure" (PKI). Certification authorities within a PKI can be established in a hierarchical structure, where some certification authorities only certify other certification authorities, which provide services directly to users. In such a structure, some certification authorities are subordinate to other certification authorities. In other conceivable structures, all certification authorities may operate on an equal footing. In any large PKI, there would likely be both subordinate and superior certification authorities. Other solutions may include, for example, certificates issued by relying parties.

(i) *Public key infrastructure*

37. Setting up a PKI is a way to provide confidence that (*a*) a user's public key has not been changed and in fact corresponds to that user's private key; and (b) the cryptographic techniques being used are sound. To provide such confidence, a PKI may offer a number of services, including the following: (*a*) managing cryptographic keys used for digital signatures; (*b*) certifying that a public key corresponds to a private key; (*c*) providing keys to end-users; (*d*) publishing revocation information on public keys or certificates; (*e*) managing personal tokens (e.g. smart cards) that can identify the user with unique personal identification information or can generate and store an individual's private keys; (*f*) checking the identification of end-users and providing them with services; (*g*) providing time-stamping services; and (*h*) managing cryptographic keys used for confidentiality encryption where the use of such a technique is authorized.

38. A PKI may be based on various hierarchical levels of authority. For example, models considered in certain countries for the establishment of possible PKIs include references to the following levels: (*a*) a unique "root authority", which would certify the technology and practices of all parties authorized to issue cryptographic key pairs or certificates in connection with the use of such key pairs and would register subordinate certification authorities;[53] (*b*) various certification authorities, placed below the root authority, which would certify that a user's public key actually corresponds to that user's private key (i.e. has not been tampered with); and (*c*) various local registration authorities, placed below the certification authorities, which would receive requests from users for cryptographic key pairs or for certificates in connection with the use of such key pairs, requiring proof of identification and checking identities of potential users. In certain countries, it is envisaged that notaries public might act as, or support, local registration authorities.

[53] The question as to whether a government should have the technical ability to retain or recreate private confidentiality keys may be dealt with at the level of the root authority.

39. PKIs organized in a hierarchical structure are scalable in the sense that they may incorporate entire new PKI "communities" simply by having their root authority establish a trust relationship with a new community's root authority.[54] The root authority of the new community may be incorporated directly under the "root" of the receiving PKI, thus becoming a subordinate certification services provider within that PKI. The root authority of the new community may also become a subordinate certification services provider to one of the subordinate certification services providers within the existing PKI. Another attractive feature of hierarchical PKIs is that it makes it easy to develop certification paths because they run in one direction only, from a user's certificate back to the trust point. Furthermore, certification paths within a hierarchical PKI are relatively short and the users of a hierarchy know implicitly which applications a certificate may be used for, based on the position of the certification services provider within the hierarchy. However, hierarchical PKIs have drawbacks as well, mainly as a consequence of reliance on a single trust point. If the root authority is compromised, the entire PKI is compromised. Furthermore, some countries have found it difficult to select one single entity as a root authority and to impose such a hierarchy on all other certification services providers.[55]

40. The so-called "mesh" PKI is an alternative to a hierarchical PKI. Under this model, certification services providers are connected in a peer-to-peer relationship. All certification services providers in such a model can be trust points. Generally, users will trust the certification services providers that issued their certificate. Certification services providers will issue certificates to each other; the pair of certificates describes their reciprocal trust relationship. The lack of hierarchy in such a system means that certification services providers cannot impose conditions governing the types of certificate issued by other certification services providers. If a certification services provider wishes to limit the trust extended to other certification services providers, it must specify these limitations in the certificates issued to its peers.[56] Harmonizing conditions and limitations of mutual recognition may however be an extremely complex objective.

41. A third alternative structure is built around the so-called "bridge" certification services provider. This structure may be particularly useful to allow various pre-existing PKI communities to trust each other's certificates. Unlike a certification services provider in a mesh PKI, a bridge certification services provider does not issue certificates directly to users. Neither is a bridge certification services provider intended to be used as a trust point by the users of the PKI, as would be the case with a root certification services provider. Instead, the bridge certification services provider establishes peer-to-peer trust relationships with the different user communities, thus allowing the users to keep their natural trust points within their respective PKIs. If a user community implements a trust domain in the form of a hierarchical PKI, the

[54] William T. Polk and Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, National Institute of Standards and Technology (September 2000), available at http://csrc.nist.gov/pki/documents/B2B-article.pdf (accessed on 5 June 2008).

[55] Polk and Hastings (*Bridge Certification Authorities* ...) note that in the United States, it was very difficult to single out one agency of the Government to assume overall authority over the federal PKI.

[56] *Polk and Hastings, Bridge Certification Authorities … .*

bridge certification services provider will establish a relationship with the root authority of that PKI. However, if the user community implements a trust domain by creating a mesh PKI, the bridge certification services provider will only need to establish a relationship with one of the PKI's certification services providers, which then becomes the principal certification services provider within that PKI for the purpose of establishing the bridge of trust to the other PKI. The bridge of trust that joins two or more PKIs through their mutual relationship with a bridge certification services provider enables users from the different user communities to interact with each other through the bridge certification services provider with a specified level of trust.[57]

(ii) Certification services provider

42. To associate a key pair with a prospective signatory, a certification services provider (or certification authority) issues a certificate, which is an electronic record that lists a public key together with the name of the certificate subscriber as the "subject" of the certificate, and which may confirm that the prospective signatory identified in the certificate holds the corresponding private key. The principal function of a certificate is to bind a public key with a particular signatory. A "recipient" of the certificate desiring to rely upon a digital signature created by the signatory named in the certificate can use the public key listed in the certificate to verify that the digital signature was created with the corresponding private key. If such verification is successful, a level of assurance is provided technically that the signatory created the digital signature and that the portion of the message used in the hash function (and, consequently, the corresponding data message) has not been modified since it was digitally signed.

43. To assure the authenticity of the certificate with respect to both its contents and its source, the certification services provider digitally signs it. The issuing certification services provider's digital signature on the certificate can be verified by using the public key of the certification services provider listed in another certificate by another certification services provider (which may, but need not, be on a higher level in a hierarchy), and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness. Recording the digital signature in a certificate issued by the certification services provider (sometimes referred to as a "root certificate") is another possible way of verifying a digital signature.[58]

44. In each case, the issuing certification services provider may digitally sign its own certificate during the operational period of the other certificate used to verify the certification services provider's digital signature. Under the laws of some States, one way of building trust in the digital signature of the certification services provider might be to publish the public key of the certification services provider or certain data pertaining to the root certificate (such as a "digital fingerprint") in an official gazette.

[57] The bridge certification services provider was the structure eventually chosen to set up the PKI system for the United States Government (Polk and Hastings, *Bridge Certification Authorities ...*). This was also the model followed to develop the PKI system of the Government of Japan.

[58] *UNCITRAL Model Law on Electronic Signatures ...*, part two, para. 54.

45. A digital signature corresponding to a message, whether created by the signatory to authenticate a message or by a certification services provider to authenticate its certificate, should generally be reliably time-stamped to allow the verifier to determine whether the digital signature was created during the operational period stated in the certificate and whether the certificate was valid (e.g. was not mentioned in a revocation list) at the relevant time, which is a condition of the verifiability of a digital signature.

46. To make a public key and its correspondence to a specific signatory readily available for verification, the certificate may be published in a repository or made available by other means. Typically, repositories are online databases of certificates and other information available for retrieval and use in verifying digital signatures.

47. Once issued, a certificate may prove to be unreliable, for example in situations where the signatory misrepresents its identity to the certification services provider. In other circumstances, a certificate may be reliable when issued, but may become unreliable afterwards. If the private key is compromised, for example through loss of control of the private key by the signatory, the certificate may lose its trustworthiness or become unreliable, and the certification services provider (at the signatory's request or even without the signatory's consent, depending on the circumstances) may suspend (temporarily interrupt the operational period) or revoke (permanently invalidate) the certificate. In a timely fashion upon suspending or revoking a certificate, the certification services provider may be expected to publish a notice of the revocation or suspension, or to notify persons who enquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate. Similarly, where applicable, the certification services provider's own certificate should also be reviewed for possible revocation, as should the certificate issued for the verification of the signature of the time-stamping authority on the time-stamp tokens and the certificate of the certification services provider that issued the certificate of the time-stamping authority.

48. Certification authorities could be operated by private-sector service providers or government authorities. In a few countries, it is envisaged that, for public policy reasons, only government entities should be authorized to operate as certification authorities. In most countries, however, either certification services are entirely left for the private sector, or State-run certification services providers coexist with private-sector providers. There are also closed certification systems, where small groups set up their own certification services provider. In some countries, State-owned certification services providers issue certificates only in support of digital signatures used by the public administration. Irrespective of whether certification authorities are operated by public entities or by private-sector service providers, and of whether certification authorities would need to obtain a licence to operate, there is typically more than one certification services provider operating within a PKI. Of particular concern is the relationship between the various certification authorities (see paras. 38-41 above).

49. It may be incumbent upon the certification services provider or the root authority to ensure that its policy requirements are met on an ongoing basis. While the selection of certification authorities may be based on a number of factors, including the strength of the public key being used and the identity of the user, the trustworthiness of any

certification services provider may also depend on its enforcement of standards for issuance of certificates and the reliability of its evaluation of data received from users who request certificates. Of particular importance is the liability regime applying to any certification services provider with respect to its compliance with the policy and security requirements of the root authority or higher-level certification services provider, or with any other applicable requirement, on an ongoing basis. Of equal importance is the obligation of the certification services provider to act in accordance with the representations made by it with respect to its policies and practices, as envisaged in article 9, paragraph 1 (*a*), of the Model Law on Electronic Signatures.

(c) Practical problems in public key infrastructure implementation

50. Despite the considerable knowledge on digital signature technologies and the way they function, the implementation of public key infrastructures and digital signature schemes has, in practice, faced some problems that have kept the level of use of digital signatures below expectations.

51. Digital signatures work well as a means to verify signatures that are created during the period of validity of a certificate. However, once the certificate expires or is revoked, the corresponding public key loses its validity, even if the key pair was not compromised. Accordingly, a PKI scheme would require a digital signature management system to ensure the availability of the signature over time. The main difficulty results from the risk that the "original" electronic records (that is, the binary digits – or "bits" – that make up the computer file in which the information is recorded), including the digital signature, may become unreadable or unreliable over time, mainly because of the obsolescence of the software, the equipment or both. In addition, the digital signature may become insecure as a consequence of scientific advances in cryptanalysis, the signature verification software may not be available over long periods of time or the document may lose its integrity.[59] This makes the long-term retention of electronic signatures generally problematic. Even though digital signatures were for some time believed to be essential for archival purposes, experience has shown that they are not immune to long-term risks. Since every alteration to the record after the time when the signature was created will cause the verification of the signature to fail, reformatting operations intended to keep a record legible for the future (such as data migration or conversion) may affect the durability of the signature.[60] In actuality,

[59] Jean-François Blanchette, "Defining electronic authenticity: an interdisciplinary journey", available at http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf (accessed on 5 June 2008) (paper published in a supplemental volume of the 2004 International Conference on Dependable Systems and Networks (DSN 2004), Florence, Italy, 28 June-1 July 2004), pp. 228-232.

[60] "In the end, all we can preserve in an electronic context are bits. However, it has been clear for a long time that it is very difficult to keep a set of bits indefinitely. With the lapse of time, the set of bits becomes illegible (to the computer and thus to humans) as a result of the technological obsolescence of the application program and/or of the hardware (e.g. the reader). The problem of the durability of PKI-based digital signatures has been poorly studied so far because of its complexity. … Although the authentication tools that were used in the past, such as handwritten signatures, seals, stamps, fingerprints etc. are also subject to reformatting (e.g. microfilming) because of the obsolescence of the paper carrier, they never become completely useless after reformatting. There is always at least a copy available that can be compared with other original authentication tools." (Jos Dumortier and Sofie Van den Eynde, *Electronic Signatures and Trusted Archival Services*, p. 5 (available at http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where, accessed on 5 June 2008).

digital signatures were conceived more for providing security for the communication of information than for the preservation of information over time.[61] Initiatives to overcome this problem have not yet resulted in a durable solution.[62]

52. Another area where digital signatures and PKI schemes may give rise to practical problems concerns data security and privacy protection. Certification services providers must keep safe the keys used to sign certificates issued to their customers and may be exposed to attempts by outsiders to gain unauthorized access to the keys (see also part two, paras. 223-226 below). Furthermore, certification services providers need to obtain a series of personal data and business information from persons applying for certificates. This information needs to be stored by the certification services provider

[61] In 1999, archivists from various countries launched the International Research on Permanent Authentic Records in Electronic Systems (InterPARES) project with the aim of "developing the theoretical and methodological knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form" (see http://www.interpares.org, accessed on 5 June 2008). The draft report of the Authenticity Task Force (available at http://www.interpares.org/documents/atf_draft_final_report.pdf, accessed on 5 June 2008), which was part of the first phase of the project (InterPARES 1, concluded in 2001), indicated that "digital signatures and public key infrastructures (PKI) are examples of technologies that have been developed and implemented as a means of authentication for electronic records that are transmitted across space. Although record-keepers and information technology personnel place their trust in authentication technologies to ensure the authenticity of records, these technologies were never intended to be, and are not currently viable as, a means of ensuring the authenticity of electronic records over time" (emphasis added). The final report of InterPARES 1 is available at http://www.interpares.org/book/index.htm (accessed on 5 June 2008). The continuation of the project (InterPARES 2), aims to develop and articulate the concepts, principles, criteria and methods that can ensure the creation and maintenance of accurate and reliable records and the long-term preservation of authentic records in the context of artistic, scientific and government activities developed from 1999 and 2001.

[62] The European Electronic Signature Standardization Initiative (EESSI), for example, was created in 1999 by the Information and Communications Technology Standards Board, a collaborative group of organizations concerned with standardization and related activities in information and communications technologies established to coordinate the standardization activity in support of the implementation of the European Union directive on electronic signatures (see *Official Journal of the European Communities*, L 13/12, 19 January 2000). The EESSI consortium (a standardization effort which seeks to translate the requirements of the European directive on electronic signatures into European standards) sought to address the need for ensuring the long-term preservation of cryptographically signed documents through its standard on electronic signature formats (Electronic Signature Formats ES 201 733, ETSI, 2000). The format distinguishes between signature validation moments: the initial validation and a later validation. The format for later validation encapsulates all of the information that can eventually be used in the validation process, such as revocation information, time stamps, signature policies etc. This information is gathered at the stage of initial validation. The designers of these electronic signature formats were concerned with the security threat to the validity of the signature that results from decay in cryptographic strength. To guard against this threat of decay, EESSI signatures are regularly time-stamped afresh, with signing algorithms and key sizes appropriate to state-of-the-art cryptanalytic methods. The problem of software longevity was addressed in a 2000 report by EESSI, which introduced "trusted archival services", a new type of commercial service that would be offered by yet-to-be-specified competent bodies and professions, in order to guarantee the long-term preservation of cryptographically signed documents. The report lists a number of technical requirements such archival services should provide, among them, "backward compatibility" with computer hardware and software, through either preservation of equipment or emulation (see Blanchette, "Defining electronic authenticity…"). A follow-up study on the EESSI recommendation on trusted archival services by the Interdisciplinary Centre for Law and Information Technology of the Katholieke Universiteit Leuven, Belgium, entitled *European Electronic Signature Standardization Initiative: Trusted Archival Services* (Phase 3, final report, 28 August 2000) is available at http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf?where=, accessed on 5 June 2008). EESSI was closed in October 2004. Systems to implement EESSI recommendations do not seem to be currently in operation (see Dumortier and Van den Eynde, Electronic Signatures and Trusted Archival Services ...).

for future reference. Certification services providers must take the necessary measures to ensure that access to such information is in accordance with applicable data protection laws.[63] However, unauthorized access remains a real threat.

2. Biometrics

53. A biometric is a measurement used to identify an individual through his or her intrinsic physical or behavioural traits. Traits that may be used for recognition in biometrics include DNA; fingerprints; iris, retina, hand or facial geometry; facial thermogram; ear shape; voice; body odour; blood vessel patterns; handwriting; gait; and typing patterns.

54. The use of biometrical devices typically involves capturing a biometrical sample, in digital form, of a biological feature of an individual. The biometrical data are then extracted from the sample to create a reference template. The identity of the person to whom the biometrical sample relates is confirmed or the authenticity of communications purportedly originating from that person is verified by comparing his or her biometrical data with those stored in the reference template.[64]

55. Biometrical techniques involve a number of risks related to the storage of biometrical data since biometrical patterns are typically not revocable. When biometrical systems have been compromised, the legitimate user has no recourse but to revoke the identification data and switch to another set of uncompromised identification data. Therefore, special rules are needed to prevent the abuse of biometrical databases.

56. The accuracy of biometrical techniques cannot be absolute since biological features tend to be inherently variable and any measurement may involve deviation. In this respect, biometrics are not considered unique identifiers but rather semi-unique identifiers. To accommodate those variations, the accuracy of biometrics may be manipulated by setting the threshold for matching the reference template with the extracted sample. However, a low threshold may bias the test towards false acceptance while a high threshold may tend towards false rejections. Nevertheless, the accuracy of authentication provided by biometrics may be adequate in the majority of commercial applications.

[63] See the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris, 1980), available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (accessed on 5 June 2008); Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, *European Treaty Series*, No. 108), available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (accessed on June 2008); Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95); and directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*Official Journal of the European Communities*, L 281, 23 November 1995, available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett (accessed on June 2008)).

[64] International Association for Biometrics and International Computer Security Association, *1999 Glossary of Biometric Terms* (copy available with the Secretariat).

57. Moreover, data protection and human rights issues arise in relation to the storage and disclosure of biometrical data. Data protection laws,[65] although they may not refer expressly to biometrics, aim at protecting personal data relating to natural persons, and the processing of such data, both in their raw form and as templates, is at the core of biometrics technology.[66] Moreover, measures may be required to protect consumers against risks generated by the private use of biometrical data, as well as in case of identity theft. Other legal domains, including labour and health law, may also come into play.[67]

58. Technical solutions might assist in addressing some concerns. For instance, storage of biometrical data on smart cards or tokens may protect against unauthorized access, which could occur if the data is stored on a centralized computer system. Moreover, best practices have been developed to reduce risks in different areas such as scope and capabilities; data protection; user control of personal data; and disclosure, auditing, accountability and oversight.[68]

59. Biometrical devices are generally considered as offering a high level of security. While they are compatible with a range of uses, their current main usage is in government applications, particularly law enforcement applications such as immigration clearance and access controls.

60. Commercial applications have also been developed, where often biometrics are used in a two-factor authentication process requiring provision of an element in possession of the individual (biometrics) and an element in the knowledge of the individual (typically, a password or PIN). Moreover, applications have been developed to store and compare the characteristics of a person's handwritten signature. Digital-based pen tablets record the pen pressure and duration of the signing process. The data are then stored as an algorithm to be used for comparison against future signatures. However, in the light of the inherent features of biometrics, caution is also expressed on the dangers of a gradual, uncontrolled increase relating to their use in routine commercial transactions.

61. If biometrical signatures are used as a substitute for handwritten signatures, a problem of evidence may arise. As mentioned before, the reliability of biometrical evidence varies between the technologies used and the chosen false acceptance rate. Besides, there is the possibility of tampering with or falsifying biometrical data stored in digital form.

[65] See note 63.

[66] Paul de Hert, *Biometrics: Legal Issues and Implications*, background paper for the Institute for Prospective Technological Studies of the European Commission (European Communities, Directorate General Joint Research Centre, 2005), p. 13, available at http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf (accessed on 5 June 2008).

[67] For instance, in Canada, the use of biometrics was discussed with respect to the application of the Personal Information Protection and Electronic Documents Act (2000, c. 5) in the workplace (see Turner v. TELUS Communications Inc., 2005 FC 1601, 29 November 2005 (Federal Court of Canada)).

[68] See, for an example of best practices, the International Biometric Group BioPrivacy Initiative, "Best practices for privacy-sympathetic biometric deployment", available at http://www.bioprivacy.org (accessed on 5 June 2008).

62. The general reliability tests under the UNCITRAL Model Law on Electronic Signatures and Model Law on Electronic Commerce, as well as under the more recent United Nations Convention on the Use of Electronic Communications in International Contracts,[69] can be applied to the use of biometrical signatures. To ensure uniformity, it might also be useful to develop international guidelines on the use and management of biometrical methods.[70] Whether such standards would be premature, given the current state of development of biometrical technologies, and might risk hampering the continued development of biometrical technologies needs to be carefully considered.

3. Passwords and hybrid methods

63. Passwords and codes are used both for controlling access to information or services and for "signing" electronic communications. In practice, the latter use is less frequent than the former, because of the risk of compromising the code if it is transmitted in non-encrypted messages. Passwords and codes are however the most widely used method of "authentication" for purposes of access control and identity verification in a broad range of transactions, including most Internet banking transactions, cash withdrawals at automated teller machines and consumer credit card transactions.

64. It should be recognized that multiple technologies can be used to "authenticate" an electronic transaction. Several technologies or several uses of a single technology can be utilized for a single transaction. For example, signature dynamics for authentication can be combined with cryptography for message integrity. Alternatively, passwords can be sent over the Internet, using cryptography (e.g. SSL in browsers) to protect them, in conjunction with the use of biometrics to trigger a digital signature (asymmetric cryptography), which, on receipt, generates a Kerberos ticket (symmetric cryptography). In developing legal and policy frameworks to deal with these technologies, consideration should be given to the role of multiple technologies. Legal and policy frameworks for electronic authentication will need to be flexible enough to cover hybrid technology approaches, as those that focus on specific technologies could impede the use of multiple technologies.[71] Technology-neutral provisions would facilitate the acceptance of such hybrid technology approaches.

[69] The draft Convention on the Use of Electronic Communications in International Contracts was approved by UNCITRAL at its thirty-eighth session (Vienna, 4-15 July 2005). The Convention was adopted by the General Assembly by its resolution 60/21 of 23 November 2005.

[70] These could be compared with the criteria for reliability presented in the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (UNCITRAL Model Law on Electronic Signatures ... , part two, para. 75).

[71] See Foundation for Information Policy Research, *Signature Directive Consultation Compilation*, 28 October 1998, which provides a compilation of responses made during consultations on the European Union draft directive on electronic signatures, prepared at the request of the European Commission, available at www.fipr.org/publications/sigdirecon.html (accessed on 5 June 2008).

4. Scanned signatures and typed names

65. The main reason for legislative interest in electronic commerce in the private law area has been concern about how new technologies may affect the application of rules of law that were conceived for other media. This attention to technology has often led, deliberately or not, to a focus on sophisticated technologies that offer a higher level of security for electronic authentication and signature methods. It is often neglected, in that context, that a very large number, if not the majority, of business communications exchanged throughout the world do not make use of any particular authentication or signature technology.

66. In day-to-day practice, companies around the world are often satisfied, for instance, with exchanging messages by e-mail without the use of any form of authentication or signature other than the typed name, title and address of parties at the bottom of their communications. Sometimes a more formal appearance is given by the use of facsimile or scanned images of handwritten signatures, which of course constitute only a copy in digitalized form of a handwritten original. Neither typed names on unencrypted e-mail messages nor scanned signatures offer a high level of security or can definitely prove the identity of the originator of the electronic communication in which they appear. Nevertheless, business entities freely choose to use these forms of "authentication" in the interest of ease, expediency and cost-effectiveness of communications. It is important for legislators and policymakers to bear in mind these widespread business practices when considering regulating electronic authentication and signature. Stringent requirements for electronic authentication and signature, in particular the imposition of a particular method or technology, may inadvertently cast doubt as to the validity and enforceability of a significant number of transactions that are entered into every day without the use of any particular kind of authentication or signature. That, in turn, may stimulate parties acting in bad faith to avoid the consequences of obligations they freely assumed by questioning the authenticity of their own electronic communications. It is unrealistic to expect that imposing a certain high level of authentication and signature requirements would eventually lead all parties to actually use them on a daily basis. Recent experience with sophisticated methods, such as digital signatures, has shown that concerns about cost and complexity often limit the practical use of authentication and signature techniques.

C. Electronic identity management

67. In the electronic world, natural or legal persons may access the services of a number of providers. Every time a person registers with a service provider to access its services, an electronic "identity" is created. Moreover, a single identity may be linked to a number of accounts for each application or platform. The multiplication of identities and of their accounts may hinder their management both for the user and for the service provider. These difficulties could be avoided by having a single electronic identity for each person.

68. The registration with a service provider and the creation of an electronic identity entails the establishment of a mutually trusted relationship between the person and the provider. The creation of a single electronic identity requires gathering together those bilateral relationships into a broader framework where they could be managed jointly, in what is referred to as identity management. Benefits of identity management on the provider side may include security improvements, easier regulatory compliance and greater business agility; on the user side, they may include facilitated access to information.

69. Identity management may be described in the context of the following approaches:

(*a*) *The traditional user access approach.* This approach follows the log-on paradigm, and is typically based on the use of information contained in a device such as a smart card or otherwise held by the customer and which the customer uses to log on to a service. The user access approach to identity management focuses on the administration of user authentication, access rights, access restrictions, account profiles, passwords and other attributes in one or more applications or systems. It aims at facilitating and controlling access to applications and resources while protecting confidential personal and business information from unauthorized users;

(*b*) *The services approach.* This represents a more innovative paradigm, and is based on a system that delivers personalized services to users and their devices. Under this approach, the scope of identity management becomes broader and includes all the resources of the company that are used to deliver online services, such as network equipment, servers, portals, content, applications and products, as well as a user's credentials, address books, preferences and entitlements. In practice, it could include, for instance, information relating to parental control settings and participation in loyalty programmes.

70. Efforts are under way to expand identity management at both the business and the governmental levels. However, it should be noted that policy choices in the two scenarios may differ considerably. The governmental approach, for instance, may be more oriented towards better serving citizens' needs and therefore may be slanted towards interaction with physical persons. In contrast, commercial applications need to take into account the increasing use of automated machines in business transactions and therefore may adopt features meant to accommodate the specific needs of those machines.

71. Difficulties identified in relation to identity management systems include privacy concerns due to the risks associated with the misuse of unique identifiers. Moreover, issues may arise also with respect to differences in applicable legal regulations, especially in relation to the possibility to delegate authority to act for another. Solutions built around voluntary business cooperation based on a so-called circle of trust, where participants are required to rely on the correctness and accuracy of the information provided to them by other members of the circle, have been suggested. However, this

approach may not be fully sufficient to regulate all related matters and might still require the adoption of a legal framework. Guidelines have also been developed to provide a legal framework for circles of trusted infrastructures.[72]

72. With respect to technical interoperability, the International Telecommunication Union has established a focus group on identity management to facilitate and advance the development of a generic identity management framework and means of discovery of autonomous distributed identities and identity federations and implementations.[73]

73. Identity management solutions are being developed also in the framework of e-government. For instance, in the context of the European Union "i2010: a European information society for growth and employment" initiative,[74] a study on identity management in e-government was initiated to facilitate progress towards a coherent approach in electronic identity management in e-government in the European Union based on existing expertise and initiatives in the European Union member States.[75]

74. The distribution of electronic signature devices, often in the form of smart cards, as part of e-government initiatives is becoming increasingly common. Nationwide distribution of smart cards has been launched, for example, in Belgium, where such cards were originally introduced in a number of provinces in 2003[76] and, after a successful trial period, eventually extended to the entire country.[77] The Belgian system essentially involves the issuance of physical identity cards equipped with a chip which contains the data needed by a citizen to generate a digital signature.[78]

[72] The Liberty Alliance Project (see www.projectliberty.org) is an alliance of more than 150 companies and non-profit and governmental organizations from around the globe. The consortium is committed to developing an open standard for federated network identity that supports all current and emerging network devices. Federated identity offers businesses, governments, employees and consumers a more convenient and secure way to control identity information in today's digital economy and is a key component in driving the use of e-commerce and personalized data services, as well as Web-based services. Membership is open to all commercial and non-commercial organizations.

[73] See http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html (accessed on 20 March 2008).

[74] Communication from the Commission of the European Communities to the European Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: "i2010 – A European Information Society for growth and employment", COM(2005) 229 final (Brussels, 1 June 2005), available at http://eur-lex.europa.eu (accessed on 20 March 2008).

[75] See *Modinis Study on Identity Management in eGovernment: Identity Management Issue Report* (European Commission, Directorate General Information Society and Media, 18 September 2006), pp. 9-12, available at https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi (accessed on 6 June 2008).

[76] The electronic identity card was introduced in Belgium in 2003 by the Loi du 25 mars 2003 modifiant le loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques (Moniteur belge, Ed. 4, 28 March 2003, p. 15921).

[77] See the Arrêté royal du 1er septembre 2004 portant la décision de procéder à l'introduction généralisée de la carte d'identité électronique (Moniteur belge, Ed. 2, 15 September 2004, p. 56527). For general information, see http://eid.belgium.be (accessed on 6 June 2008).

[78] For general information, see http://eid.belgium.be (accessed on 6 June 2008).

75. Austria has developed an identity management system that records identification attributes for each Austrian citizen but does not incorporate those attributes into citizens' official identification documents. Instead, Austria chose technology-neutral standards and, as a result, a range of technology solutions have been developed and adopted by consumers. The Austrian system is based on a "person identity link", which is a structure signed by the issuing public authority that assigns a unique identification feature of a person (for example, a registration number) to one or more certificates belonging to that person. As such, the person identity link can be used for the unique, automated identification of a person when that person approaches the public authority during the course of a procedure.[79] This "unique identification feature" may be stored on any smart card of the individual's choice (e.g. automated teller machine card, social security card, student identification card, labour union or professional association membership card, a personal computer or laptop). Signature devices may also be transmitted via mobile phone, in the form of one-time codes specially generated by the mobile phone services provider, which acts as custodian of the citizen's unique identification feature.

76. This system allows for the issuance of sector-specific identifiers, which are kept strictly separate but are all linked to a central identity store. This architecture precludes data-sharing issues and protects data privacy. The card, known as the "citizen card", is intended to become the official identity document for electronic administrative procedures, such as the filing of applications via the Internet. The citizen card establishes a security infrastructure that is available to all, including commercial customers. Companies can develop secure online services for their customers by building on the infrastructure provided by the citizen card.

77. As a consequence of initiatives such as those described above, a very large number of citizens may receive devices with, inter alia, secure electronic signature capabilities at low cost. While the primary goal of initiatives of this type may not be commercial, such devices may equally be used in the commercial world. The convergence of the two domains of application is increasingly acknowledged.[80]

[79] Zentrum für sichere Informationstechnologie Austria (A-Sit), *XML Definition of the Person Identity Link* (available at http://www.buergerkarte.at/konzept/personenbindung/spezifikation/aktuell/ (accessed on 6 June 2008)).

[80] See, for instance, *2006 Korea Internet White Paper* (Seoul, National Internet Development Agency of Korea, 2006), p. 81, with reference to the dual use in e-government and e-commerce applications of the Electronic Signature Act of the Republic of Korea (available at http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1, accessed on 6 June 2008).

II. Legal treatment of electronic authentication and signatures

78. Creating trust in electronic commerce is of great importance for its development. Special rules may be needed to increase certainty and security in its use. Such rules may be provided in a variety of legislative texts: international legal instruments (treaties and conventions); transnational model laws; national legislation (often based on model laws); self-regulatory instruments;[81] or contractual agreements.[82]

79. A significant volume of electronic commercial transactions is performed in closed networks, that is, groups with a limited number of participants accessible only to previously authorized persons or companies. Closed networks support the operation of a single entity or an existing closed user group, such as financial institutions participating in the interbank payment system, securities and commodities exchanges, or an association of airlines and travel agents. In these cases, participation in the network is typically restricted to institutions and companies previously admitted to the group. Most of these networks have been in place for several decades, use sophisticated technology and have acquired a high level of expertise in the functioning of the system. The rapid growth of electronic commerce in the last decade has led to the development of other network models, such as supply chains or trade platforms.

80. Although these new groups were originally structured around direct computer-to-computer connections as were most of the closed networks already in existence at that time, there is an increasing trend towards using publicly accessible means, such as the Internet, as a common connection facility. Even under these more recent models, a closed network retains its exclusive character. Typically, closed networks operate under previously agreed contractual standards, agreements, procedures and rules known by various names such as "system rules", "operation rules" or "trading partner agreements" that are designed to provide and guarantee the necessary operational functionality, reliability and security for the members of the group. These rules and agreements often deal with matters such as recognition of the legal value of electronic

[81] See, for example, Economic Commission for Europe, United Nations Centre for Trade Facilitation and Electronic Business, recommendation No. 32, entitled "E-commerce self regulatory instruments (codes of conduct)" (ECE/TRADE/277), available at http://www.unece.org/cefact/recommendations/rec_index.htm (accessed on 5 June 2008).

[82] Many initiatives at the national and international levels aim at developing model contracts. (see, for example, Economic Commission for Europe, Working Party on the Facilitation of International Trade Procedures, recommendation No. 26, entitled "The commercial use of interchange agreements for electronic data interchange" (TRADE/WP.4/R.1133/Rev.1); and United Nations Centre for Trade Facilitation and Electronic Business, recommendation No. 31, entitled "Electronic commerce agreement" (ECE/TRADE/257), both available at http://www.unece.org/cefact/recommendations/rec_index.htm (accessed on 5 June 2008)).

communications, time and place of dispatch or receipt of data messages, security procedures for gaining access to the network and authentication or signature methods to be used by the parties.[83] Within the limits of the contractual freedom under applicable law, such rules and agreements are usually self-enforcing.

81. However in the absence of contractual rules, or to the extent that applicable law may limit their enforceability, the legal value of electronic authentication and signature methods used by the parties will be determined by the applicable rules of law, in the form of default or mandatory rules. The various options used in different jurisdictions to develop a legal framework for electronic signatures and authentication are discussed in the present chapter.

A. Technology approach of legislative texts

82. Electronic authentication legislation and regulation has taken many different forms at the international and domestic levels. Three main approaches for dealing with signature and authentication technologies can be identified: (*a*) the minimalist approach; (*b*) the technology specific-approach; and (*c*) the two-tiered or two-pronged approach.[84]

1. Minimalist approach

83. Some jurisdictions recognize all technologies for electronic signature, following a policy of technological neutrality.[85] This approach is called minimalist because it gives a minimum legal status to all forms of electronic signature. Under the minimalist approach, electronic signatures are considered to be the functional equivalent of handwritten signatures, provided that the technology employed is intended to serve certain specified functions and in addition meets certain technology-neutral reliability requirements.

84. The UNCITRAL Model Law on Electronic Commerce provides the most widely used set of legislative criteria for establishing a generic functional equivalence between electronic and handwritten signatures. Article 7, paragraph 1, of the Model Law provides:

[83] For a discussion of issues typically covered in trading partner agreements, see Amelia H. Boss, “Electronic data interchange agreements: private contracting toward a global environment”, *Northwestern Journal of International Law and Business*, vol. 13, No. 1 (1992), p. 45.

[84] Susanna F. Fischer, “Saving Rosencrantz and Guildenstern in a virtual world? A comparative look at recent global electronic signature legislation,” *Journal of Science and Technology Law*, vol. 7, No. 2 (2001), pp. 234 ff.

[85] For example, Australia and New Zealand.

"(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

> "(*a*) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
>
> "(*b*) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."

85. This provision contemplates the two main functions of handwritten signatures: to identify the signatory, and to indicate the signatory's intent with respect to the signed information. Any technology that can perform these two functions in electronic form should, according to the Model Law on Electronic Commerce, be regarded as satisfying a legal signature requirement. The Model Law is therefore technologically neutral; that is, it does not depend on or presuppose the use of any particular type of technology and could be applied to the communication and storage of all types of information. Technological neutrality is particularly important in view of speed of technological innovation and helps to ensure that legislation remains capable of accommodating future developments and does not become obsolete too quickly. Accordingly, the Model Law carefully avoids any reference to particular technical methods of transmission or storage of information.

86. This general principle has been incorporated into the laws of many countries. The principle of technological neutrality also allows for future technological developments to be accommodated. Furthermore, this approach gives prominence to the freedom of the parties to choose technology that is appropriate to their needs. The onus is then placed on the parties' ability to determine the level of security that is adequate for their communications. This may avoid excessive technological complexity and its associated costs.[86]

87. Except in Europe, where legislation has been primarily influenced by directives issued by the European Union,[87] most countries that have legislated in relation to electronic commerce have used the Model Law on Electronic Commerce as their

[86] S. Mason, "Electronic signatures in practice", *Journal of High Technology Law*, vol. VI, No. 2 (2006), p. 153.

[87] In particular, directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (*Official Journal of the European Communities*, L 13, 19 January 2000). The directive on electronic signatures was followed by a more general one, directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (*Official Journal of the European Communities*, L 178, 17 July 2000), dealing with various aspects of the provision of information technology services and some matters of electronic contracting.

template.[88] The Model Law has also served as a basis for the domestic harmonization of e-commerce legislation in countries organized on a federal basis, such as Canada[89] and the United States of America.[90] With very few exceptions,[91] countries enacting the Model Law have preserved its technologically neutral approach and have neither prescribed nor favoured the use of any particular technology. Both the UNCITRAL Model Law on Electronic Signatures (adopted in 2001) and the more recent United Nations Convention on the Use of Electronic Communications in International Contracts (adopted by the General Assembly by its resolution 60/21 of 23 November 2005

[88] As at January 2007, legislation implementing provisions of the UNCITRAL Model Law on Electronic Commerce had been adopted in at least the following countries: Australia, Electronic Transactions Act 1999; China, Electronic Signatures Law, promulgated in 2004; Colombia, *Ley de comercio electrónico*; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*; Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos (2002)*; France, *Loi 2000-230 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (2000)*; India, Information Technology Act, 2000; Ireland, Electronic Commerce Act, 2000; Jordan, Electronic Transactions Law, 2001; Mauritius, Electronic Transactions Act 2000; Mexico, *Decreto por el que se reforman y adicionan diversas disposiciones del código civil para el Distrito Federal en materia federal, del Código federal de procedimientos civiles, del Código de comercio y de la Ley federal de protección al consumidor (2000)*; New Zealand, Electronic Transactions Act 2002; Pakistan, Electronic Transactions Ordinance, 2002; Panama, *Ley de firma digital (2001)*; Philippines, Electronic Commerce Act (2000); Republic of Korea, Framework Act on Electronic Commerce (2001); Singapore, Electronic Transactions Act (1998); Slovenia, Electronic Commerce and Electronic Signature Act (2000); South Africa, Electronic Communications and Transactions Act (2002); Sri Lanka, Electronic Transactions Act (2006); Thailand, Electronic Transactions Act (2001); Venezuela (Bolivarian Republic of), *Ley sobre mensajes de datos y firmas electrónicas (2001)*; and Viet Nam, Law on Electronic Transactions (2006). The Model Law has also been adopted in the British Crown dependencies of the Bailiwick of Guernsey (Electronic Transactions (Guernsey) Law 2000), the Bailiwick of Jersey (Electronic Communications (Jersey) Law 2000) and the Isle of Man (Electronic Transactions Act 2000); in the overseas territories of the United Kingdom of Bermuda (Electronic Transactions Act 1999), the Cayman Islands (Electronic Transactions Law 2000) and the Turks and Caicos (Electronic Transactions Ordinance 2000); and in Hong Kong Special Administrative Region (SAR) of China (Electronic Transactions Ordinance (2000)). Unless otherwise indicated, references made hereafter to statutory provisions of any of these countries refer to provisions contained in the statutes listed above.

[89] The domestic enactment of the Model Law in Canada is the Uniform Electronic Commerce Act, adopted by the Uniform Law Conference of Canada in 1999 (available with official commentary at http://www.chlc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia, accessed on 6 June 2008). The Act has since been enacted in a number of provinces and territories of Canada, including Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward Island, Saskatchewan and Yukon. The Province of Quebec enacted specific legislation (Act to Establish a Legal Framework for Information Technology (2001)), which, although being broader in scope and drafted very differently, achieves many of the objectives of the Uniform Electronic Commerce Act and is generally consistent with the UNCITRAL Model Law on Electronic Commerce. Updated information on the enactment of the Uniform Electronic Commerce Act may be found at http://www.ulcc.ca (accessed on 5 June 2008).

[90] In the United States, the National Conference of Commissioners on Uniform State Law used the UNCITRAL Model Law on Electronic Commerce as a basis for preparing the Uniform Electronic Transactions Act, which it adopted in 1999 (the text of the Act and the official commentary is available at http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm, accessed on 6 June 2008). The Uniform Electronic Transactions Act has since been enacted in the District of Columbia and in the following 46 states: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, West Virginia, Wisconsin and Wyoming. Other states are likely to adopt implementing legislation in the near future, including Illinois, which had already enacted the UNCITRAL Model Law through the Electronic Commerce Security Act (1998). Updated information on the enactment of the Uniform Electronic Transactions Act may be found at http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp (accessed on 6 June 2008).

[91] Colombia, Dominican Republic, Ecuador, India, Mauritius, Panama and South Africa.

and opened for signature on 16 January 2006) follow the same approach, although the UNCITRAL Model Law on Electronic Signatures contains some additional language (see below, para. 95).

88. When legislation adopts the minimalist approach, the issue of whether electronic signature equivalence has been proved normally falls to a judge, arbitrator or public authority to determine, generally by means of the so-called "appropriate reliability test". Under this test, all types of electronic signature that satisfy the requirements are considered valid; hence, the test embodies the principle of technological neutrality.

89. A wide array of legal, technical and commercial factors may be taken into account in determining whether, under the circumstances, a particular authentication method offers an appropriate level of reliability, including: (*a*) the sophistication of the equipment used by each of the parties; (*b*) the nature of their trade activity; (*c*) the frequency with which commercial transactions take place between the parties; (*d*) the nature and size of the transaction; (*e*) the function of signature requirements in a given statutory and regulatory environment; (*f*) the capability of communication systems; (*g*) compliance with authentication procedures set forth by intermediaries; (*h*) the range of authentication procedures made available by any intermediary; (*i*) compliance with trade customs and practice; (*j*) the existence of insurance coverage mechanisms against unauthorized messages; (*k*) the importance and the value of the information contained in the data message; (*l*) the availability of alternative methods of identification and the cost of implementation; and (*m*) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and at the time when the data message was communicated.

2. *Technology-specific approach*

90. The concern to promote media neutrality raises other important issues. The impossibility of guaranteeing absolute security against fraud and transmission error is not limited to the world of electronic commerce and applies to the world of paper documents as well. When formulating rules for electronic commerce, legislators are often inclined to aim at the highest level of security offered by existing technology.[92] The practical need for applying stringent security measures to avoid unauthorized access to data, ensure the integrity of communications and protect computer and information systems cannot be questioned. However, from the perspective of private business

[92] One of the earliest examples was the Utah Digital Signature Act, which was adopted in 1995, but was repealed effective 1 May 2006 by State Bill 20, available at http://www.le.state.ut.us/~2006/htmdoc/sbillhtm/sb0020.htm (accessed on 6 June 2008). The technology bias of the Utah Act can also be observed in a number of countries where the law only recognizes digital signatures created within a PKI as a valid means of electronic authentication, which is the case, for example, under the laws of Argentina, Ley de firma digital (2001) and Decreto No. 2628/2002 (*Reglamentación de la Ley de firma digital*); Estonia, Digital Signatures Act (2000); Germany, Digital Signature Act, enacted as article 3 of the Information and Communication Services Act of 13 June 1997; India, Information Technology Act 2000; Israel, Electronic Signature Law (2001); Japan, Law concerning Electronic Signatures and Certification Services (2001); Lithuania, Law on Electronic Signatures (2000); Malaysia, Digital Signature Act 1997; Poland, Act on Electronic Signature (2001); and the Russian Federation, Law on Electronic Digital Signature (2002).

law, it may be more appropriate to graduate security requirements in steps similar to the degrees of legal security encountered in the paper world. In the paper world, business people are in most cases free to choose among a wide range of methods to achieve integrity and authenticity of communications (for example, the different levels of handwritten signature seen in documents of simple contracts and notarized acts). Under a technology-specific approach, regulations would mandate a specific technology to fulfil the legal requirements for the validity of an electronic signature. This is the case, for instance, where the law, aiming at a higher level of security, demands PKI-based applications. Since it prescribes the use of a specific technology, it is also called the "prescriptive" approach.

91. The disadvantages of the technology-specific approach are that, in favouring specific types of electronic signature, it "risks excluding other possibly superior technologies from entering and competing in the marketplace."[93] Rather than facilitating the growth of electronic commerce and the use of electronic authentication techniques, such an approach may have the opposite effect. Technology-specific legislation risks fixing requirements before a particular technology matures.[94] The legislation may then either prevent later positive developments in the technology or become quickly outdated as a result of later developments. A further point is that not all applications may require a security level comparable with that provided by certain specified techniques, such as digital signatures. It may also happen that speed and ease of communication or other considerations may be more important for the parties than ensuring the integrity of electronic information through any particular process. Requiring the use of an overly secure means of authentication could result in wasted costs and efforts, which may hinder the diffusion of electronic commerce.

92. Technology-specific legislation typically favours the use of digital signatures within a PKI. The way in which PKIs are structured, in turn, varies from country to country according to the level of government intervention. Here, too, three main models can be identified:

(*a*) *Self-regulation.* Under this model, the field of authentication is left wide open. While the government may establish one or more authentication schemes within its own departments and related organizations, the private sector is free to set up authentication schemes, commercial or otherwise, as it sees fit. There is no mandatory high-level authentication authority and authentication service providers are responsible for ensuring interoperability with other providers, domestically and internationally,

[93] Stewart Baker and Matthew Yeo, in collaboration with the secretariat of the International Telecommunication Union (ITU), "Background and issues concerning authentication and the ITU", briefing paper presented to the Experts Meeting on Electronic Signatures and Certification Authorities: Issues for Telecommunications, Geneva, 9 and 10 December 1999, document No. 2, available at http://www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html (accessed on 6 June 2008).

[94] However, in view of the fact that PKI technology is today fairly mature and established, some of these concerns may no longer apply with the same force.

depending on the objectives of establishing the authentication scheme. No licensing or technology approvals of authentication service providers are required (with the possible exception of consumer protection regulations);[95]

(*b*) *Limited government involvement.* The government might decide to establish a voluntary or mandatory high-level authentication authority. In this case, authentication service providers may find it necessary to interoperate with the high-level authentication authority to have their tokens of authentication (or other authenticators) accepted outside their own systems. In this case, the technical and management specifications of the authentication service providers must be published as quickly as possible so that both government departments and the private sector may plan accordingly. Licensing and technology approvals for each authentication service provider could be required;[96]

(*c*) *Government-led process.* The government may decide to establish an exclusive central authentication service provider. Special-purpose authentication service providers may also be established with government approval.[97] Identity management systems (see paras. 67-77 above) represent another way in which governments may indirectly lead the process of digital signature. Some governments have already launched programmes for issuing to their citizens machine-readable identity documents ("electronic identifications") equipped with digital signature functionalities.

3. *Two-tiered or two-pronged approach*

93. In this approach, the legislation sets a low threshold of requirements for electronic authentication methods to receive a certain minimum legal status and assigns greater legal effect to certain electronic authentication methods (referred to variously as secure, advanced or enhanced electronic signatures, or qualified certificates).[98] At the basic level, legislation adopting a two-tiered system generally grants electronic signatures functional-equivalence status with handwritten signatures, based on technologically neutral criteria. Higher-level signatures, to which certain rebuttable presumptions apply, are necessary to comply with specific requirements that may relate to a particular technology. Currently, legislation of this type usually defines such secure signatures in terms of PKI technology.

[95] Asia-Pacific Economic Cooperation, *Assessment Report on Paperless Trading of APEC Economies* (Beijing, APEC secretariat, 2005), pp. 63 and 64, where the United States is cited as an example of the application of this model.

[96] See Asia-Pacific Economic Cooperation, *Assessment Report* ... , where Singapore is cited as an example.

[97] See Asia-Pacific Economic Cooperation, *Assessment Report* ... , where China and Malaysia are cited as examples.

[98] Aalberts and van der Hof, *Digital Signature Blindness* … , para. 3.2.2.

94. This approach is typically chosen in jurisdictions that consider it important to address certain technological requirements in their legislation, but wish, at the same time, to leave room for technological developments. It can provide a balance between flexibility and certainty in relation to electronic signatures, by leaving it to the parties to decide, as a commercial judgement, whether the cost and inconvenience of using a more secure method is suitable to their needs. These texts also provide guidance as to the criteria for the recognition of electronic signatures in the context of a certification authority model. It is generally possible to combine the two-tiered approach with any type of certification model (whether self-regulated, voluntary accreditation or a government-led scheme), in much the same way as might be done under the technology-specific approach (see above, paras. 90-92). Thus, while some rules may be flexible enough to accommodate different electronic signature certification models, some systems would only recognize licensed certification services providers as possible issuers of secure or qualified certificates.

95. The first jurisdictions to have passed legislation adopting the two-tiered approach include Singapore[99] and the European Union.[100] They were followed by a number of others.[101] The UNCITRAL Model Law on Electronic Signatures allows an enacting State to set up a two-tiered system through regulations, even though it does not actively promote it.[102]

[99] Section 8 of the Electronic Transactions Act of Singapore admits any form of electronic signature, but only secure electronic signatures that meet the requirements of section 17 of the Act (i.e. those which are "(*a*) unique to the person using it; (*b*) capable of identifying such person; (*c*) created in a manner or using a means under the sole control of the person using it; and (*d*) linked to the electronic record to which it relates in a manner that if the record was changed the electronic signature would be invalidated") enjoy the presumptions listed in section 18 (inter alia, that the signature "is of the person to whom it correlates" and that the signature "was affixed by that person with the intention of signing or approving the electronic record"). Digital signatures supported by a trustworthy certificate that complies with the provisions of section 20 of the Act are automatically considered to be "secure electronic signatures" for the purposes of the Act.

[100] Like the Electronic Transactions Act of Singapore, the European Union directive on electronic signatures (*Official Journal of the European Communities*, L 13/12, 19 January 2000) distinguishes between an "electronic signature" (defined in art. 2, para. 1, as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication") and an "advanced electronic signature" (defined in art. 2, para. 2, as an electronic signature that meets the following requirements: "(*a*) it is uniquely linked to the signatory; (*b*) it is capable of identifying the signatory; (*c*) it is created using means that the signatory can maintain under his sole control; and (*d*) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable"). The directive, in article 5, paragraph 2, mandates the States members of the European Union to ensure that an electronic signature "is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds" that it is "in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device". However only advanced electronic signatures "which are based on a qualified certificate and which are created by a secure-signature-creation device" are declared to "(*a*) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (*b*) are admissible as evidence in legal proceedings". (see art. 5, para. 1, of the directive).

[101] For example, Mauritius and Pakistan. For details of the respective statutes, see note 88 above.

[102] The UNCITRAL Model Law on Electronic Signatures, in its article 6, paragraph 3, provides that an electronic signature is considered to be reliable if (*a*) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person; (*b*) they were, at the time of signing, under the control of the signatory and of no other person; (*c*) any alteration to the electronic signature, made after the time of signing, is detectable; and (*d*) any alteration made to that information after the time of signing is detectable where the legal requirement for a signature is intended to provide assurance as to the integrity of the information.

96. Regarding the second tier, it was proposed that countries should not require the use of second-tier signatures for form requirements relating to international commercial transactions and that secure electronic signatures should be limited to areas of the law that do not have a significant impact on international trade (e.g. trusts, family law, real property transactions).[103] Moreover, it was suggested that two-tiered laws should explicitly give effect to contractual agreements concerning the use and recognition of electronic signatures, so as to ensure that global contract-based authentication models do not run afoul of national legal requirements.

B. Evidentiary value of electronic signature and authentication methods

97. One of the main objectives of the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures was to pre-empt disharmony and possible over-regulation by offering general criteria to establish the functional equivalence between electronic and paper-based signature and authentication methods. Although the UNCITRAL Model Law on Electronic Commerce has found widespread acceptance, and an increasing number of States have used it as a basis for their e-commerce legislation, it cannot yet be assumed that the principles of the Model Law have achieved universal application. The attitude taken by various jurisdictions in relation to electronic signatures and authentication typically reflects the general approach of the jurisdiction to writing requirements and the evidentiary value of electronic records.

1. "Authentication" and general attribution of electronic records

98. The use of electronic methods of authentication involves two aspects that are relevant for the present discussion. The first aspect relates to the general issue of attribution of a message to its purported originator. The second relates to the appropriateness of the identification method used by the parties for the purpose of meeting specific form requirements, in particular legal signature requirements. Also relevant are legal notions that imply the existence of a handwritten signature, such as is the case for the notion of a "document" in some legal systems. Even though these two aspects may often be combined or, depending on the circumstances, may not be entirely distinguishable one from another, an attempt to analyse them separately may be useful, as it appears that courts tend to reach different conclusions according to the function being attached to the authentication method.

[103] Baker and Yeo, "Background and issues concerning authentication …".

99. The Model Law on Electronic Commerce deals with attribution of data messages in its article 13. That provision has its origin in article 5 of the UNCITRAL Model Law on International Credit Transfers,[104] which defines the obligations of the sender of a payment order. Article 13 of the Model Law on Electronic Commerce is intended to apply where there is a question as to whether an electronic communication was really sent by the person who is indicated as being the originator. In the case of a paper-based communication, the problem would arise as the result of an alleged forged signature of the purported originator. In an electronic environment, an unauthorized person may have sent the message, but the authentication by code, encryption or similar means would be accurate. The purpose of article 13 is not to attribute authorship of a data message or to establish the identity of the parties. Rather, it deals with the attribution of data messages, by establishing the conditions under which a party may rely on the assumption that a data message was actually from the purported originator.

100. Article 13, paragraph 1, of the Model Law on Electronic Commerce recalls the principle that an originator is bound by a data message if it has effectively sent that message. Paragraph 2 refers to a situation where the message was sent by a person other than the originator who had the authority to act on behalf of the originator. Paragraph 3 deals with two kinds of situation in which the addressee could rely on a data message as being that of the originator: first, situations in which the addressee properly applied an authentication procedure previously agreed to by the originator; and second, situations in which the data message resulted from the actions of a person who, by virtue of his or her relationship with the originator, had access to the originator's authentication procedures.

101. A number of countries have adopted the rule in article 13 of the Model Law on Electronic Commerce, including the presumption of attribution established in paragraph 3 of that article.[105] Some countries expressly refer to the use of codes, passwords or other means of identification as factors that create a presumption of authorship.[106] There are also more general versions of article 13, in which the presumption created by proper verification through a previously agreed procedure is rephrased as an indication of elements that may be used for attribution purposes.[107]

[104] United Nations publication, Sales No. E.99.V.11, available at http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf (accessed on 6 June 2008).

[105] Colombia (art. 17); Ecuador (art. 10); Jordan (art. 15); Mauritius (sect. 12, subsect. 2); Philippines (sect. 18, para. 3); Republic of Korea (art. 7, para. 2); Singapore (sect. 13, subsect. 3); Thailand (sect. 16); and Venezuela (Bolivarian Republic of) (art. 9). The same rules are also contained in the laws of the British Crown dependency of Jersey (art. 8) and the British overseas territories of Bermuda (sect. 16, para. 2) and Turks and Caicos (sect. 14). For details of the respective statutes, see note 88 above.

[106] Mexico (see note 88 above), art. 90, para. I.

[107] For example, the Uniform Electronic Transactions Act of the United States (see note 90) provides in section 9, subsection (*a*), that an electronic record or electronic signature "is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable." Section 9, subsection (*b*), provides further that the effect of an electronic record or electronic signature attributed to a person under subsection (*a*) "is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law".

102. However, other countries have adopted only the general rules in article 13, namely that a data message is that of the originator if it was sent by the originator him or herself, or by a person acting on the originator's behalf, or by a system programmed by or on behalf of the originator to operate automatically.[108] In addition, several countries that have implemented the Model Law on Electronic Commerce have not included any specific provision based on article 13.[109] The assumption in those countries was that no specific rules were needed and that attribution was better left to ordinary methods of proof, in the same way as attribution of documents on paper: "The person who wishes to rely on any signature takes the risk that the signature is invalid, and this rule does not change for an electronic signature."[110]

103. Other countries, however, have preferred to take the provisions of the Model Law on Electronic Commerce on attribution separately from provisions on electronic signatures. This approach is based on the understanding that attribution in a documentary context serves the primary purpose of providing a basis for reasonable reliance, and may include broader means than those more narrowly used for identifying individuals. Some laws, such as the United States Uniform Electronic Transactions Act, emphasize this principle by stating, for example, that "an electronic record or electronic signature is attributable to a person if it was the act of the person", which "may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable."[111] Such a general rule on attribution does not affect the use of a signature as a device for attributing a record to a person, but is based on the recognition that "a signature is not the only method for attribution."[112] According to the commentary on the United States Act, therefore:

[108] Australia (sect. 15, para. 1); essentially in the same manner, India (sect. 11); Pakistan (sect. 13, subsect. 2); and Slovenia (art. 5). See also Hong Kong SAR of China (sect. 18) and the British Crown dependency of the Isle of Man (sect. 2). For details of the respective statutes, see note 88 above.

[109] For example, Canada, France, Ireland, New Zealand and South Africa.

[110] Canada, Uniform Electronic Commerce Act (with official commentary) (see note 89), commentary to section 10.

[111] United States, Uniform Electronic Transactions Act (1999) (see note 90), section 9. Paragraph 1 of the official comments to section 9 offer the following examples where both the electronic record and electronic signature would be attributable to a person: a person "types his/her name as part of an e-mail purchase order"; a "person's employee, pursuant to authority, types the person's name as part of an e-mail purchase order"; or a "person's computer, programmed to order goods upon receipt of inventory information within particular parameters, issues a purchase order which includes the person's name, or other identifying information, as part of the order".

[112] Paragraph 3 of the official comments to section 9 states: "The use of facsimile transmissions provides a number of examples of attribution using information other than a signature. A facsimile may be attributed to a person because of the information printed across the top of the page that indicates the machine from which it was sent. Similarly, the transmission may contain a letterhead that identifies the sender. Some cases have held that the letterhead actually constituted a signature because it was a symbol adopted by the sender with intent to authenticate the facsimile. However, the signature determination resulted from the necessary finding of intention in that case. Other cases have found facsimile letterheads NOT to be signatures because the requisite intention was not present. The critical point is that with or without a signature, information within the electronic record may well suffice to provide the facts resulting in attribution of an electronic record to a particular party.".

> "4. Certain information may be present in an electronic environment that does not appear to attribute but which clearly links a person to a particular record. Numerical codes, personal identification numbers, public and private key combinations all serve to establish the party to whom an electronic record should be attributed. Of course security procedures will be another piece of evidence available to establish attribution.
>
> "The inclusion of a specific reference to security procedures as a means of proving attribution is salutary because of the unique importance of security procedures in the electronic environment. In certain processes, a technical and technological security procedure may be the best way to convince a trier of fact that a particular electronic record or signature was that of a particular person. In certain circumstances, the use of a security procedure to establish that the record and related signature came from the person's business might be necessary to overcome a claim that a hacker intervened. The reference to security procedures is not intended to suggest that other forms of proof of attribution should be accorded less persuasive effect. It is also important to recall that the particular strength of a given procedure does not affect the procedure's status as a security procedure, but only affects the weight to be accorded the evidence of the security procedure as tending to establish attribution."[113]

104. It is also important to bear in mind that a presumption of attribution would not of itself displace the application of rules of law on signatures, where a signature is needed for the validity or proof of an act. Once it is established that a record or signature is attributable to a particular party, "the effect of a record or signature must be determined in light of the context and surrounding circumstances, including the parties' agreement, if any" and of "other legal requirements considered in light of the context".[114]

105. Against the background of this flexible understanding of attribution, the courts in the United States seem to have taken a liberal approach to the admissibility of electronic records, including e-mail message, as evidence in civil proceedings.[115] Courts in the United States have dismissed arguments that e-mail messages were inadmissible as evidence because they were unauthenticated and parol evidence.[116] The courts have found instead that e-mail messages obtained from the plaintiff during the discovery process were self-authenticating, since "the production of documents during discovery

[113] Official comments on section 9.

[114] Paragraph 6 of the official comments on section 9.

[115] *Commonwealth Aluminum Corporation v. Stanley Metal Associates*, United States District Court for the Western District of Kentucky, 9 August 2001, Federal Supplement, 2nd series, vol. 186, p. 770; and *Central Illinois Light Company (CILCO) v. Consolidation Coal Company (Consol)*, United States District Court for the Central District of Illinois, 30 December 2002, Federal Supplement, 2nd series, vol. 235, p. 916.

[116] *Sea-Land Service, Inc. v. Lozen International, LLC*, United States Court of Appeals for the Ninth Circuit, 3 April 2002, Federal Reporter, 3rd series, vol. 285, p. 808.

from the parties' own files is sufficient to justify a finding of self-authentication".[117] The courts tend to take into account all available evidence and do not reject electronic records as being prima facie inadmissible.

106. In countries that have not adopted the Model Law on Electronic Commerce, there seem to be no specific legislative provisions dealing with attribution in an analogous fashion. In those countries, attribution is typically a function of the legal recognition of electronic signatures and the presumptions attached to records authenticated with particular types of electronic signature. Concerns about the risk of manipulation in electronic records have, for instance, led courts in some of those countries to dismiss the value of e-mail messages as evidence in court proceedings, on the grounds that e-mail messages do not offer adequate guarantees of integrity.[118] Further examples of a more restrictive approach to the evidentiary value of electronic records and attribution can be found in recent cases involving Internet auctions, in which courts have applied a high standard for attribution of data messages. Those cases have typically involved suits for breach of contract on the grounds of lack of payment for goods allegedly purchased in Internet auctions. Claimants maintained that the defendant was the buyer, as the highest bid for the goods had been authenticated with the defendant's password and had been sent from the defendant's e-mail address. The courts have found that those elements were not sufficient to firmly conclude that it was in fact the defendant who had participated in the auction and submitted the winning bid for the goods. The courts have used various arguments to justify that position. For example, passwords were not reliable because anyone who knew the defendant's password could have used its e-mail address from anywhere and participated in the auction using the defendant's name,[119] a risk that some courts estimated as very high, on the basis of expert evidence regarding security threats to Internet communications networks, in particular through the use of Trojan Horses capable of "stealing" a person's password.[120] The risk of unauthorized use of a person's identification device (password) should be borne by the party that offered goods or services through a particular medium, as there was no legal presumption that messages sent through an Internet website with recourse to a person's access password to such website were attributable

[117] *Superhighway Consulting, Inc. v. Techwave, Inc.*, United States District Court for the Northern District of Illinois, Eastern Division, 16 November 1999, U.S. Dist. LEXIS 17910.

[118] Germany, Amtsgericht (District Court) Bonn, Case No. 3 C 193/01, 25 October 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 332/2002, available at http://www.jurpc.de/rechtspr/20020332.htm (accessed on 6 June 2008).

[119] Germany, Amtsgericht (District Court) Erfurt, Case No. 28 C 2354/01, 14 September 2001, JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht, JurPC Web-Dok. No. 71/2002, available at http://www.jurpc.de/rechtspr/20020071.htm (accessed on 6 June 2008); see also Landesgericht (Land Court) Bonn, Case No. 2 O 472/03, 19 December 2003, JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht, JurPC Web-Dok. No. 74/2004, available at http://www.jurpc.de/rechtspr/20040074.htm (accessed on 6 June 2008).

[120] Germany, Landesgericht (Land Court) Konstanz, Case No. 2 O 141/01 A, 19 April 2002, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 291/2002, available at http://www.jurpc.de/rechtspr/20020291.htm (accessed on 6 June 2008).

to that person.[121] Such a presumption might conceivably be attached to an "advanced electronic signature" as defined in law, but the holder of a simple password should not bear the risk of it being misused by unauthorized persons.[122]

2. *Ability to meet legal signature requirements*

107. In some countries, the courts have been inclined to interpret signature requirements liberally. As previously indicated (see introduction, paras. 2-4), this has been typically the case in some common law jurisdictions in connection with statute of frauds requirements that certain transactions must be in writing and bear a signature in order to be valid. Courts in the United States have also been receptive to legislative recognition of electronic signatures, admitting their use in situations not expressly contemplated in the enabling statute, such as the issue of judicial warrants.[123] More importantly for a contractual context, the courts have also assessed the adequacy of the authentication in the light of the dealings between the parties, rather than using a strict standard for all situations. Thus, where the parties had regularly used e-mail in their negotiations, the courts have found that the originator's typed name in an e-mail message satisfied statutory signature requirements.[124] A person's deliberate choice to type his name at the conclusion of all e-mails messages has been considered to be valid authentication.[125] The readiness of the United States courts to accept that e-mail messages and names typed therein are capable of satisfying writing requirements[126] follows a liberal interpretation of the notion of "signature", which is understood as encompassing "any symbol executed or adopted by a party with present intention to authenticate a writing" so that, in some instances, "a typed name or letterhead on a document is sufficient to satisfy the signature requirement".[127] Where the parties do not deny having written or received communications by e-mail, statutory signature requirements would be met, since courts have "long recognized that a binding

[121] Germany, Landesgericht (Land Court) Bonn, Case No. 2 O 450/00, 7 August 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 136/2002, available at http://www.jurpc.de/rechtspr/20020136.htm (accessed on 6 June 2008).

[122] Germany, Oberlandesgericht (Court of Appeal) Köln, Case No. 19 U 16/02, 6 September 2002, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 364/2002, available at http://www.jurpc.de/rechtspr/20020364.htm (accessed on 6 June 2008).

[123] *Department of Agriculture and Consumer Services v. Haire*, Fourth District Court of Appeal of Florida, Case Nos. 4D02-2584 and 4D02-3315, 15 January 2003.

[124] *Cloud Corporation v. Hasbro, Inc.*, United States Court of Appeals for the Seventh Circuit, 26 December 2002, Federal Reporter, 3rd series, vol. 314, p. 296.

[125] *Jonathan P. Shattuck v. David K. Klotzbach*, Superior Court of Massachusetts, 11 December 2001, 2001 Mass. Super. LEXIS 642.

[126] *Central Illinois Light Company v. Consolidation Coal Company*, United States District Court for the Central District of Illinois, Peoria Division, 30 December 2002, Federal Supplement, 2nd Series, vol. 235, p. 916.

[127] Ibid., p. 919: "Internal documents, invoices and e-mails can be used to satisfy the Illinois [Uniform Commercial Code] statute of frauds." In the concrete case, however, the court found that the alleged contract failed to satisfy the statute of frauds, not because the e-mail messages as such could not validly record the terms of a contract, but because there was no indication that the authors of the e-mail messages and the persons mentioned therein were employees of the defendant.

signature may take the form of any mark or designation thought proper by the party to be bound", provided that the author "intends to bind himself".[128]

108. Courts in the United Kingdom of Great Britain and Northern Ireland have taken a similar approach, generally considering the form of a signature to be less relevant than the function it serves. Thus, courts would consider the fitness of the medium both to attribute a record to a particular person and to indicate the person's intention with respect to the record. E-mail messages may therefore constitute "documents", and names typed in e-mail messages may be "signatures".[129] Some courts have declared that they "have no doubt that if a party creates and sends an electronically created document then he will be treated as having signed it to the same extent that he would in law be treated as having signed a hard copy of the same document" and that "the fact that the document is created electronically as opposed to as a hard copy can make no difference."[130] On occasion, courts have rejected arguments that e-mails constituted signed contracts for the purposes of the statute of frauds, mainly because the intent to be bound by the signature was lacking. There seems to be no precedent, however, where courts would have denied a priori the ability of e-mails and names typed therein to meet statutory writing and signature requirements. In some cases, it was found that the requirements of the statute of frauds were not met because the e-mails in question only reflected ongoing negotiations and not a final agreement, for instance because during the negotiations one of the parties had contemplated that a binding contract would be entered into once a "deal memo" had been signed, and not before.[131] In other cases courts have suggested that they might have been inclined to admit as a signature the originator's "name or initials" at "the end of the e-mail" or "anywhere else in the body of the e-mail", but held that the "automatic insertion of a person's e-mail address after the document has been transmitted by either the sending and/or receiving [Internet service provider]" was not "intended for a signature".[132] Although British courts seem to interpret the writing requirements of the statute of frauds more strictly than their United States counterparts, they are generally inclined to admit the use of any type of electronic signature or authentication method, even outside any specific statutory authorization, as long as the method in question serves the same functions as a handwritten signature.[133]

[128] *Roger Edwards, LLC v. Fiddes & Son, Ltd.*, United States District Court for the District of Maine, 14 February 2003, Federal Supplement, 2nd Series, vol. 245, p. 251.

[129] *Hall v. Cognos Limited* (Hull Industrial Tribunal, Case No. 1803325/97) (unreported).

[130] *Mehta v. J. Pereira Fernandes S.A.* [2006] EWHC 813 (Ch), (United Kingdom, England and Wales High Court, Chancery Division), [2006] 2 Lloyd's Rep 244 (United Kingdom, England and Wales, Lloyd's List Law Reports).

[131] *Pretty Pictures Sarl v. Quixote Films Ltd.*, 30 January 2003 ([2003] EWHC 311 (QB), (United Kingdom, England and Wales High Court, Law Reports Queen's Bench, [2003] All ER (D) 303 (January)) (United Kingdom, All England Direct Law Reports (Digests)).

[132] *Mehta v. J. Pereira Fernandes S.A.* ... .

[133] *Mehta v. J. Pereira Fernandes S.A.* ... , No. 25: "It is noteworthy that the Law Commission's view in relation to [the European Union directive on electronic commerce (2000/31/EC)] is that no significant changes are necessary in relation to statutes that require signatures because whether those requirements have been satisfied can be tested in a functional way by asking whether the conduct of the would-be signatory indicates an authenticating intention to a reasonable person. … Thus, as I have already said, if a party or a party's agent sending an e-mail types his or her or his or her principal's name to the extent required or permitted by existing case law in the body of an e-mail, then in my view that would be a sufficient signature for the purposes of [the statute of frauds]."

109. Courts in civil law jurisdictions tend generally to follow a more restrictive approach, arguably because for many of those countries the notion of "document" ordinarily implies the use of some form of authentication, thus becoming hardly dissociable from a "signature". Courts in France, for instance, had been reluctant to accept electronic means of identification as equivalent to handwritten signatures until the adoption of legislation expressly recognizing the validity of electronic signatures.[134] A slightly more liberal line is taken by decisions that accept the electronic filing of administrative complaints for the purpose of meeting a statutory deadline, at least as long as they are subsequently confirmed by regular correspondence.[135]

110. In contrast to their restrictive approach to the attribution of data messages in the formation of contracts, German courts seem to have been liberal in the acceptance of identification methods as equivalent to handwritten signatures in court proceedings. The debate in Germany has evolved around the increasing use of scanned images of a legal counsel's signature to authenticate computer facsimiles containing statements of appeals transmitted directly from a computer station via modem to a court's facsimile machine. In earlier cases, courts of appeal[136] and the Federal Court of Justice[137] had held that a scanned image of a handwritten signature did not satisfy existing signature requirements and offered no proof of a person's identity. Identification might conceivably be attached to an "advanced electronic signature", as defined in German law. Generally, however, it was for the legislator and not the courts to establish the conditions for the equivalence between writings and intangible communications transmitted by data transfers.[138] That understanding was eventually reversed in view of the unanimous opinion of the other high federal courts that accepted the delivery of certain procedural pleas by means of electronic communication of a data message accompanied by a scanned image of a signature.[139]

[134] The Court of Cassation of France rejected the receivability of a statement of appeal signed electronically, because there were doubts as to the identity of the person who created the signature and the appeal had been signed electronically before entry into force of the law of 13 March 2000, which recognized the legal effect of electronic signatures (Cour de cassation, Deuxième chambre civile, 30 April 2003, *Sté Chalets Boisson c/ M. X.*, available at http://www.juriscom.net/jpt/visu.php?ID=239 (accessed on 6 June 2008)).

[135] France, Conseil d'État, 28 December 2001, No. 235784, *Élections municipales d'Entre-Deux-Monts* (original available with the Secretariat).

[136] For instance, Oberlandesgericht (Court of Appeal) Karlsruhe, Case No. 14 U 202/96, 14 November 1997, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 09/1998, available at http://www.jurpc.de/rechtspr/19980009.htm (accessed on 6 June 2008).

[137] Germany, Bundesgerichtshof (Federal Court of Justice), Case No. XI ZR 367/97, 29 September 1998, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 05/1999, available at http://www.jurpc.de/rechtspr/19990005.htm (accessed on 6 June 2008).

[138] Ibid.

[139] In a decision on a case referred to it by the Federal Court of Justice of Germany, the Joint Chamber of the Highest Federal Courts of Germany noted that form requirements in court proceedings were not an end in themselves. Their purpose was to ensure a sufficiently reliable determination of the content of the writing and the identity of the person from whom it emanated. The Joint Chamber noted the evolution in the practical application of form requirements to accommodate earlier technological developments such as telex or facsimile. The Joint Chamber held that accepting the delivery of certain procedural pleas by means of electronic communication of a data message with a scanned image of a signature would be in line with the spirit of existing case law (Gemeinsamer Senat der obersten Gerichtshöfe des Bundes, GmS-OGB 1/98, 5 April 2000, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 160/2000, available at http://www.jurpc.de/rechtspr/20000160.htm (accessed on 6 June 2008)).

111. It is interesting to note that even courts in some civil law jurisdictions that have adopted legislation favouring the use of PKI-based digital signatures, such as Colombia,[140] have taken a similarly liberal approach and confirmed, for example, the admissibility of judicial proceedings conducted entirely by electronic communications. The submissions exchanged during such proceedings were valid, even if they were not signed with a digital signature, since the electronic communications used methods that allowed for the identification of the parties.[141]

112. Case law on electronic signatures is still rare and the small number of court decisions to date does not provide a sufficient basis to draw firm conclusions. Nevertheless, a brief review of existing precedents reveals several trends. It seems that the legislative approach taken to electronic signatures and authentication has influenced the attitude of courts on this issue. Arguably, the legislative focus on electronic "signatures", without an accompanying general rule on attribution, has led to excessive attention being paid to the identity function of authentication methods. This has, in some countries, engendered a certain degree of mistrust vis-à-vis any authentication methods that do not satisfy the statutory definition of an electronic "signature". It is therefore doubtful that the same courts that have adopted a liberal approach in the context of judicial or administrative appeals would be equally liberal in respect of signature requirements for the validity of contracts. Indeed, while in a contractual context a party might be faced with the risk of repudiation of the agreement by the other party, in the context of civil proceedings it is typically the party using electronic signatures or records that is interested in confirming its approval of the record and its contents.

3. Efforts to develop electronic equivalents for special forms of signature

(a) International applications: electronic apostilles

113. A special commission met in The Hague from 28 October to 4 November 2003 to review the practical operation of the Convention Abolishing the Requirement of Legalisation for Foreign Public Documents (the Hague Apostille Convention), the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters[142] (the Hague Evidence Convention) and the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (the Hague Service

[140] For example, Colombia, which has adopted the UNCITRAL Model Law on Electronic Commerce, including the general provisions of its article 7, but has established a legal presumption of authenticity only in respect of digital signatures (*Ley de comercio electrónico*, art. 28).

[141] Colombia, Juzgado Segundo Promiscuo Municipal Rovira Tolima, *Juan Carlos Samper v. Jaime Tapias*, 21 July 2003, Rad. 73-624-40-89-002-2003-053-00. The Court found that the process undertaken via electronic means was valid notwithstanding that the e-mail messages were not digitally signed because (*a*) the sender of the data messages could be fully identified; (*b*) the sender of the data messages consented to and affirmed the content of the data messages sent; (*c*) the data messages were safely kept in the Tribunal; and (*d*) the messages could be reviewed at any time (available at http://www.camara-e.net/_upload/80403--0-7-diaz082003.pdf, accessed on 6 June 2008).

[142] United Nations, *Treaty Series*, vol. 658, No. 9432.

Convention).[143] The meeting of the Special Commission on the Practical Operation of the Hague Apostille, Evidence and Service Conventions was attended by 116 delegates representing 57 Member States, States parties to one or more of the conventions under review and observers. The Special Commission emphasized that the three conventions operated in an environment that was subject to important technical developments. Although this evolution could not be foreseen at the time of adoption of the three conventions, the Special Commission underlined that modern technologies were an integral part of modern-day society and their usage a matter of fact.[144] In this respect, the Special Commission noted that the spirit and letter of the conventions did not constitute an obstacle to the usage of modern technology and that their application and operation could be further improved by relying on such technologies.[145] The Special Commission recommended that States parties to the conventions and the Permanent Bureau of the Hague Conference on Private International Law should work towards the development of techniques for the generation of electronic apostilles "taking into account inter alia the UNCITRAL model laws on electronic commerce and on electronic signatures, both being based on the principles of non-discrimination and functional equivalence."[146] In April 2006, the Permanent Bureau of the Hague Conference on Private International Law and the National Notary Association (NNA) of the United States launched the electronic Apostille Pilot Program (e-APP). Under the programme, the Hague Conference and NNA are, together with any interested State, developing, promoting and assisting in the implementation of software models for (*a*) the issuance and use of electronic apostilles (e-apostilles), and (*b*) the operation of electronic registers of apostilles (e-registers).[147] The programme contemplates two distinct but ultimately identical formats for e-apostilles. Both methods protect the underlying document and the e-apostille certificate from unauthorized modifications, but each one presents a different interface to the recipient.

114. Under the first method, a competent authority can add the apostille certificate as the final page to an existing underlying public document in a given format (e-APP contemplates documents being exchanged in the Portable Document Format (PDF)). The recipient would open the file and find the e-apostille certificate included as the last page of the document. If this format is chosen, the underlying public document and the e-apostille certificate form one continuous document or, put another way, one single electronic file. One could still choose to print one or more pages of this single file, so that the e-apostille certificate could be printed by itself.[148]

[143] Ibid., vol. 847, No. 12140.

[144] Hague conference on Private International Law "Conclusions and recommendations adopted by the Special Commission on the Practical Operation of the Hague Apostille, Evidence and Service Conventions: 28 October to 4 November 2003", para.4 (available at http://hcch.e-vision.nl/upload/wop/lse_concl_e.pdf, accessed on 6 June 2008).

[145] Hague conference on Private International Law "Conclusions and recommendations adopted by the Special Commission ...".

[146] Hague conference on Private International Law "Conclusions and recommendations adopted by the Special Commission ...", para. 24.

[147] Christophe Bernasconi and Rich Hansberger, "Electronic Apostille Pilot Program (e-APP): memorandum on some of the technical aspects underlying the suggested model for the issuance of electronic apostilles (e-apostilles)" available at http://www.hcch.net/upload/wop/genaff_pd18e2007.pdf (accessed on 26 May 2008).

[148] "Electronic Apostille Pilot Program ...", para. 18.

115. Under the second method, the underlying public document is attached as a separate file to the e-apostille certificate. The recipient still receives a single PDF file but, upon opening the file, the user first views the e-apostille certificate and can then open the attached underlying public document to view it as a separate PDF file. It has been suggested that this method provides a more intuitive interface for the recipient of the apostillized document (for example, it has been adopted by the United States Department of State for its electronic patent filings and as the model for e-apostilles). By attaching the underlying public document as a file to the e-apostille certificate, the intent is to make it very clear to the recipient when he or she first opens the document that he or she is dealing with an apostille. From there, he or she can then open the underlying public document to view its contents."[149]

116. Under either model, the operation of e-apostilles involves the issuance of certificates in electronic form digitally signed by the appropriate competent authority for the purposes of the Hague Apostille Convention. Each competent authority would further keep a register in electronic form allowing for verification of certificates issued to support e-apostilles.[150]

117. In countries that have abolished legalization or apostille requirements, it is conceivable to develop systems whereby foreign notarized records would be given legal recognition on the basis of verification of the electronic signature or authentication method used by the originating notary public. The electronic signature of the originating notary must be verifiable by the user of the document (generally another notary) in a simple and quick manner. This can be done via the Internet by accessing the site of the originating notary's certification services provider, which, at least in Europe, is typically the national chamber to which the notary belongs. A related matter concerns the verification of the originating notary's authority to authenticate records under the legal system in which he or she operates. In order to facilitate that process and obviate the need for consulting a foreign supervisory body, if any, entrusted with licensing notaries, it has been proposed that certification services providers established under the auspices of chambers of notaries should only issue certificates to notaries currently authorized to exercise the function of notary public so that any suspension or revocation of a notary's authority should automatically prevent verification of the notary's signature.[151]

[149] "Electronic Apostille Pilot Program ...", para. 19.

[150] For more information on the operation of e-apostilles, see the e-APP website at http://www.e-app.info/ (accessed on 6 June 2008).

[151] Ugo Bechini and Bernard Reynis, "La signature électronique transfrontalière des notaires: une réalit européenne", *La semaine juridique (édition notariale et immobilière)*, No. 39, 24 September 2004, p. 1447.

(b) Domestic applications: seals, notarization and attestation

118. Some jurisdictions have already abolished the requirement for seals on the ground that sealing is no longer relevant in today's context. An attested (i.e. witnessed) signature has been substituted in its place.[152] Other jurisdictions have legislation that allows secure electronic signatures to satisfy the requirement for sealing. For instance, Ireland has specific provisions for secure electronic signatures, with appropriate certification, to be used in place of a seal, subject to the consent of the person or public body to which the document under seal is required or permitted to be given.[153] Canada provides that requirements for a person's seal under certain federal laws are satisfied by a secure electronic signature that identifies the secure electronic signature as the person's seal.[154]

119. A number of countries have launched initiatives that contemplate the use of electronic documents and signatures in land transactions involving deeds. The model used in Victoria, Australia, envisages the use of secure digital signature technology via the Internet with digital cards issued by a certification authority. In the United Kingdom, the model envisages execution of deeds by solicitors on behalf of their clients via an intranet. In some legislation, the possibility of using "electronic seals" as an alternative to manual seals is recognized officially, while the technical details of the form of the electronic seal are left to be separately determined.[155]

120. The United States Uniform Real Property Electronic Recording Act[156] expressly states that a physical or electronic image of a stamp, impression or seal need not accompany an electronic signature. Essentially, it is only the information on the seal, rather than the seal itself, that is required. It also provides that any statute, regulation or standard that requires a personal or corporate stamp, impression or seal is satisfied by an electronic signature. These physical indicia are inapplicable to a fully electronic document. Nevertheless, this act requires that the information that would otherwise

[152] For example, United Kingdom, Law of Property (Miscellaneous Provisions) Act 1989, which implemented the Law Reform Commission Report on "Deeds and escrows" (Law Com. No. 143, 1987).

[153] Ireland, Electronic Commerce Act, section 16. However, where the document to be under seal is required or permitted to be given to a public body or to a person acting on behalf of a public body, the public body that consents to the use of an electronic signature may nevertheless require that it be in accordance with particular information technology and procedural requirements.

[154] Canada, Personal Information Protection and Electronic Documents Act (2000), part 2, section 39. The federal laws referred to are the Federal Real Property and Federal Immovables Act and the Federal Real Property Regulations.

[155] Examples are found in requirements relating to the validation of documents by licensed or registered professionals, for example the Engineering and Geoscientific Professions Act (Manitoba, Canada) in respect of the Association of Professional Engineers and Geoscientists of the Province of Manitola, which defines an "electronic seal" as the form of identification issued by the Association to any member to be used in the electronic validation of documents in computer-readable form (see http://apegm.mb.ca/keydocs/act/index.html, accessed on 6 June 2008).

[156] The Uniform Real Property Electronic Recording Act of the United States was prepared by the National Conference of Commissioners on Uniform State Laws and is available at http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm (accessed on 6 June 2008). It has been adopted in Arizona, Arkansas, Connecticut, Delaware, the District of Columbia, Florida, Idaho, Illinois, Kansas, Minnesota, Nevada, New Mexico, North Carolina, South Carolina, Tennessee, Texas, Virginia, Washington and Wisconsin (see http://www.nccusl.org, accessed on 20 March 2008).

be contained in the stamp, impression or seal must be attached to, or logically associated with, the document or signature in an electronic fashion.[157] Thus, the notarial stamp or impression that is required under the laws of some states is not required for an electronic notarization under this act. Nor is there a need for a corporate stamp or impression as would otherwise be required under the laws of some states to verify the action of a corporate officer.

121. Seals are not frequently used on private documents in civil law jurisdictions, although most such jurisdictions make extensive use of notarization as a means of ensuring identity of persons and authenticity of documents. In several civil law jurisdictions, notaries have already introduced information and telecommunications technologies as a standard tool of their work. In many countries, chambers of notaries have established certification services providers to issue certificates supporting the use of electronic signatures (typically digital signatures) by member notaries and sometimes also by the public.

122. In Italy, the Council of Notaries was authorized on 12 September 2002 by the Authority for Information Technology in Government to offer certification services to Italian notaries, whose digital signatures may be verified online.[158] Furthermore, Italian notaries are in the process of a complete migration towards the use of electronic technologies for the transmission of records to public registries. For the transmission of memorandums and articles of association and their amendments to commercial registries, for instance, paper documents have already been completely eliminated. Significant progress has also been made as regards the electronic transmission of records of transactions involving real property, although paper documents are still in use owing purportedly to delays in the introduction of electronic communications technologies in the court system. These services are provided with support from a corporation specially established in 1997 by the Council and the National Fund for Notaries for the purpose of handling information and communication technologies services for Italian notaries.[159] A similar system is in use in Spain where the general Council of Notaries established its own certification authority and notaries have developed a system for electronic filing of records with trade registers.[160]

123. In France, the revised text of article 1317 of the Civil Code, for instance, allows the recording of "authentic acts" by electronic means under conditions to be established by the Council of State. The French High Council of Notaries has established a certification system for digital signatures used by French notaries.[161] The system used by French notaries is certified by a corporation established by several agencies of the Government of France to offer certification services. Although French notaries are not yet using electronic transmission of records to the same extent as Italian and Spanish

[157] That is, criteria similar to those embodied in the Uniform Electronic Transactions Act of the United States.

[158] See http://ca.notariato.it (accessed on 6 June 2008).

[159] See www.notariato.it, under "Servizi Notartel" (accessed on 6 June 2008).

[160] See http://www.notariado.org/n_tecno (accessed on 6 June 2008).

[161] "La signature électronique notariale certifiée", *La revue fiscale notariale*, No. 10, October 2007, Alerte 53.

notaries, the development in May 2006 of the Télé@actes application should enable notaries to exchange title deeds with mortgage registries in an entirely electronic form. Work is also under way to digitize hard copies of real estate deeds.

124. In Germany, the 1993 Federal Act for Expediting Registry Procedures[162] made it possible to carry out real estate, trade and other statutory registration requirements in electronic form. The subnational judiciary administrations have used this possibility to varying extents and through various technical approaches.[163] The introduction of an electronic registry system enabled German notaries to exchange information directly with the registries by means of electronic communications. With a view to ensuring that notarized electronic records offer the same level of reliability as paper-based notarized records, German notaries established a certification services provider in accordance with the requirements of the German Electronic Signatures Law. The certification services provider was granted a licence by the German telecommunications regulator on 15 December 2000. As was already the case in other countries, the certification system established by the German notaries is a PKI-based system using digital signature technology. Certificates issued by the certification services provider of the Federal Chamber of Notaries certify not only the public key used by the notary to sign documents but also the signatory's authority as a sworn notary. Under the German system, digital signatures are used to authenticate records both at the time they are established and at the time of any reproduction. In the guidelines issued by the Federal Chamber of Notaries, notaries are reminded of the need to ensure secure transmission of electronic documents, for instance by using only SSL-secured connections.[164] In order to facilitate processing of electronic records by registries or their use by customers, German notaries are required to create documents in a standard format (Extensible Markup Language, or XML).[165] The German rules for issuing authentic electronic records require two layers of authentication by the notary. All electronic records, together with their annexes and the files containing the notary's digital signature, are linked and archived together in the ZIP file format and the entire ZIP file is authenticated once more with the notary's digital signature.

125. Electronic equivalents of notarized acts are also being used increasingly in Austria. The basic features of the Austrian system for electronic notarization are generally similar to those of the German system. One particular feature of the Austrian system, however, is the establishment of a centralized electronic registry ("cyberDOC") for the safe keeping of documents in electronic form. An independent company jointly established by the Austrian Chamber of Civil Law Notaries and

[162] Germany Bundesgesetztblatt, part I, 20 December 1993, p. 2182.

[163] See the information on the extent of implementation of electronic registries in Germany by the Federal Chamber of Notaries at http://www.bnotk.de/Service/Elektronischer_Rechtsverkehr/Registerelektronisierung.html (accessed on 6 June 2008).

[164] See *"Empfehlungen zur sicheren Nutzung des Internet"*, Rundschreiben 13/2004 der Bundesnotarkammer vom 12.03.2004 (available at http://www.bnotk.de/Service/Rundschreiben/RS.2004.13.sichere.Internetnutzung.html, accessed on 6 June 2008).

[165] See *"Hinweise und Anwendungsempfehlungen für den elektronischen Handels-, Genossenschafts- und Partnerschaftsregisterverkehr"* Rundschreiben 25/2006 der Bundesnotarkammer vom 07.12.2006 (available at http://www.bnotk.de/Service/Empfehlungen+Hinweise/RS25-06_El-Handelsregisterverkehr.html, accessed on 6 June 2008).

Siemens AG, provides notaries with an electronic archive that includes authentication functions.[166] Austrian notaries are obliged by law to record and store all notarial deeds perfected after 1 January 2000 in this archive.

126. While generally the authentication function of the notary in respect of signatures can be replicated in an electronic environment by the use of electronic authentication and signature methods, other functions require more extensive solutions. Notarized acts must typically mention, as appropriate, the date on which they are established, the date on which they are registered and the date on which they are signed or copied. The simple use of automatic techniques, it has been suggested, may substitute for a date certified by the notary.[167]

127. More important, though, are the procedures for maintaining electronic records of notarized acts. Notaries are typically mandated by law to keep a record of the documents they receive or produce. Replicating that general record in an electronic environment poses a number of challenges. Another—and more significant—problem relates to the risk of technical incompatibility between different software and equipment that may be used by notaries for that purpose. The rapid evolution of information and communications technologies increases the need for migrating data from one format or medium to another. The readability of data migrated to new formats and media, however, is not always guaranteed. This makes it necessary to conceive control procedures that allow for the verification of the integrity of the contents of a record prior to and after migration. As has already been pointed out, encryption technology based on PKIs does not necessarily assure the readability of the digital signatures themselves over time (see para. 51 above). This requires careful management of the migration process, and possibly a confirmation of the authentication originally used. It has been found that, in order to ensure consistency and interoperability, it is preferable to entrust this function to a trusted third party rather than to the individual notaries.[168]

128. This was, for instance, the model eventually chosen by legislators in France. The recent reform of rules governing notarized records generally established the conditions for functional equivalence between paper-based notarized acts and electronic records.[169] Among the provisions concerning mainly information security, the new rules established a centralized archive of notarized acts in electronic form that ensures that the electronic records are kept in a manner that preserves their integrity; are only accessible to the notaries that generated them; are migrated to new formats, as technically needed without altering their content; and are capable of recording subsequent information by the notary without altering their original content.

[166] See Österreichische Notariatskammer (Austrian Chamber of Civil Law Notaries), available at http://www.notar.at, under “Cyberdoc” (accessed on 6 June 2008).

[167] Didier Froger, “Les contraintes du formalisme et de l’archivage de l’acte notarié établi sur support dématérialisé”, La semaine juridique (édition notariale et immobilière), No. 11, 12 March 2004, p. 1130.

[168] Didier Froger, “Les contraintes du Formalisme ...”.

[169] France. “Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires”, Journal Officiel, 11 August 2005, p. 96.

129. Despite the progress made in recent years, some doubts remain about how new rules authorizing the electronic equivalent of paper-based notarized acts can be reconciled with the essential elements of authentic acts, in particular the need for the physical presence of the parties before the notary.[170] On the assumption that physical presence is indispensable for the establishment of an authentic legal record, the challenge is to develop possible adaptations of existing forms to future technologies.[171] In that connection, it has been said that cryptology does not substitute for the tangible symbols of the public authority and the parties' consent.[172] Thus, some rules require the parties and the witnesses to be able to actually see an image of their signature on the screen; similarly, an image of the notary's seal has to appear on all acts.[173]

130. In the United States, there are three principal statutes that are relevant for electronic notarization: the Uniform Electronic Transactions Act,[174] the Electronic Signatures in Global and National Commerce Act (E-sign)[175] and the Uniform Real Property Electronic Recording Act.[176] In combination, they provide that the legal requirements for a document, or a signature associated with a document to be notarized, acknowledged, verified, witnessed or made under oath will be satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the document or signature. A number of states have since developed systems for notarization through electronic means. The Pennsylvania Department of State, for instance, together with a special team of county recorders have developed the e-Notary Registry and Electronic Notary Seal Program, which allows for real-time authentication of notaries and secure online delivery of verified electronic notary seals. This electronic notarization system is aimed at streamlining business transactions between government officials and businesses and at increasing protection for the public against forgery and fraud, while maintaining the fundamental components of notarization. The system makes use of digital certification services from a commercial services provider.[177]

131. Notaries interested in participating in this electronic notarization initiative must apply to the state's Bureau of Commissions, Elections and Legislation to become an approved electronic notary (e-notary). The notary public must obtain, for a fee, a digital certificate in the form of an electronic notary seal from the federally certified certification authority approved by the Office of Administration and the Secretary of the Commonwealth of Pennsylvania and selected by the recorders of deeds participating in the

[170] Pierre-Yves Gautier and Xavier Linant de Bellefonds, "De l'écrit électronique et des signatures qui s'y attachent", *La semaine juridique (édition générale)*, No. 24, 14 June 2000, I 236, sects. 8-10.

[171] Pierre Catala, "Le formalisme et les nouvelles technologies", *Répertoire du notariat Defrénois*, No. 20, 2000, pp. 897-910.

[172] Luc Grynbaum, "Un acte authentique électronique pour les notaires", Communication Commerce électronique, No. 10, October 2005, com. 156.

[173] Decree No. 71-941, as amended by decree No. 2005-973, art. 17, para. 3, (see note 169).

[174] See note 90.

[175] Codified as United States Code, title 15, chapter 96, sections 7001-7031.

[176] See note 156.

[177] Anthony Garritano, "National e-notary standards in progress", *Mortgage Servicing News* (New York), vol. 10, No. 2, 1 March 2006, p. 11.

electronic notarization initiative. Prior to obtaining a digital certificate, the approved e-notary must appear in person before any of the recorders of deeds participating in the electronic notarization initiative and present the approval letter from the Department of State and satisfactory evidence of identity to the recorder of deeds. The approved e-notary must ensure that for each electronic notarization the following information is attached to or logically associated with the electronic signature or electronic record being notarized, acknowledged or verified: the e-notary's full name along with the words "notary public", the name of the municipality and county in which the e-notary maintains an office and the date on which the e-notary's commission is due to expire. The e-notary must ensure that the individual for whom he or she is performing an electronic notarization personally appears before him or her for each electronic notarization performed. According to the Department of State of Pennsylvania, the fundamental components of notarization, including personal appearance of the document signers before the notary, still apply. Nevertheless, rather than a paper document and a rubber stamp notary seal, the notary digitally affixes his or her identifying information to a document which exists as electronic data in a computer-readable form.[178]

132. In much the same way as in civil law jurisdictions, there has been some discussion in common law jurisdictions as to the ability of electronic means to replicate the function of traditional notarization and authentication methods. As long as the notarization is essentially limited to confirming the integrity of documents and the identity of the signatories, there seems to be no insurmountable difficulty in using electronic communications as the equivalent of paper documents. However, the situation becomes less clear when the authenticity of a document or record is certified by a notary's confirmation of a person's presence at the act of executing the document or record.[179]

133. It has been argued that traditional witnessing processes, such as attestation, which may be used in connection with, but also independently from, the drawing up of a public deed by a notary public, are not wholly adaptable to the process of electronically signing documents, since there is no assurance that the image on the screen is in fact the document to which the electronic signature will be affixed. All that the witness and the signatory can see is a representation on the screen, capable of being read by a human being, of what is allegedly in the information system. When the wit-

[178] See http://www.dos.state.pa.us/dos/site/default.asp, under "Notaries", "Electronic Notarization" (accessed on 5 June 2008).

[179] "With technology now enabling 'teleconferences' between parties in different cities, or even different nations, the future will likely bring broadened statutory definitions of 'personal appearance' whereby a notary in Los Angeles might attest to a televised signature affixation by a person in London. The notary's audial interaction with the absent signer and real-time acquisition of the signer's video image would seem prerequisites for such remote electronic notarizations. Yet, while these electronic notarial acts, with the notary at one site and the acknowledger or affiant at another, are at least conceivable without audial interaction, as the widespread use of electronic mail demonstrates, visual interaction seems a sine qua non. How else for the notary to determine that a remote signer is not being blatantly coerced and to record a visual image providing evidence that the transmitter was not an impostor using a stolen private key. Just as the Nebraska Supreme Court in 1984 (*Christensen v. Arant*) held that mere audial contact through an intervening door did not suffice as physical presence in the traditional legal sense, so it is likely that mere electronic contact through a nonvisual medium will not suffice as physical presence in the futuristic legal sense" (Charles N. Faerber, "Being there: the importance of physical presence to the notary", The John Marshall Law Review, vol. 31, spring 1998, pp. 749-776).

ness sees the signatory pressing the keyboard, the witness will not know with certainty what is actually happening. Thus, it would be possible to ensure that the screen display corresponds to the contents of the information system and that the signatory's keystrokes correspond to his or her intentions only if the information system has been confirmed to effect a trusted path by trusted evaluation criteria.[180]

134. However, a secure electronic signature would be able to perform a function similar to the attesting witness by identifying the person purporting to sign the deed. Using a secure electronic signature without a human witness, it could be possible to verify the authenticity of the signature, the identity of the person to whom the signature belongs, the integrity of the document and probably even the date and time of signing. In this sense, a secure electronic signature may even be superior to an ordinary handwritten signature. The advantages of having, in addition, an actual witness to attest a secure digital signature would probably be minimal unless the voluntary nature of the signing is in question.[181]

135. Existing legislation has not gone so far as to entirely replace attestation requirements with electronic signatures, but merely allows the witness to use an electronic signature. The Electronic Transactions Act of New Zealand provides that the electronic signature of a witness meets the legal requirement for a signature or seal to be witnessed. The technology to be used in making the electronic signature is not specified, but must adequately identify the witness and adequately indicate that the signature or seal has been witnessed; and be as reliable as is appropriate given the purpose for which, and the circumstances in which, the witness's signature is required.[182]

136. The Personal Information Protection and Electronic Documents Act of Canada provides that requirements in federal law for a signature to be witnessed are satisfied with respect to an electronic document if each signatory and each witness sign the electronic document with their secure electronic signature.[183] A statement required to be made under certain federal laws declaring or certifying that any information given by a person making the statement is true, accurate or complete may be made in electronic form if the person signs it with his or her secure electronic signature.[184] A statement required to be made under oath or solemn affirmation under federal law may be made in electronic form if the person who makes the statement signs it with his or her

[180] This is referred to as the "what you see is what you sign" (WYSIWYS) problem in the literature (see also for a discussion of trusted display controllers) (V. Liu and others, "Visually sealed and digitally signed documents", Association of Computing Machinery, *ACM International Conference Proceedings Series*, vol. 56; and *Proceedings of the Twenty-seventh Australasian Conference on Computer Science*, vol. 26 (Dunedin, New Zealand, 2004), p. 287).

[181] See discussions in Joint Infocomm Development Authority of Singapore and the Attorney-General's Chambers, *Joint IDA-AGC Review of Electronic Transactions Act Stage II: Exclusions under Section 4 of the ETA*, consultation paper LRRD No. 2/2004 (Singapore, 2004), parts 5 and 8, available at www.agc.gov.sg, under "Publications" (accessed on 6 June 2008).

[182] New Zealand, Electronic Transactions Act (see note 88), section 23.

[183] Canada, Personal Information Protection and Electronic Documents Act (2000), part 2, sect. 46.

[184] Canada, Personal Information Protection ..., section 45.

secure electronic signature, and the person before whom the statement was made, and who is authorized to take statements under oath or solemn affirmation, signs it with his or her secure electronic signature.[185] An alternative that has been suggested to provide further assurance is for the electronic signature to be executed by or in the presence of a trusted professional such as a lawyer or a notary.[186]

[185] Canada, Personal Information Protection ..., section 44.

[186] Conveyancers will need to have electronic signatures and authentication from a recognized certification authority. Buyers and sellers might need to empower conveyancers to sign by written authority. See "E-conveyancing: the strategy for the implementation of e-conveyancing in England and Wales" (United Kingdom, Land Registry, 2005), available at http://www.cofrestrfatir.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc (accessed on 5 June 2008). The project is scheduled to be implemented in tranches from 2006 to 2009.

Part two

Cross-border use of electronic signature and authentication methods

Contents

Page

I. Legal recognition of foreign electronic authentication and signature methods

137. Legal and technical incompatibilities are the two principal sources of difficulties in the cross-border use of electronic signature and authentication methods, in particular where they are intended to substitute for a legally valid signature. Technical incompatibilities affect the interoperability of authentication systems. Legal incompatibilities may arise because the laws of different jurisdictions impose different requirements in relation to the use and validity of electronic signature and authentication methods.

A. International impact of domestic laws

138. Where domestic laws allow for electronic equivalents of paper-based authentication methods, the criteria for the validity of such electronic equivalents may be inconsistent. For example, if the law recognizes only digital signatures, other forms of electronic signatures will not be acceptable. Other inconsistencies in the criteria for the recognition of electronic authentication and signature methods may not prevent their cross-border use in principle, but the cost and inconvenience arising from the need to comply with the requirements imposed by various jurisdictions may reduce the speed and efficiency gains expected from the use of electronic communications.

139. The following sections discuss the impact of varying legal approaches to technology on the growth of cross-border recognition. They also summarize the emerging international consensus on the measures that could potentially facilitate the international use of electronic signature and authentication methods.

1. International obstacles created by conflicting domestic approaches

140. Technology-neutral approaches, especially those which incorporate a "reliability test", tend to resolve legal incompatibilities. International legal instruments adopting this approach include the UNCITRAL Model Law on Electronic Commerce (in its article 7, paragraph 1 (*b*)) and the United Nations Convention on the Use of Electronic Communications in International Contracts (in its article 9, paragraph 3). Under this approach, an electronic signature or authentication method that can both identify the signatory and indicate the signatory's intention in respect of the information contained in the electronic communication will fulfil signature requirements, provided it meets

several criteria. In the light of all the circumstances, including any agreement between the originator and the addressee of the data message, the signature or authentication method must be shown to be as reliable as is appropriate for the purpose for which the data message is generated or communicated. Alternatively, by itself or in conjunction with other evidence, it must be shown to have fulfilled these purposes.

141. Arguably, the minimalist approach facilitates cross-border use of electronic authentication and signatures, since under this approach any method of electronic signature or authentication may be validly used to sign or authenticate a contract or communication, as long as it meets the above general conditions. The consequence of this approach, however, is that such conditions are typically only confirmed a posteriori, and there is no assurance that a court will recognize the use of any particular method.

142. Cross-border use of electronic authentication and signatures becomes a real issue in systems that either mandate or favour a particular technology. The complexity of the problem increases in direct relation to the level of governmental regulation of electronic signatures and authentication and the degree of legal certainty that the law attaches to any specific method or technology. The reasons for this are simple: where the law does not attach any particular legal value or presumption to particular types of electronic signature or authentication, and merely provides for their general equivalence to handwritten signatures or paper-based authentication, the risks of reliance on an electronic signature are the same as the risk of reliance on a handwritten signature under existing law. However, where more legal presumptions are attached by the law to a particular electronic signature (typically those regarded as "secure" or "advanced"), the increased level of risk is shifted from one party to another. One fundamental assumption of technology-specific legislation is that such a general a priori shift in legal risks may be justified by the level of reliability offered by a given technology, once certain standards and procedures are complied with. The downside to this approach is that once reliability a priori is predicated upon the use (among other conditions) of a particular technology, all other technologies—or even the same technology used under slightly different conditions—become a priori unreliable, or at least fall under suspicion a priori of unreliability.

143. Conflicting technology-specific national legislation may therefore inhibit rather than promote the use of electronic signatures in international commerce. This could happen in two distinct but closely interrelated ways.

144. First, if electronic signatures and the certification services providers who authenticate them are subject to conflicting legal and technical requirements in different jurisdictions, this may inhibit or prevent electronic signatures from being used in many cross-border transactions, if the electronic signature cannot satisfy the various jurisdictional requirements simultaneously.

145. Second, technology-specific legislation, particularly legislation that favours digital signatures, which is also the case in the two-tiered approach, is likely to give rise to a patchwork of conflicting technical standards and licensing requirements that will

make the use of electronic signatures across borders very difficult. A system in which each country prescribes its own standards may also prevent parties from entering into mutual recognition and cross-certification agreements.[187] Indeed, a major remaining problem relating, in particular, to digital signatures is that of cross-border recognition. The Working Party on Information Security and Privacy (WPSIP) of the Organization for Economic Cooperation and Development (OECD) (hereinafter OECD WPSIP) has noted that although the approach adopted by most jurisdictions appears to be non-discriminatory, differences in local requirements will continue to engender interoperability problems.[188] For the purposes of the present study, the following weaknesses noted by OECD WPSIP may be relevant:

(*a*) *Interoperability.* Challenges and limitations to interoperability were found to be prevalent. At the technical level, although there is an abundance of standards, the lack of "core", common standards for some technologies was cited as a problem. At the legal/policy level, the difficulty in principals understanding their respective trust framework, including assignment of liability and compensation, were cited as factors that were impeding progress. According to OECD WPSIP, this is an area that "would appear to require closer examination and scrutiny with a view to perhaps developing common tools to assist jurisdictions in achieving the level of interoperability desired for a particular application or system";

(*b*) *Recognition of foreign authentication services.* The focus of efforts according to OECD WPSIP has been on establishing domestic services. Thus, mechanisms for recognizing foreign authentication services "are generally not very well developed". On this basis, OECD WPSIP suggests that this "would appear to be an area where further work would be useful. Given that any work in this area would be highly related to the more general subject of interoperability, the topics could be combined";

(*c*) *Acceptance of credentials.*[189] In some cases, the acceptance of the credentials issued by other entities was cited as a barrier to interoperability. As such, OECD WPSIP suggests that consideration could be given to the possibility of developing a set of best practices or guidelines for issuing credentials for authentication purposes. Work may already be under way in several jurisdictions on this issue that could provide useful input to any initiatives of OECD WPSIP in this regard;

[187] Baker and Yeo, "Background and issues concerning authentication …".

[188] Organization for Economic Cooperation and Development, Working Party on Information Security and Privacy, *The Use of Authentication across Borders in OECD Countries* (DSTI/ICCP/REG(2005)4/FINAL), available at http://www.oecd.org/dataoecd/1/10/35809749.pdf (accessed on 6 June 2008).

[189] A credential is a token given to prove that an individual or a specific device has gone through an authentication process. Credentials that are bound to the user are essential for identification purposes. Bearer credentials may be sufficient for some forms of authorization. Examples are a valid driving licence, a person's social security number or other identification number, or smart cards (Centre for Democracy and Technology, "Privacy principles for authentication systems", available at http://www.cdt.org/privacy/authentication/030513interim.shtml (accessed on 5 June 2008)).

(*d*) *A range of authentication methods in use.* OECD WPSIP found that in virtually all OECD member States, a range of authentication solutions was in use. The methods range from passwords on the one hand, to tokens, digital signatures and biometrics on the other. Depending on the application, and its requirements, the methods can be used alone, or in combination. While many would view this as positive, the information gathered in the OECD WPSIP survey suggests that the range of possibilities is so great that application providers and users run the risk of being hopelessly confused as to which method is appropriate for their requirements. According to OECD WPSIP, this would suggest that there could be some benefit to introducing a reference tool for assessing the various authentication methods and the degree to which their attributes address requirements identified by application providers or users.

146. Confidence in the use of electronic signature and authentication methods in international transactions might be raised by wide adoption of the United Nations Convention on the Use of Electronic Communications in International Contracts and implementation of its technology-neutral approach to electronic signatures and authentication. However, it is unrealistic to expect that this would entirely obviate the need for a harmonized solution for dealing with incompatible legal and technical standards. Many countries may still prescribe the use of specific authentication methods in certain types of transaction. Also, some countries may feel that more concrete guidance is needed to assess the reliability of signature and authentication methods, in particular foreign ones, and their equivalence to methods used or at least known in the country.

2. *Emerging consensus*

147. The policy divergence that has occurred internationally is probably the result of a combination of factors, in varying degrees. As has been seen earlier (see paras. 2-6 above), some countries tend to have more stringent and particularized form requirements with respect to signatures and documents, while others focus on the intent of the signing party and permit a broad range of ways to prove the validity of signatures. These general differences usually find their way into specific legislation dealing with electronic authentication and signature methods (see paras. 83-112 above). An additional source of inconsistency results from the varying degree of governmental interference with technical aspects of electronic authentication and signature methods. Some countries are inclined to play a direct role in setting standards for new technologies, possibly in the belief that this confers a competitive advantage to local industry.[190]

148. The divergent policies may also reflect different assumptions about how authentication technologies will emerge. One scenario, the so-called "universal authentication paradigm",[191] assumes that the principal purpose of authentication technologies will be to verify identities and attributes among persons who have no pre-existing relationship with each other and whose common use of technology is not the subject of contractual agreement. Therefore, the authentication or signature technology should

[190] Baker and Yeo, "Background and issues concerning authorization …".

[191] Baker and Yeo, "Background and issues concerning authorization …".

confirm the identity or other attributes of a person to a potentially unlimited number of persons and for a potentially unlimited number of purposes. This model stresses the importance of technical standards and of the operational requirements of certification services providers when trusted third parties are involved. Another scenario, the so-called "bounded authentication paradigm", advocates that the principal use of authentication and signature technologies will be to verify identities and attributes among persons whose common use of the technology takes place under contractual agreements.[192] Therefore, the authentication technology should confirm the identity or other attributes of the certificate holder only for a set of specifically defined purposes and within a defined community of potentially relying parties who are subject to common terms and conditions for the use of the technology. Under this model, focus is on the legal recognition of the contractual agreements.

149. Despite these discrepancies, some of which still prevail, the findings of OECD WPISP[193] suggest that there now appears to be a growing international consensus on the basic principles that should govern electronic commerce and in particular electronic signature. The following findings are particularly interesting for the present study:

(*a*) *Non-discriminatory approach to "foreign" signatures and services.* The legislative frameworks do not deny legal effectiveness to signatures originating from services based in other countries as long as these signatures have been created under the same conditions as those given legal effect domestically. On this basis, the approach appears to be non-discriminatory, as long as local requirements, or their equivalent, are met. This is consistent with findings in previous surveys on authentication done by OECD WPISP;

(*b*) *Technology-neutrality.* While virtually all respondents indicated that their legislative and regulatory framework for authentication services and e-signatures was technology-neutral, the majority indicated that, where e-government applications were involved, or where maximum legal certainty of the electronic signature was required, the use of PKI was specified. On that basis, while legislative frameworks may be technology-neutral, policy decisions seem to require the technology to be specified;

(*c*) *PKI prevalence.* According to OECD WPISP, PKI seems to be the authentication method of choice when strong evidence of identity and high legal certainty of the electronic signature is required. It is used in specific "communities of interest" where all users seem to have a prior business relationship of some form. The use of PKI-enabled smart cards and the integration of digital certificate functions into application software have made the use of this method less complicated for users. However, it is generally acknowledged that PKI is not required for all applications and that the choice of authentication method should be made on the basis of its suitability for the purposes for which it would be used.

[192] Baker and Yeo, "Background and issues concerning authorization …".

[193] Organization for Economic Cooperation and Development, *The Use of Authentication across Borders in OECD Countries ….*

150. Furthermore, OECD WPISP found that regulatory frameworks in all the countries surveyed had some form of legislative or regulatory framework in place to provide for the legal effect of electronic signatures at the domestic level. OECD WPISP found that, while the details of the legislation might differ between jurisdictions, a consistent approach appeared nevertheless to be discernible, in that most domestic laws were based on existing international or transnational frameworks (i.e. the UNCITRAL Model Law on Electronic Signatures and directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures[194]).

151. The essential points of this emerging consensus have been restated in the recommendation on electronic authentication adopted by the OECD Council on 12 June 2007, which, inter alia, invites States:

(*a*) To work towards establishing technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities;

(*b*) To foster the development, provision and use of electronic authentication products and services that embody sound business practices, including technical and non-technical safeguards to meet the participants' needs, in particular with respect to security and privacy of their information and identity;

(*c*) To encourage in both the private and public sectors, business and legal compatibility and technical interoperability of authentication schemes, to facilitate cross-sectoral and cross-jurisdictional online interactions and transactions and to ensure that authentication products and services can be deployed at both the national and the international levels;[195]

(*d*) To take steps to raise the awareness of all participants, including those in non-member State economies, on the benefits of the use of electronic authentication at the national and the international levels.

152. These recommendations are largely consistent with the overall approach taken by UNCITRAL in the area of electronic commerce (e.g. facilitation rather than regulation, technology-neutrality, respect for freedom of contract, non-discrimination). There are, however, several legal issues that need to be addressed to facilitate the use of electronic authentication and signature methods in an international or cross-border context.

[194] *Official Journal of the European Communities*, L 13/12, 19 January 2000.

[195] *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication* (Paris, June 2007), available at http://www.oecd.org/dataoecd/32/45/38921342.pdf (accessed on 6 June 2008).

B. Criteria for recognition of foreign electronic authentication and signature methods

153. As noted above, one of the main obstacles to the cross-border use of electronic signatures and authentication has been a lack of interoperability, due to conflicting or divergent standards or their inconsistent implementation. Various forums have been established to promote standards-based, interoperable PKI as a foundation for secure transactions in electronic commerce applications. They include both intergovernmental[196] and mixed public sector and private sector organizations[197] at a global[198] or regional level.

154. Some of this technical work aims at developing technical standards for the provision of the information necessary for meeting certain legal requirements.[199] How-

[196] In the Asia-Pacific region, the Asia-Pacific Economic Cooperation (APEC) forum has developed "Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction eCommerce" (eSecurity Task Group, APEC Telecommunications and Information Working Group, December 2004) (available at http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf (original available with the Secretariat)). These Guidelines are intended to assist in developing schemes that are potentially interoperable and in reviewing the interoperability of existing schemes. The Guidelines cover classes or types of certificate used in transnational e-commerce only. The Guidelines are not intended to address other certificates, nor are they intended to limit schemes to only issuing certificates covered by the Guidelines.

[197] Within the European Union, the European Electronic Signature Standardization Initiative (EESSI) was created in 1999 by the Information and Communications Technology (ICT) Standards Board to coordinate the standardization activity in support of the implementation of European Union directive 1999/93/EC on electronic signatures. The ICT Standards Board itself is an initiative of the European Committee for Standardization (CEN), which was created by national standards organizations and two non-profit organizations: the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). EESSI has developed various standards to promote interoperability, but their implementation has been slow, allegedly because of their complexity (Paolo Balboni, "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information and Communications Technology Law*, vol. 13, No. 3 (2004), pp. 211-242).

[198] For example, the Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit, international consortium founded in 1993 to promote the development, convergence and adoption of standards for electronic business. OASIS has established a PKI Technical Committee comprised of PKI users, vendors and experts to address issues related to the deployment of digital certificates technology. The PKI Technical Committee has developed an action plan that contemplates, inter alia, developing specific profiles or guidelines that describe how the standards should be used in particular applications so as to achieve PKI interoperability; creating new standards, where needed; and providing interoperability tests and testing events (OASIS, PKI Technical Committee, "PKI action plan" (February 2004), available at http://www.oasis-open.org/committees/pki/pkiactionplan.pdf (accessed on 6 June 2008)).

[199] For example, ETSI has developed a standard (TS 102 231) to implement a non-hierarchical structure that, among other things, can address also cross recognition of PKI domains and, therefore, of certificates' validity. Basically, ETSI technical standard TS 102 231 specifies a standard for the provision of information on the status of a provider of certification services (called a "trust service provider"). It adopts the form of a signed list, the "Trust Service Status List", as the basis for presentation of this information. The Trust Service Status List specified by ETSI accommodates the requirement of evidence as to whether the provider of a trust service is or was operating under the approval of any recognized scheme at either the time the service was provided or the time at which a transaction reliant on that service took place. In order to fulfil that requirement, the Trust Service Status List must contain information from which it can be established whether the certification services provider's service was, at the time of the transaction, known by the scheme operator and if so what the status of the service was (i.e. whether it was approved, suspended, cancelled or revoked). The Trust Service Status List contemplated by ETSI technical standard TS 102 231 must therefore contain not only the service's current status, but also the history of its status. Therefore, the list becomes a combination of valid services ("white list") and cancelled or revoked services ("black list") (see http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc, accessed on 6 June 2008).

ever, to a large extent, this important work is mainly concerned with technical aspects rather than legal issues and falls outside the scope of this study. The discussion in the following sections is therefore focused on the formal and substantive legal requirements for cross-border recognition of electronic signatures.

1. Place of origin, reciprocity and local validation

155. Place of origin has been a classic factor in affording legal recognition to foreign documents or acts. This is typically done on the basis of reciprocity, so that signatures and certificates of a given country will be given domestic effect to the extent that domestic signatures and certificates are given legal effect in the other country. Another possibility is to subject the domestic effect of the foreign signature and certificate to some form of validation or acknowledgement by a domestic certification services provider, certification authority or regulator. These approaches may be combined.[200]

156. It is not common for domestic laws expressly to deny legal recognition to foreign signatures or certificates, which may confirm the appearance of their non-discriminatory character. In practice, however, many recognition regimes are likely to have some discriminatory impact, even if unintended. The European Union directive on electronic signatures, for example, generally bans discrimination of foreign qualified certificates (i.e. PKI-based digital signatures). However, this works mainly in favour of certificates issued by certification services providers established within the territory of the States members of the European Union. A certification services provider established in a non-European-Union country has three options to obtain recognition of its certificate in the European Union: fulfil the requirements of the European Union directive on electronic signatures and obtain accreditation under a scheme established in a member State; establish a cross certification with a certification services provider established in a European Union member State; or operate under the umbrella of a general recognition at the level of international agreement.[201] The manner in which the European Union directive regulates international aspects suggests that ensuring conditions for market access abroad of European Union providers of certification services was one of the objectives pursued by the directive.[202] By cumulating the

[200] In Argentina, for instance, foreign certificates and electronic signatures are recognized if there is a reciprocity agreement between Argentina and the country of origin of the foreign certification authority or if there is acknowledgement by a certification authority licensed in Argentina and authenticated by the enforcement authority (see *Ley de firma digital* (2001), art. 16).

[201] Indeed, under article 7 of the Directive, European Union member States only must ensure that the certificates issued by a certification services provider in a third country are recognized as legally equivalent to certificates issued by a certification services provider established within the Community if (*a*) the certification services provider “fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State”; or (*b*) a certification services provider established within the Community that fulfils the requirements laid down in the Directive “guarantees” the certificate; or (*c*) the certificate or the certification services provider “is recognized under a bilateral or multilateral agreement between the Community and third countries or international organisations.”

[202] The concern with securing access by European certification services providers to foreign markets is clear from the formulation of article 7, paragraph 3, of the Directive, which provides that “whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries”.

requirement of substantive equivalence with European Union standards with the additional requirement of accreditation under a scheme established in a member State, the European Union directive on electronic signatures effectively requires foreign certification services providers to comply both with their original and with the European Union regime, which is a higher standard than is required from certification services providers accredited in a State member of the European Union.[203]

157. Article 7 of the European Union directive on electronic signatures has been implemented with some variations.[204] Ireland and Malta, for instance, recognize foreign digital signatures (qualified certificates, under European Union terminology) as equivalent to domestic signatures, as long as other legal requirements are satisfied. In other cases, recognition is subject to domestic verification (Austria, Luxembourg) or a decision of a domestic authority (Czech Republic, Estonia, Poland). This tendency to insist on some form of domestic verification, which is typically justified by a legitimate concern as to the level of reliability of foreign certificates, leads in practice to a system of discrimination of foreign certificates on the basis of their geographical origin.

2. Substantive equivalence

158. Consistent with a long-standing tradition, UNCITRAL declined to endorse geographical considerations when proposing factors for recognition of foreign certificates and electronic signatures. Indeed, article 12, paragraph 1, of the UNCITRAL Model Law on Electronic Signatures expressly provides that in determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had either to the geographical location where the certificate is issued or the electronic signature created or used or to the geographical location of the place of business of the issuer or signatory.

159. Paragraph 1 of article 12 of the UNCITRAL Model Law on Electronic Signatures is intended to reflect the basic principle that the place of origin, in and of itself, should in no way be a factor in determining whether and to what extent foreign certificates or electronic signatures should be recognized as capable of being legally effective. Determination of whether, or the extent to which, a certificate or an electronic signature is capable of being legally effective should depend on its technical reliability, rather than the place where the certificate or the electronic signature was issued. Non-discrimination provisions similar to article 12 of the Model Law on Electronic Signatures can also be found in some domestic regimes, such as the United States Electronic Signatures in Global and National Commerce Act 2000.[205] These provisions provide that the place of origin, in and of itself, should not be a factor in determining whether and to what extent foreign certificates or electronic signatures

[203] Jos Dumortier and others, “The legal and market aspects of electronic signatures”, study for the European Commission Directorate General Information Society, Katholieke Universiteit Leuven, 2003, p. 58.

[204] Jos Dumortier and others, “The legal and market aspects of electronic signatures”…, pp. 92-94.

[205] United States Code, title 15, chapter 96, section 7031 (Principles governing the use of electronic signatures in international transactions).

should be recognized as capable of being legally effective in an enacting State. They recognize that the legal effectiveness of a certificate or electronic signature should depend on its technical reliability.[206]

160. Rather than geographical factors, the Model Law establishes a test of substantive equivalence between the reliability levels offered by the certificates and signatures in question. Accordingly, if the foreign certificate offers a substantially equivalent level of reliability as a certificate issued in the enacting State, it shall have the same legal effect. By the same token, an electronic signature created or used outside the country shall have the same legal effect as an electronic signature created or used in the country if it offers a substantially equivalent level of reliability. The equivalence between the reliability levels offered by the domestic and foreign certificates and signatures must be determined in accordance with recognized international standards and any other relevant factors, including an agreement between the parties to use certain types of electronic signatures or certificates, unless the agreement would not be valid or effective under applicable law.

161. The Model Law does not require or promote reciprocity arrangements. In fact, the Model Law contains no specific suggestion as to the legal techniques through which advance recognition of the reliability of certificates and signatures complying with the law of a foreign country might be made by an enacting State (e.g. a unilateral declaration or a treaty).[207] Possible methods to achieve that result that were mentioned during the preparation of the Model Law included, for example, automatic recognition of signatures complying with the laws of another State if the laws of the foreign State required a level of reliability at least equivalent to that required for equivalent domestic signatures. Other legal techniques through which advance recognition of the reliability of foreign certificates and signatures might be made by an enacting State could include unilateral declarations or treaties.[208]

[206] *UNCITRAL Model Law on Electronic Signatures* ..., part two, para. 83.

[207] Ibid., para. 157.

[208] See the report of the Working Group on Electronic Commerce on the work of its thirty-seventh session (A/CN.9/483, paras. 39 and 42).

II. Methods and criteria for establishing legal equivalence

162. As indicated above, the survey undertaken by OECD WPISP found that most legislative frameworks were at least in principle non-discriminatory towards foreign electronic signatures and authentication, provided local requirements or their equivalent were met, in the sense that they did not deny legal effectiveness to signatures relating to services originating in foreign countries, provided those signatures had been created under the same conditions as those recognized under domestic law.[209] However, OECD WPISP also noted that mechanisms for recognizing foreign authentication services were generally not well developed and identified this as an area where future work might be useful. Given that any work in this area would be closely related to the more general subject of interoperability, OECD WPISP suggested that the topics could be combined. OECD WPISP suggested that a set of best practices or guidelines might be developed. More recently, OECD has noted that mechanisms for recognizing foreign authentication services have been developed but there is limited experience in cross-jurisdictional applications. Furthermore, jurisdictions need some means of assessing the trust framework of their partners. Although OECD expressed the hope that its own guidelines and the framework they offer may assist in this regard, it pointed out that more comprehensive work on the issue needed to be carried out.[210] The following sections discuss the legal arrangements and mechanisms for international interoperability and factors that determine the equivalence of liability regimes. They focus primarily on issues arising out of the international use of electronic signature and authentication methods supported by certificates issued by a trusted third-party certification services provider, in particular digital signatures under a PKI, since legal difficulties are more likely to arise in connection with the cross-border use of electronic signature and authentication methods that require the involvement of third parties in the signature or authentication process.

A. Types and mechanisms of cross recognition

163. The additional burden placed on foreign certification services providers by domestic technology-driven requirements has the potential to become a barrier to international trade.[211] For example, laws relating to the means by which national

[209] Organization for Economic Cooperation and Development, *The Use of Authentication across Borders in OECD Countries ….*

[210] *OECD Recommendation on Electronic Authentication …*, p. 27.

[211] See Alliance for Global Business, "A discussion paper on trade-related aspects of electronic commerce in response to the WTO's e-commerce work programme", April 1999, p. 29 (available at http://www.biac.org/statements/iccp/AGBtoWTOApril1999.pdf, accessed on 6 June 2008).

authorities grant recognition to foreign electronic signatures and certificates could discriminate against foreign businesses. So far, every legislature that has considered this issue has included in its laws some requirement relating to the standards adhered to by the foreign certification services provider, so the issue is inextricably related to the broader question of conflicting national standards. At the same time, legislation may also impose other geographical or procedural limitations that prevent cross-border recognition of electronic signatures.

164. In the absence of an international PKI, a number of concerns could arise with respect to the recognition of certificates by certification authorities in foreign countries. The recognition of foreign certificates is often achieved by a method called "cross certification". In such a case, it is necessary that substantially equivalent certification authorities (or certification authorities willing to assume certain risks with regard to the certificates issued by other certification authorities) recognize the services provided by each other, so that their respective users can communicate with each other more efficiently and with greater confidence in the trustworthiness of the certificates being issued. Legal issues may arise with regard to cross-certifying or chaining of certificates when there are multiple security policies involved, such as determining whose misconduct caused a loss and upon whose representations the user relied.

1. Cross recognition

165. Cross recognition is an interoperability arrangement in which the relying party in the area of a PKI can use authority information in the area of another PKI to authenticate a subject in the area of the other PKI.[212] This is typically the result of a formal licensing or accreditation process in the area of the other PKI, or of a formal audit process performed on the representative certification services provider of the PKI area.[213] The onus of whether to trust a foreign PKI area lies with the relying party or the owner of the application or service, rather than with a certification services provider that the relying party directly trusts.

166. Cross recognition would typically occur at the PKI level rather than at the level of the individual certification services provider. Thus, where one PKI recognizes another PKI, it automatically recognizes any certification services providers accredited under that PKI scheme. Recognition would be based on assessment of the other PKI's accreditation process rather than assessing each individual certification services provider accredited by the other PKI. Where PKIs issue multiple classes of certificates, the cross-recognition process involves identifying a class of certificates acceptable for use in both areas and basing the assessment on that class of certificates.

[212] The concept of cross recognition was developed in 2000 by the then Asia-Pacific Economic Cooperation Telecommunications and Information Working Group, Electronic Authentication Task Group (see *Electronic Authentication: Issues Relating to Its Selection and Use*, APEC publication No. 202-TC-01.2 (APEC, 2002), available at http://www.apec.org/apec/publications/all_publications/telecommunications.html (accessed on 6 June 2008)).

[213] Definition based on the work of the APEC Telecommunications and Information Working Group, Electronic Authentication Task Group.

167. Cross recognition entails issues of technical interoperability at the application level only, i.e. the application must be able to process the foreign certificate and access the directory system of the foreign PKI area to validate the status of the foreign certificate. It should be noted that, in practice, certification services providers issue certificates with various levels of reliability, according to the purposes for which the certificates are intended to be used by their customers. Depending on their respective level of reliability, certificates and electronic signatures may produce varying legal effects, both domestically and abroad. For example, in certain countries, even certificates that are sometimes referred to as "low-level" or "low-value" certificates might, under certain circumstances (e.g. where parties have agreed contractually to use such instruments), produce legal effect (see below, paras. 202-210). Therefore, the equivalence to be established is between functionally comparable certificates.

168. As said above, in cross recognition the decision to trust a foreign certificate lies with the relying party, not with its certification services provider. It does not necessarily involve a contract or agreement between two PKI domains. Detailed mapping of certificate policies[214] and certificate practice statements[215] is also unnecessary, as the relying party decides whether to accept the foreign certificate based on whether the certificate has been issued by a trustworthy foreign certification services provider. The certification services provider is regarded as trustworthy if it has been licensed or accredited by a formal licensing or accreditation body, or has been audited by a trusted independent third party. The relying party makes an informed decision unilaterally based on the policies stipulated in the certificate policy or certificate practice statement in the foreign PKI domain.

2. Cross certification between public key infrastructures

169. Cross certification refers to the practice of recognizing another certification services provider's public key to an agreed level of confidence, normally by virtue of a contract. It essentially results in two PKI domains being merged (in whole or in part) into a larger domain. To the users of one certification services provider, the users of the other certification services provider are simply signatories within the extended PKI.

170. Cross certification involves technical interoperability and the harmonization of certificate policies and certificate practice statements. Policy harmonization, in the form of the harmonization of certificate policies and certificate practice statements, is necessary to ensure that PKI domains are compatible both in terms of their certificate management operations (i.e. certificate issuance, suspension and revocation) and in their adherence to similar operational and security requirements. The amount of liability coverage is also relevant. This step is highly complex, as these documents are typically voluminous and deal with a wide range of issues.

[214] A certificate policy is 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.

[215] A certificate practice statement is a statement of the practices that a certification services provider employs in issuing certificates.

171. Cross certification is most suitable for relatively closed business models, e.g. if both PKI domains share a set of applications and services, such as e-mail or financial applications. Having technically compatible and operable systems, congruent policies and the same legal structures would greatly facilitate cross certification.

172. Unilateral cross certification (whereby one PKI domain trusts another but not vice versa) is uncommon. The trusting PKI domain must ensure unilaterally that its policies are compatible with those of the trusted PKI domain. Its use seems to be limited to applications and services where the trust required for the transaction involved is unilateral, e.g. an application in which the merchant has to prove the identity to the customer before the latter submits confidential information.

B. Equivalence of standards of conduct and liability regimes

173. Whether international use of electronic signature and authentication methods is based on a cross-recognition or cross-certification scheme, a decision to recognize a whole PKI or one or more foreign certification services providers or to establish equivalent levels between classes of certificates issued under different PKIs presupposes an assessment of the equivalence between the domestic and the foreign certification practices and certificates.[216] From a legal point of view, this requires an assessment of the equivalence between three main elements: equivalence in legal value; equivalence in legal duties; and equivalence in liability.

174. Equivalence in legal value means attributing to a foreign certificate and signature the same legal effect as a domestic equivalent. The resulting domestic legal effect will be determined essentially on the basis of the value attributed by the domestic law to electronic signature and authentication methods, which has already been discussed (see above, paras. 107-112). Recognizing the equivalence in legal duties and liability regimes entails a finding that the duties imposed on the parties operating under a PKI regime correspond in substance to those existing under the domestic regime and that the liability for breaches of those duties is substantially the same.

175. Liability in the context of electronic signatures may give rise to different issues depending on the technology and the certification infrastructure used. Complex issues may arise especially in those cases where certification is provided by a dedicated third party, such as a certification services provider. In this case, there will essentially be three parties involved, namely the certification services provider, the signatory and the relying third party. To the extent that the acts or omissions of one of the parties cause harm to any of the others or contravene their express or implied duties, each could

[216] The United States Federal Public Key Infrastructure Policy Authority, Certificate Policy Working Group, for example, has developed a methodology for providing a judgement as to the equivalence between elements of policy (based on the framework defined in RFC ("Request for Comments") 2527). This methodology may be used when mapping different PKIs or mapping a PKI against these guidelines (see http://www.cio.gov/fpkipa, accessed on 6 June 2008).

become liable, or may lose the right to assert liability, against another party. Various legislative approaches have been adopted with respect to liability in connection with the use of digital signatures:

(*a*) *No specific provisions on standards of conduct or liability.* One option may be for the law to remain silent on this point. In the United States, the Electronic Signatures in Global and National Commerce Act 2000[217] does not provide for the liability of any of the parties involved in the certification service. Generally speaking, this approach has been adopted in most other jurisdictions taking a minimalist approach to electronic signatures, such as Australia;[218]

(*b*) *Standards of conduct and liability rules for certification services providers only.* Another approach is for the law to provide only for the liability of the certification services provider. This is the case under European Union directive 1999/93/EC on a Community framework for electronic signatures,[219] in which recital 22 states that "Certification-service-providers providing certification-services to the public are subject to national rules regarding liability", as outlined in article 6 of the directive. It is worth noting that article 6 applies only to "qualified signatures", which, for the time being, means PKI-based digital signatures only;[220]

(*c*) *Standards of conduct and liability rules for signatories and certification services providers.* In some jurisdictions, the law provides for the liability of the signatory and of the certification services provider, but does not establish a standard of care for the relying party. This is the case in China, under the Electronic Signatures Law of 2005. This is also the case in Singapore, under the Electronic Transactions Act, 1998;

(*d*) *Standards of conduct and liability rules for all parties.* Finally, the law may provide for standards of conduct and a basis for the liability of all parties involved. This approach is adopted in the UNCITRAL Model Law on Electronic Signatures, which indicates the duties relating to the conduct of the signatory (art. 8), of the certification services provider (art. 9) and of the relying party (art. 11). The Model Law can be said to set out criteria against which to assess the conduct of those parties. However, it leaves to the domestic law to determine the consequences of the inability to fulfil the various duties and the basis for the liability that may affect the various parties involved in the operation of electronic signature systems.

[217] United States Code, title 15, chapter 96, section 7031.

[218] It was felt, for example, that private law mechanisms admitted by Australian law, such as contractual exclusions, waivers and disclaimers of liability, and the limits posed to their operation by the common law, were better suited for regulating liability than statutory provisions (see Mark Sneddon, *Legal liability and e-Transactions: a Scoping Study for the National Electronic Authentication Council* (National Office for the Information Economy, Canberra, 2000) pp. 43-47, available at http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf (accessed on 6 June 2008)).

[219] *Official Journal of the European Communities*, L 13/12, 19 January 2000.

[220] Legislation adopted in the European Union follows this approach, for instance, the German law on electronic signature (SignaturGesetz – SigG) and the related ordinance (SigV), 2001, the Austrian Federal Electronic Signature Law (SigG) and the United Kingdom Electronic Signature Regulation 2002, section 4.

176. Differences in domestic liability regimes may be an obstacle to the cross-border recognition of electronic signatures. There are two main reasons for this. Firstly, certification services providers may be reluctant to recognize foreign certificates or the keys issued by foreign certification services providers whose liability or standards of care may be lower than their own. Secondly, users of electronic signature and authentication methods, too, may fear that lower liability limits or standards of care of a foreign certification services provider may limit the remedies available to them in case, for instance, of forgery or false reliance. For the same reasons, where the use of electronic signature and authentication methods, or the activities of certification services providers, is provided for by legislation, the law typically subjects recognition of foreign certificates or certification services providers to some assessment of substantive equivalence with the reliability offered by domestic certificates and certification services providers. The standards of care and levels of liability to which the various parties are subject constitute the main legal benchmark against which the equivalence is measured. Moreover, the ability of the certification services provider to limit or disclaim its liability will also have an impact on the level of equivalence afforded to its certificates.

1. Basis for liability in a public key infrastructure framework

177. Allocation of liability under a PKI framework is effected essentially in two ways: by means of contractual provisions or by the law (precedent, statute or both). The relations between the certification services provider and the signatory are typically of a contractual nature and, therefore, liability will typically be based on a breach of either party's contractual obligations. The relations between the signatory and the third party will depend on the nature of their dealing in any concrete instance. They may or may not be based on a contract. Lastly, the relations between the certification services provider and the relying third party would in most cases not be based on a contract.[221] Under most legal systems the basis of liability (whether contract or tort) will have extensive and significant consequences for the liability regime, in particular as regards the following elements: (*a*) the degree of fault that is required to engage a party's liability (in other words, what is the "standard of care" owed by one party to the other); (*b*) the parties that may claim damages and the extent of damages recoverable by them; and (*c*) whether and to what extent a party at fault is able to limit or disclaim its liability.

178. It flows from the above not only that the standards of liability will vary from one country to another, but also that within a given country they will vary depending on the nature of the relationship between the party held liable and the injured party. Furthermore, various legal rules and theories may have an impact on one or the other aspect

[221] Steffen Hindelang discussed in detail the possibility of creating a contractual relationship between the certification services provider and the third party under English law, coming to a negative conclusion ("No remedy for disappointed trust: the liability regime for certification authorities towards third parties outwith the EC Directive in England and Germany compared", *Journal of Information, Law and Technology*, No. 1, 2002, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/hindelang (accessed on 6 June 2008)). However, there are jurisdictions where a contractual relation might arise.

of liability under both a contractual or a common law or statutory liability regime, which sometimes lessens the differences between the two regimes. The present study cannot attempt to offer a complete detailed analysis of these general questions. It will instead focus on questions specifically raised in a PKI context and briefly discuss how domestic laws have approached them.

(a) Standard of care

179. Although different legal systems use different ranking systems and theories, for the purposes of this study it is assumed that the liability of the parties involved in a PKI framework would essentially be based on three possible standards: ordinary negligence or fault; presumed negligence (or fault with reversed burden of proof); and strict liability.[222]

(i) *Ordinary negligence*

180. Under this general standard, a person is legally required to compensate other people for the negative consequences of his or her actions, provided that the relationship to that other person is one that gives rise at law to a duty of care. Furthermore, the standard of care generally required is that of "reasonable care", which may be defined simply as the degree of care that a person of ordinary prudence, knowledge and foresight would exercise in the same or similar circumstances. In common law jurisdictions, this is often referred to as the "reasonable person" standard, whereas in several civil law jurisdictions it is often referred to as the "good family father" (*bonus pater familias*) standard. Viewed specifically from a business perspective, reasonable care refers to the degree of care that an ordinarily prudent and competent person engaged in the same line of business or endeavour would exercise under similar circumstances. Where liability is generally based on ordinary negligence, it is incumbent upon the injured party to demonstrate that the damage was caused by the other party's faulty breach of its obligations.

181. Reasonable care (or ordinary negligence) is the general standard of care contemplated in the UNCITRAL Model Law on Electronic Signatures. This standard of care applies to certification services providers in respect of issuance and revocation of certificates and disclosure of information.[223] A number of factors may be used in assessing compliance by the certification services provider with its general standard

[222] For the discussion of the liability system in this context, see Balboni, "Liability of certification service providers …", pp. 232 ff.

[223] Article 9, paragraph 1, of the Model Law states: "Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall: […] (*b*) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate; (*c*) Provide reasonably accessible means that enable a relying party to ascertain from the certificate: […]; (*d*) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise: […]."

of care.[224] The same standard also applies to signatories in respect of preventing unauthorized use and of safe-keeping of signature creation devices.[225] The Model Law extends the same general standard of reasonable care to the relying party, which is expected to take reasonable steps to verify both the reliability of an electronic signature and the validity, suspension or revocation of the certificate and to observe any limitation with respect to the certificate.[226]

182. A few countries, typically enacting States of the UNCITRAL Model Law on Electronic Commerce, have adopted the general standard of "reasonable care" for the conduct of the certification services provider.[227] In some countries, it appears that a certification services provider will "most likely be held to a general standard of reasonable care", although the fact that certification services providers, by their nature, will be parties with specialized skills in whom laypersons place trust beyond that extended to normal marketplace participants "may eventually give rise to professional status, or otherwise subject them to a higher duty of care to do what is reasonable given their specialized skills."[228] Indeed, as discussed below (see para. 189) this seems to be the situation in most countries.

183. As regards the signatory, some jurisdictions that have adopted the UNCITRAL Model Law on Electronic Signatures provide for a general standard of reasonable care.[229] In various countries the law includes a more or less extensive list of positive obligations without describing the standard of care or indicating the consequences

[224] *Model Law on Electronic Signatures …* Paragraph 146 of the Guide to Enactment states "In assessing the liability of the certification service provider, the following factors should be taken into account, inter alia: (*a*) The cost of obtaining the certificate; (*b*) The nature of the information being certified; (*c*) The existence and extent of any limitation on the purpose for which the certificate may be used; (*d*) The existence of any statement limiting the scope or extent of the liability of the certification service provider; and (*e*) Any contributory conduct by the relying party. In the preparation of the Model Law, it was generally agreed that, in determining the recoverable loss in the enacting State, weight should be given to the rules governing limitation of liability in the State where the certification service provider was established or in any other State whose law would be applicable under the relevant conflict-of-laws rule."

[225] Article 8 of the Model Law states: "Where signature creation data can be used to create a signature that has legal effect, each signatory shall: (*a*) Exercise reasonable care to avoid unauthorized use of its signature creation data; and (*b*) Without undue delay, utilize means made available by the certification service provider […], or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if: (i) The signatory knows that the signature creation data have been compromised; or (ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised." Further, the signatory must "exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate".

[226] Article 11, subparagraphs (*a*), (*b*) (i) and (*b*) (ii).

[227] For example, the Cayman Islands, Electronic Transactions Law, 2000, section 28; and Thailand, Electronic Transactions Act (2001), section 28.

[228] "Certification authority: liability issues", prepared for the American Bankers Association by Thomas J. Smedinghoff, February 1998, section 1.1, available at http://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf (accessed on 6 June 2008).

[229] For example, Thailand, Electronic Transactions Act (2001), section 27.

of failure to comply with those obligations.[230] In some countries, however, the law expressly complements the list of obligations with a general declaration of liability of the signatory for his or her breach,[231] which in one case is even of a criminal nature.[232] Arguably, there may not be a single standard of care, but a staggered system, with a general standard of reasonable care as a default rule for the signatory's obligations, which is however raised to a warranty standard in respect of some specific obligations, typically those that relate to accuracy and truthfulness of representations made.[233]

184. The situation of the relying party is a peculiar one, because it is unlikely that either the signatory or the certification services provider could be damaged by an act or omission of the relying party. In most circumstances, if the relying party fails to exercise the requisite degree of care, he or she would bear the consequences of his or her actions, but would not incur any liability towards the certification services provider. It is not surprising, therefore, that, when addressing the role of relying parties, domestic laws on electronic signatures seldom provide more than a general list of basic duties of the relying party. This is generally the case in jurisdictions that have adopted the UNCITRAL Model Law on Electronic Signatures, which recommends a standard of reasonable care in relation to the conduct of the relying party.[234] In some cases, however, this requirement is not expressly stated.[235] It should be noted that the express or implied duties of the relying party are not irrelevant for the certification services provider. Indeed, a breach by the relying party of its duty of care may provide

[230] For example, Argentina, *Ley de firma digital (2001)*, article 25; Cayman Islands, Electronic Transactions Law, 2000, section 31; Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 24; Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 17; India, Information Technology Act, 2000, sections 40-42; Mauritius, Electronic Transactions Act 2000, articles 33-36; Peru, *Ley de firmas y certificados digitales*, article 17; Turkey, Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (2005), article 15; Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 21; and Venezuela (Bolivarian Republic of), *Ley sobre mensajes de datos y firmas electrónicas*, article 19.

[231] China, Electronic Signatures Law, promulgated 2004, article 27; Colombia, *Ley 527 sobre comercio electrónico*, article 40; Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, articles 53 and 55; Panama, *Ley de firma digital (2001)*, articles 37 and 39; Russian Federation, *Federal Law on Electronic Digital Signature (2002)*, clause 12; Venezuela (Bolivarian Republic of), *Ley sobre mensajes de datos y firmas electrónicas*, article 19; and Viet Nam, *Law on Electronic Transactions*, article 25.

[232] Pakistan, Electronic Transactions Ordinance, 2002, section 34.

[233] For example, Singapore, Electronic Transactions Act (chapter 88). Section 37, paragraph 2, of the Act provides that by accepting a certificate the signatory certifies to all who reasonably rely on the information contained in the certificate that (*a*) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate; (*b*) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and (*c*) all information in the certificate that is within the knowledge of the subscriber is true. Section 39, paragraph 1, in turn only contemplates a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such certificate and prevent its disclosure to a person not authorized to create the subscriber's digital signature. This seems also to be the case in the Bolivarian Republic of Venezuela, where article 19 of the *Ley sobre mensajes de datos y firmas electrónicas* expressly qualifies the obligation to avoid unauthorized use of the signature creation device as one of "due diligence", whereas other obligations are expressed in categorical terms.

[234] Cayman Islands, Electronic Transactions Law, 2000, section 21; Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 107; and Thailand, Electronic Transactions Act (2001), section 30.

[235] Turkey, Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (2005), article 16; and Viet Nam, Law on Electronic Transactions, article 26.

the certification services provider with a defence against liability claims by a relying party, for example, when the certification services provider can show that the damage sustained by the relying party could have been avoided or mitigated had the relying party taken reasonable measures to ascertain the validity of the certificate or the purposes for which it could be used.

(ii) *Presumed negligence*

185. The second possibility is a fault-based system with a reversed burden of proof. Under this system, a party's fault is presumed whenever damage has resulted from an act attributable to it. The rationale for such a system is generally the assumption that, under certain circumstances, damage could in the normal course of events only have occurred because a party failed to comply with its obligations or abide by a standard of conduct expected from it.

186. In civil law, presumed fault may occur in connection with liability for breach of contract,[236] and also for various instances of tort liability. Examples include vicarious liability for the acts of employees, agents, infants or animals, liability arising in the course of some commercial or industrial activity (environmental damage, damage to adjacent property, transportation accidents). The theories justifying the reversal of the burden of proof and the particular instances in which it is admitted vary from country to country.

187. In practice, such a system leads to a result similar to the enhanced standard of care that is expected from professionals under common law. Professionals must have a minimum amount of special knowledge and skills necessary to act as a member of the profession and have a duty to act as a reasonable member of the profession would in a given circumstance.[237] This does not necessarily mean that the burden of proof is reversed, but the higher standard of care expected from the professional means in practice that professionals are deemed to be capable of avoiding doing harm to persons that hire their services or whose welfare is otherwise entrusted to them if they act according to those standards. Under certain circumstances, however, the so-called

[236] Section 280, paragraph 1, of the Civil Code of Germany, for instance, declares the debtor liable for damage arising out of the breach of a contractual obligation unless the debtor is not responsible for the breach. Article 97, paragraph 1, of the Code of Obligations of Switzerland states this principle in even clearer terms: if the creditor does not obtain performance, the debtor is liable to compensate the resulting damage unless it can prove that the failure to perform was not attributable to its own fault. A similar rule is contained in article 1218 of the Civil Code of Italy. Under French law, negligence is always presumed if the contract involved a promise of a certain result, but negligence must be established where the object of the contract was to offer a standard of performance, rather than a specific result (see Gérard Légier, "Responsabilité contractuelle", *Répertoire de droit civil Dalloz*, Nos. 58-68, August 1989).

[237] W. Page Keeton and others, *Prosser and Keeton on the Law of Torts*, 5th ed. (Saint Paul, Minnesota, West Publishing, 1984), section 32, p. 187.

res ipsa loquitur doctrine allows courts to presume, absent proof to the contrary, that the occurrence of damage in the "ordinary course of things" is only possible due to a person's failure to exercise reasonable care.[238]

188. If this rule is applied to the activities of certification services providers, it would mean that whenever a relying party or a signatory sustains damage as a result of using an electronic signature or certificate, and that damage can be attributed to a failure by the certification services provider to act in accordance with its contractual or statutory obligations, the certification services provider is presumed to have been negligent.

189. Presumed negligence seems to be the prevailing standard used under domestic laws. Under the European Union directive on electronic signatures, for example, the certification services provider is liable for damages towards any entity that reasonably relies on the qualified certificate unless the certification services provider proves that it has not acted negligently.[239] In other words, the certification services provider's liability is based on negligence with a reversal of the burden of proof: the certification services provider must prove that its actions were not negligent, since it is in the best position to do so, having the technical skills and access to the relevant information (both of which signatories and relying third parties might not possess).

190. This is also the case under various domestic laws outside the European Union that provide for an extensive list of duties to be observed by certification services providers, which generally subject them to liability for any loss caused by their failure to comply with their statutory obligations.[240] It is not altogether clear whether all of these

[238] "There must be reasonable evidence of negligence. But where the thing is shown to be under the management of the defendant or his servants, and the accident is such, as in the ordinary course of things, that it does not happen if those who have the management use proper care, it affords reasonable evidence, in the absence of explanation by the defendants, that the accident arose from want of care." (C. J. Erle in Scott v. *The London and St. Katherine's Docks Co.*, Ex. Ch., 3 H & C 596, 601, 159 Eng. Rep. 665, 667 (1865)).

[239] *Official Journal of the European Communities*, L 13/12, 19 January 2001. Article 6 of the directive provides a minimum standard of liability. It would be possible for enacting States to strengthen the liability of the certification services provider, for instance by introducing a strict liability regime or extending liability also to non-qualified certificates. However, this has not happened so far and is unlikely to happen since it would place the certification services providers of one country in a disadvantaged position with respect to other European Union certification services providers (Balboni "Liability of certification service providers …", p. 222).

[240] Argentina, *Ley de firma digital (2001)*, article 38; Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 14; Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 31; Panama, *Ley de firma digital (2001)*, article 51; and Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 22.

laws actually reverse the burden of proof, but several do provide quite explicitly for such a reversal, either generally[241] or in relation to specific obligations.[242]

191. The preference for a system of presumed fault is arguably the result of concerns that liability based on ordinary negligence would not be fair to the relying party, which may lack the technological knowledge, as well as the access to relevant information, to satisfy the burden of showing the certification services provider's negligence.

(iii) *Strict liability*

192. Strict liability or "objective liability" is a rule used in various legal systems to attach liability to a person (typically manufacturers or operators of potentially dangerous or harmful products or equipment) without a finding of fault or breach of a duty of care. The person is held to be liable simply for placing a defective product on the market or for the malfunctioning of a piece of equipment. Since liability is assumed from the mere fact that loss or damage has occurred, the individual legal elements required to establish an action such as negligence, breach of a warranty or intentional conduct need not be established.

193. Strict liability is an exceptional rule under most legal systems and is ordinarily not presumed, absent clear statutory language. In the context of electronic signature and authentication methods, strict liability might impose an excessive burden on the certification services provider, which, in turn, might hinder the commercial viability of the industry at an early stage of its development. At present, no country appears to impose strict liability on either the certification services provider or any other parties involved in the electronic signature process. It is true that in countries that provide for a catalogue of positive obligations for certification services providers, the standard of care for certification services providers is typically very high, approaching in some cases a strict liability regime, but the certification services provider can still be released from liability if it can show that it acted with the required diligence.[243]

[241] China, Electronic Signatures Law, promulgated 2004, article 28: "If an electronic signatory or a person who relies on an electronic signature incurs a loss as a result of relying on the electronic signature certification service provided by an electronic certification service provider while engaging in civil activities, and if the electronic certification service provider fails to provide evidence that the provider was not at fault, then the electronic certification service provider shall bear liability for damages"; see also Turkey, Electronic Signature Law 2004, article 13: "Electronic Certificate Service Providers shall be liable for compensation for damages suffered by third parties as a result of infringing the provisions of this Law or the ordinances published in accordance with this Law. Liability of compensation shall not occur if the Electronic Certificate Service Provider proves the absence of negligence."

[242] "An authorized certification service provider is not liable for errors in the information in an accredited certificate where (*a*) the information was provided by or on behalf of the person identified in the accredited certificate; and (*b*) the certification service provider can demonstrate that he has taken all reasonably practical measures to verify that information" (Barbados, chapter 308B, Electronic Transactions Act (1998), section 20); see also Bermuda, Electronic Transactions Act, 1999, section 23, paragraph 2 (*b*).

[243] For example, in Chile, Ecuador and Panama.

(b) Parties entitled to claim damages and extent of damages recoverable

194. One important issue in determining the extent of liability of certification services providers and signatories concerns the group of persons that might be entitled to claim compensation for damage caused by a breach by either party of its contractual or statutory obligations. Another related matter is the extent of the obligation to compensate and the types of damage that should be recompensed.

195. Contractual liability generally follows upon the breach of a contractual obligation. In a PKI context, a contract would usually exist between the signatory and the certification services provider. The consequences of breaches by one party of its contractual obligations to another party are determined by the words of the contract, as governed by applicable laws of contract. For electronic signatures and certificates, liability outside a clearly defined contractual relationship would typically arise in situations where a person has sustained damage in reasonable reliance on information provided either by the certification services provider or the signatory, which has turned out to be false or inaccurate. Normally, the relying third party does not enter into a contract with the certification services provider and probably does not interact with the certification services provider at all, except for relying on the certification. This may give rise to difficult questions not entirely answered in some jurisdictions.

196. Under most civil law systems, it could be assumed that a certification services provider would be liable for loss sustained by the relying party as a result of reliance on inaccurate or false information even without specific provisions to that effect in specific legislation dealing with electronic signatures. In several jurisdictions, this liability may follow from the general tort liability provision that has been introduced into most civil law codifications,[244] with few exceptions.[245] In some jurisdictions, an analogy could be drawn between the activities of a certification services provider and notaries public, who are generally held liable for damage caused by negligence in the performance of their duties.

197. In common law jurisdictions, however, the situation may not be so clear. Where a tort is committed in the performance of acts governed by a contract, common law jurisdictions have traditionally required some privity of contract between the tortfeasor and the injured party. Since the relying third party does not enter into a contract with the certification services provider and probably does not interact with the certification services provider at all, except for relying on the false certification, it may be difficult in some common law jurisdictions (absent an explicit statutory provision)

[244] Article 1382 of the Civil Code of France provides that whatever human act that causes damage to someone else obliges the one by whose fault it occurred to compensate it. This general liability rule has inspired similar provisions in various other countries, such as article 2043 of the Civil Code of Italy and article 483 of the Civil Code of Portugal.

[245] The Civil Code of Germany contains three general provisions (sections 823 I, 823 II and 826) and a few specific rules dealing with a number of rather narrowly defined tortuous situations. The main provision is section 823 I, which differs from the French Code to the extent that it expressly refers to injury to someone else's life, body, health, freedom, property or another right.

for the relying party to establish a cause of action against the certification services provider.[246] If there is no privity of contract, a cause of action at tort under the common law would require a showing of a breach of a duty of care owed by the tortfeasor to the injured party. Whether or not for the certification services provider such a duty exists in respect of all possible relying parties is not entirely clear. Generally, the common law is reluctant to subject a person to "liability in an indeterminate amount, for an indeterminate time, to an indeterminate class"[247] for negligent misrepresentation unless the negligent words "are uttered directly, with knowledge or notice that they will be acted on, to one to whom the speaker is bound by some relation of duty, arising out of public calling, contract or otherwise, to act with care if he acts at all".[248]

198. In this case, the issue at stake is to determine what is the spectrum of persons to whom a certification services provider (or the signatory for that matter) would owe a duty of care. There are basically three standards that may be used to define the spectrum of persons who in such a situation may validly assert claims against the certification services provider:[249]

(*a*) *Foreseeability standard.* This is the broadest standard of liability. Under this standard, the signatory or the certification services provider will be liable to any person for whom reliance on the false representations was reasonably foreseeable;

(*b*) *Standard based on intent and knowledge.* This is a narrower standard that limits liability to loss suffered by a member of the group of persons for whose benefit and guidance one intends to supply information or knows that the recipient intends to supply it;

(*c*) *Privity standard.* This is the most limited standard, creating a duty owed solely to the client, or one with whom the information provider had specific contact.

199. The UNCITRAL Model Law on Electronic Signatures does not attempt to circumscribe the universe of persons who may fall under the category of "relying parties", which could include "any person having or not a contractual relationship with the signatory or the certification services provider."[250] Similarly, under the European Union directive on electronic signatures, the certification services provider is liable for damages towards "any entity or legal or natural person who reasonably relies"

[246] For instance, for English common law, an author concludes that "in the absence of legislation, [the certification services provider]'s liability to [the third party] is far from certain, yet [the third party] foreseeably suffers loss as a result of her negligence. Moreover, it is difficult to see how [the third party] can protect itself. If there is no liability, there is at least an arguable lacuna, and negligence on the part of the [certification services provider], in particular, creates a clear lacuna. The common law might fill lacunae, but the process is uncertain and unreliable" (Paul Todd, E-Commerce Law (Abingdon, Oxon, Cavendish Publishing Limited, 2005), pp. 149-150). Similar conclusions were reached for Australian law; see Sneddon, *Legal liability and e-transactions* ..., p. 15.

[247] Judge Cardozo in *Ultramares Corporation v. George A. Touche et al*, Court of Appeals of New York, 6 January 1931, 174 N.E. 441, p. 445.

[248] Judge Cardozo in *Ultramares Corporation v. George A. Touche et al* ..., p. 447.

[249] Smedinghoff, "Certification authority: liability issues" ..., sect. 4.3.1.

[250] *UNCITRAL Model Law on Electronic Signatures* ..., para. 150.

on the qualified certificate. The European Union directive is clearly built around a PKI scheme, since it applies only in cases of digital signatures (qualified certificates). The notion of entity is usually interpreted as referring to third relying parties, and the directive has been implemented by all but two European Union member States in that sense.[251]

200. Like the UNCITRAL Model Law on Electronic Signatures, the European Union directive on electronic signatures does not narrow down the categories of persons that may qualify as relying parties. It has therefore been suggested that, even under common law, "in the provision of certification services it is self-evident that a certification service provider owes a duty of care towards anyone who may rely upon their certificate in deciding to accept a particular electronic signature in a particular transaction, since the very purpose for which the certificate was issued is to encourage such reliance."[252]

201. Another point of interest concerns the nature of loss recoverable from a signatory or certification services provider. For instance, in some common law jurisdictions, claims for purely economic losses for product defects are not recoverable in tort. However, cases of intentional fraud, or in some jurisdictions even negligent misrepresentation, are regarded as exceptions to the economic loss rule.[253] It is interesting to note, in that connection, that the United Kingdom Electronic Signatures Regulations 2002 did not reproduce the provisions on liability of the European Union directive on electronic signatures. Therefore, standard rules on liability apply, which, in this case, relate to the test of the proximity of the damage.[254] The amount of damages recoverable is typically left for general contract or tort law. Some laws expressly require certification services providers to purchase liability insurance or otherwise make public to all potential signatories, among other information, the financial guaranties for its possible liability.[255]

(c) Ability to contractually limit or disclaim liability

202. Certification services providers are expected to seek routinely as much as possible to limit their contractual and tort liability towards the signatory and relying parties. As far as the signatory is concerned, limitation clauses will typically be contained in elements of the contract documentation, such as certification practice statements. Such statements may impose a cap on the liability per incident, per series of incidents or per period of time and may exclude certain classes of damages.

[251] The exceptions being Denmark and Hungary (Balboni, "Liability of certification service providers …", p. 220.

[252] Lorna Brazell, *Electronic Signatures: Law and Regulation* (London, Sweet and Maxwell, 2004), p. 187.

[253] Smedinghoff, "Certification authority: liability issues" …, section 4.5.

[254] Dumortier and others, "The legal and market aspects of electronic signatures" …, p. 215.

[255] Turkey, Electronic Signature Law, 2004, article 13; and Argentina, *Ley de firma digital (2001)*, article 21 (*a*) (1); see also Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 104 (III).

Another technique would be the inclusion in certificates of the maximum amount of the value of the transaction for which the certificate may be used, or restrict the use of the certificate to certain purposes only.[256]

203. While most legal systems generally recognize the right of contract parties to limit or exclude liability through contractual provisions, this right is usually subject to various limitations and conditions. In most civil law jurisdictions, for instance, a total exclusion of liability for a person's own fault is not admissible[257] or is subject to clear limitations.[258] Moreover, if the terms of the contract are not freely negotiated, but rather are imposed or pre-established by one of the parties ("adhesion contracts"), some types of limitation clauses may be found to be "abusive" and therefore invalid.

204. In common law jurisdictions a similar result may flow from various theories. In the United States, for instance, courts generally will not enforce contract provisions found to be "unconscionable". Although this concept usually depends on a determination of the particular circumstances of the case, it generally refers to contract terms "which no man in his senses, not under delusion would make, on the one hand, and which no fair and honest man would accept on the other"[259] and that are characterized by "an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favourable to the other party".[260] Similarly to the civil law notion of "contract of adhesion", the doctrine has been applied to prevent instances of "commercial sharp practices" by parties with superior bargaining power.[261] Not every contract term that comes about this way is invalid. However, although courts generally enforce standard form or adhesion contracts where there is no ability to bargain regarding the terms, even in consumer contracts, sometimes a court will decline to enforce a clause in a standard contract if its insertion amounts to unfair surprise.[262]

[256] See Smedinghoff, "Certification authority: liability issues" …, section 5.2.5.4; and Hindelang, "No remedy for disappointed trust …", section 4.1.1.

[257] In France, it is in principle possible to exclude liability arising out of a breach of contract. In practice, however, courts tend to invalidate such clauses whenever it is found that the clause would release the party from the consequences of a breach of a "fundamental" contractual obligation (see Légier, "Responsabilité contractuelle" …, Nos. 262 and 263).

[258] In most civil law countries, the law prohibits the disclaimer of liability arising out of gross negligence or violation of duty imposed by a rule of public policy. Some countries have explicit rules to this effect, such as article 100 II of the Code of Obligations of Switzerland and article 1229 of the Civil Code of Italy. Other countries, such as Portugal, do not have a similar statutory rule, but achieve essentially the same result as Italy (see António Pinto Monteiro, *Cláusulas Limitativas e de Exclusão de Responsabilidade Civil* (Coimbra, Faculdade de Direito de Coimbra, 1985), p. 217.

[259] *First Financial Ins. Co. v. Purolator Security, Inc.*, 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), citing Hume v. U.S., 132 U.S. 406, 410 (1975), cited in Smedinghoff, "Certification authority: liability issues" …, section 5.2.5.4.

[260] *First Financial Ins. Co. v. Purolator Security, Inc.* …, citing *Williams v. Walker-Thomas Furniture Co.*, 350 F.2d 315, 320 (D.C. 1965), cited in Smedinghoff, "Certification authority: liability issues" …, section 5.2.5.4.

[261] *First Financial Ins. Co. v. Purolator Security, Inc.*, 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), cited in Smedinghoff, "Certification authority: liability issues" …, section 5.2.5.4.

[262] Raymond T. Nimmer, *Information Law*, section 11.12[4][a], at 11-37, cited in Smedinghoff, "Certification authority: liability issues" …, section 5.2.5.4.

205. Lastly, in both civil law and common law systems, consumer protection rules may significantly reduce the ability of a certification services provider to limit its liability vis-à-vis the signatory, in circumstances where the limitation of liability would effectively deprive the signatory of a right or remedy recognized by the applicable law.

206. The possibility for the certification services provider to limit its potential liability vis-à-vis the relying party would in most cases be subject to even greater restrictions. Apart from closed business models where a relying party would be required to adhere to contract terms,[263] quite often the relying party will not be bound by contract to the certification services provider or even the signatory. Thus, to the extent that the relying party might have a claim at tort against the certification services provider or the signatory, those parties might have no means of effectively limiting their liability, since under most legal systems this would require giving the relying party adequate notice of the limitation of liability. Lack of knowledge of the identity of the relying party prior to the occurrence of the damage may prevent the certification services provider (and arguably even more so, the signatory) from putting in place an effective system for limiting its liability. This problem is typical of open systems where strangers interact with no prior contact and leaves the signatory exposed to potentially devastating consequences.[264] This situation was felt by many, in particular representatives of the certification industry, to be a major impediment to wider use of electronic signature and authentication methods, given the difficulty for certification services providers to assess their exposure to liability.

207. The desire to clarify the law on this aspect has led a number of countries to expressly recognize the right of certification services providers to limit their liability. The European Union directive on electronic signatures, for example, obliges European Union member States to ensure that a certification services provider may indicate in a qualified certificate "limitations on the use of that certificate" as long the limitations "are recognizable to third parties".[265] These limitations may be typically of two categories: there may be limits on the types of transaction for which particular certificates or classes of certificates may be used; there may also be limits on the value of the transactions in connection with which the certificate or class of certificates may be used. Under either hypothesis, the certification services provider is expressly exempted from liability "for damage arising from use of a qualified certificate that exceeds the limitations placed on it".[266] Furthermore, the European Union directive on electronic signatures mandates European Union member States to ensure that a certification services provider "may indicate in the qualified certificate a limit on the value of transactions

[263] Such as envisaged for the E-Authentication Federation administered by the General Services Administration of the United States Government (see E-Authentication Federation, Interim Legal Document Suite, version 4.0.7, available at http://www.cio.gov/eauthentication/documents/LegalSuite.pdf (accessed on 6 June 2008)).

[264] Sneddon, "*Legal liability and e-transactions ...*", p. 18.

[265] European Union directive on electronic signatures, article 6, paragraph 3.

[266] European Union directive on electronic signatures ….

for which the certificate can be used, provided that the limit is recognizable to third parties".[267] In such a case the certification services provider shall not be liable for damage resulting from this maximum limit being exceeded.[268]

208. The European Union directive on electronic signatures does not establish a cap for the liability that the certification services provider may incur. However, the directive does allow a certification services provider to limit the maximum value per transaction for which certificates may be used, exempting the certification services provider from liability exceeding that value cap.[269] As a matter of business practice, certification services providers also often introduce an overall cap to their liability, on a contractual basis.

209. Several other domestic laws support those contractual practices by recognizing a limit on the liability of the certification services provider towards any potentially affected party. Typically, these laws allow limitations as specified in the certificate practice statement of the certification services provider, and in some cases expressly exempt the certification services provider from liability where a certificate was used for a purpose different from the one for which it was issued.[270] Furthermore, some laws recognize the right of certification services providers to issue certificates of different classes and to establish different recommended levels of reliance,[271] which typically provide different levels of limitation (and of security) depending on the fee paid. However, some laws expressly prohibit any limitations of liability other than as a result of limitations on the use or value of certificates.[272]

210. Countries that have adopted a minimalist approach have, in turn, regarded legislative intervention as generally undesirable and have preferred to leave the matter for the parties to regulate by contract.[273]

[267] European Union directive on electronic signatures, article 6, paragraph 4.

[268] European Union directive on electronic signatures ….

[269] Dumortier and others, "The legal and market aspects of electronic signatures" …, p. 55; see also Hindelang, "No remedy for disappointed trust …", section 4.1.1; Balboni ("Liability of certification service providers …", p. 230) goes further by stating that "by article 6 (4), it is only possible to limit the value of the transaction […], which has nothing to do with a limitation of the potential amount of damage that can arise from that transaction".

[270] Argentina, *Ley de firma digital (2001)*, article 39; Barbados, chapter 308B, Electronic Transactions Act (1998), section 20, paragraphs 3 and 4; Bermuda, Electronic Transactions Act, 1999, section 23, paragraphs 3 and 4; Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 14; and Viet Nam, Law on Electronic Transactions, article 29, paragraphs 7 and 8 (the latter however without express exemption of liability).

[271] Singapore, Electronic Transactions Act (chapter 88) 1998, sections 44 and 45; and Mauritius, Electronic Transactions Act 2000, articles 38 and 39.

[272] Turkey, Electronic Signature Law, 2004, article 13.

[273] See, for Australia, Sneddon, *Legal liability and e-transactions* …, pp. 44-47; and for the United States, Smedinghoff, "Certification authority: liability issues" …, section 5.2.51.

2. Particular instances of liability in a public key infrastructure framework

211. The main focus of discussions concerning liability in connection with the use of electronic signature and authentication methods has been the basis and characteristics of the liability of certification services providers. It is generally accepted that the basic duty of a certification services provider is to utilize trustworthy systems, procedures and human resources and to act in accordance with representations that the certification services provider makes with respect to its policies and practices.[274] In addition, the certification services provider is expected to exercise reasonable care to ensure the accuracy and completeness of all material representations it makes in connection with a certificate. All these activities may expose a certification services provider to a varying degree of liability, depending on the applicable law. The following paragraphs identify the instances that carry a greater risk for a certification services provider of being exposed to liability and summarize the way in which domestic laws deal with such liability.

(a) Failure to issue or delay in issuing a certificate

212. A certification services provider typically issues certificates upon application by candidate signatories. If an application meets the certification services provider's criteria, the certification services provider may issue a certificate. It is conceivable that an applicant might meet the criteria but nevertheless be rejected or delayed, either because the certification services provider simply makes a mistake, or because the certification services provider's application facilities are unavailable by design or accident, or because the certification services provider, for ulterior motives, wishes to delay or deny issuance of a certificate to the applicant. Applicants rejected or delayed under these circumstances may have a claim against the certification services provider.[275]

213. If there is a competitive market for certification services, there might be no real harm to an applicant if a certification services provider were to refuse to issue a certificate, either by accident or on purpose. However, in the absence of meaningful competition, a certification services provider's refusal to issue a certificate or delay in issuing a certificate could cause serious harm where the rejected applicant is unable to engage in a particular business without the certificate. Even if competitive alternatives were available, one could envision transaction-specific losses arising from circumstances where a certificate was requested in connection with a particular transaction and, as a result of delay or denial, the certificate was not available in time for the intended transaction, forcing the applicant to forgo the valuable transaction.[276]

[274] UNCITRAL Model Law on Electronic Signatures …, article 9, subparagraphs 1 (*a*) and 1 (*b*).

[275] Smedinghoff, "Certification authority: liability issues" …, section 3.2.1.

[276] Smedinghoff, "Certification authority: liability issues" …, section 3.2.1.

214. This kind of scenario is unlikely to arise in an international context, since most signatories would be more likely to seek the services of certification services providers located in their own countries.

(b) Negligence when issuing a certificate

215. The principal function of a certificate is to bind an identity of the signatory to a public key. Accordingly, the principal task of a certification services provider is to verify, in conformance with its stated practices, that an applicant is the purported signatory and is in control of the private key corresponding to the public key listed in the certificate. Failure to do so may expose the certification services provider to potential liability to the signatory, or to a third party that relies on the certificate.

216. Damage to the signatory might be caused, for example, by the erroneous issuance of a certificate to an impostor using a misappropriated identity. The certification services provider's own employees or contractors might conspire to issue erroneous certificates using the certification services provider's signing key against improper applications by the impostor. Those persons might negligently issue an erroneous certificate, either by failing to perform properly the certification services provider's stated validation procedures in reviewing the impostor's application, or by using the certification services provider's signing key to create a certificate that has not been approved. Lastly, a malefactor might impersonate a signatory using forged, but seemingly authentic, identification documents, and convince the certification services provider, despite careful and non-negligent adherence to its published policies, to issue a certificate to the impostor.[277]

217. Erroneous issuance to an impostor could have very serious consequences. Relying parties who conduct online transactions with the impostor may rely on the incorrect data in the erroneously issued certificate and, as a result of that reliance, ship goods, transfer funds, extend credit or undertake other transactions with the expectation that they are dealing with the impersonated party. When the fraud is discovered, the relying parties may have suffered substantial loss. In this situation, there are two injured parties: the relying party who was defrauded by the erroneously issued certificate, and the person whose identity was impersonated in the erroneously issued certificate. Both will have claims against the certification services provider. Another scenario might be the negligent issuance of a certificate to a fictitious person, in which case only the relying party would suffer damage.[278]

218. Article 9 of the UNCITRAL Model Law on Electronic Signatures provides, inter alia, that a certification services provider shall exercise reasonable care to ensure

[277] Smedinghoff, "Certification authority: liability issues" …, section 3.2.1.

[278] Smedinghoff, "Certification authority: liability issues" …, section 3.2.1.

the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate. This general duty has been literally transposed into the domestic legislation of several countries implementing the Model Law,[279] although in some countries the standard seems to have been raised from reasonable care to a higher warranty standard.[280]

219. The regime established by the European Union directive on electronic signatures obliges European Union member States, as "a minimum", to ensure that by issuing a certificate as a qualified certificate to the public, or by guaranteeing such a certificate to the public, a certification services provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate: (*a*) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate; (*b*) for assurance that, at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate; (*c*) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification services provider generates them both; unless the certification services provider proves that he has not acted negligently.[281]

220. Other domestic laws generally coincide in imposing on certification services providers the obligation to verify the accuracy of the information on the basis of which a certificate is issued. In some countries, a certification services provider is generally held liable to any person who reasonably relied on the certificate for the accuracy of all information in the accredited certificate as from the date on which it was issued,[282] or guarantees its accuracy,[283] although in some of those countries the certification services provider may qualify this warranty by an appropriate statement in the certificate.[284] Some laws, however, expressly exempt the certification services provider from liability for inaccurate signatory-provided information, subject to verification according to the certificate practice statement, provided that the certification services provider can prove that it took all reasonable measures to verify the information.[285]

[279] For example, Thailand, Electronic Transactions Act (2001), section 28, paragraph 2; and Cayman Islands (British overseas territory), Electronic Transactions Law, 2000, section 28 (*b*).

[280] For example, China, Electronic Signatures Law, article 22: "Electronic certification service providers shall ensure that the contents of electronic signature certificates are complete and accurate during their valid term, and shall ensure that parties relying on electronic signatures can verify or comprehend all of the recorded contents of electronic signature certificates and other relevant matters", emphasis added.

[281] European Union directive on electronic signatures …, article 6, paragraph 1.

[282] Barbados, chapter 308B, Electronic Transactions Act (1998), section 20, paragraph 1 (*a*); Bermuda, Electronic Transactions Act, 1999, section 23; Hong Kong SAR of China, Electronic Transactions Ordinance, section 39; India, Information Technology Act, 2000, section 36 (*e*); Mauritius, Electronic Transactions Act 2000, section 27, paragraph 2 (*d*); and Singapore, Electronic Transactions Act, sections 29, subsection (2) (*a*) and (*c*), and 30, subsection (1).

[283] Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 18; and Viet Nam, *Law on Electronic Transactions*, article 31 (*d*).

[284] For example, Barbados, Bermuda, Hong Kong SAR of China, Mauritius and Singapore.

[285] Argentina, *Ley de firma digital (2001)*, article 39 (*c*).

221. In other countries the same result is achieved not by a statutory warranty, but by imposing on certification services providers a general duty to verify the information supplied by the signatory before issuing a certificate,[286] or to establish systems for verifying such information.[287] In some cases, there is an obligation to revoke a certificate immediately upon finding out that information on which the certificate was issued was inaccurate or false.[288] In a few cases, however, the law is silent about the issuance of certificates, merely requiring the certification services provider to comply with its certification practice statement[289] or to issue the certificate as agreed with the signatory.[290] This does not mean that the law does not contemplate any liability for certification services providers. On the contrary, some laws clearly contemplate certification services provider liability, by requiring the certification services provider to purchase adequate third-party liability insurance covering all contractual and extra-contractual damage caused to signatories and third parties.[291]

222. The certification services provider's duty to verify the accuracy of the information that is provided is supplemented by a duty of the signatory to "exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate".[292] The signatory could therefore be held liable, either to the certification services provider or to the relying party, for providing false or inaccurate information to the certification services provider when applying for a certificate. Sometimes this is formulated as a general duty to provide accurate information to the certification services provider,[293] or to exercise reasonable care to ensure the correctness of the information;[294] sometimes the signatory is expressly declared liable for damages resulting from its failure to comply with this particular requirement.[295]

[286] Argentina, *Ley de firma digital (2001)*, article 21 (*o*); Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*, article 12 (*e*); Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 104 (I); and Venezuela (Bolivarian Republic of), *Ley sobre mensajes de datos y firmas electrónicas*, article 35.

[287] Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 30 (*d*).

[288] Argentina, *Ley de firma digital (2001)*, article 19 (*e*) (2).

[289] Peru, Decreto reglamentario de la ley de firmas y certificados digitales, article 29 (*a*).

[290] Colombia, *Ley 527 sobre comercio electrónico*, article 32 (*a*); Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 40 (*a*); and Panama, *Ley firma digital (2001)*, article 49, paragraph 7.

[291] Bolivarian Republic of Venezuela, *Ley sobre mensajes de datos y firmas electrónicas*, article 32.

[292] UNCITRAL Model Law on Electronic Signatures …, article 8, subparagraph 1 (*c*).

[293] Argentina, *Ley de firma digital (2001)*, article 25; Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 24; and Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99 (III).

[294] Cayman Islands, Electronic Transactions Law 2000, section 31 (*c*).

[295] Colombia, *Ley 527 sobre comercio electrónico*, article 40; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 55; Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99 (III); and Panama, *Ley de firma digital (2001)*, article 39.

(c) Unauthorized use of signature or compromised certificate practice statement

223. There are two aspects of unauthorized use of signature creation devices and certificates. On the one hand, a signature creation device might not be properly kept or be otherwise compromised, for instance by misappropriation by an agent of the signatory. On the other hand, the actual signing hierarchy of the certification services provider might be compromised, for instance if either the certification services provider's own signing key or the root key are lost, or disclosed to or used by unauthorized persons, or otherwise compromised.

224. The signing hierarchy might be compromised in various ways. The certification services provider or one of its employees or contractors might accidentally destroy or lose control of the key, the data centre that held the private key might be damaged by an accident, or the certification services provider's key might be destroyed intentionally or compromised by someone for unlawful purposes (e.g. a hacker). The consequences of a compromise of the signing hierarchy could be very serious. For instance, if either the private signing key or the root keys were to fall into the hands of a malefactor, that person could generate false certificates and use them to impersonate real or fictitious signatories, to the detriment of relying parties. Furthermore, once the damage was discovered, all certificates issued by the certification services provider would need to be revoked, resulting in a potentially massive claim by the entire signatory community for loss of use.

225. This matter is not dealt with in detail in the UNCITRAL Model Law on Electronic Signatures. Arguably, the general obligation of the certification services provider under the Model Law to "use trustworthy systems, procedures and human resources"[296] could be construed as imposing a duty on a certification services provider to take all necessary measures to prevent its own key (and thereby its entire signing hierarchy) from being compromised. Several domestic laws explicitly provide for such an obligation, often combined with the certification services provider's obligation to utilize trustworthy systems.[297] Sometimes there is a specific duty to take measures to avoid forgery of certificates.[298] A certification services provider is under a duty to refrain from creating or accessing the signature creation data of the signatories, and may be liable for acts of its employees who deliberately do so.[299] A certification services provider would be placed under a duty to request the revocation of its own certificate, if its signature creation data is compromised.[300]

[296] Article 9, subparagraph 1 (*f*).

[297] Argentina, *Ley de firma digital (2001)*, article 21 (*c*) and (*d*); Colombia, *Ley 527 sobre comercio electrónico*, article 32 (*b*); Mauritius, Electronic Transactions Act 2000, article 24; Panama, *Ley de firma digital (2001)*, article 49, paragraph 5; Thailand, Electronic Transactions Act (2001), section 28, paragraph 6; and Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 13.

[298] Bolivarian Republic of Venezuela, *Ley sobre mensajes de datos y firmas electrónicas*, article 35.

[299] Argentina, *Ley de firma digital (2001)*, article 21 (*b*).

[300] Argentina, Ley de firma digital (2001), article 21 (*p*).

226. The signatory is also required to exercise all due care. The UNCITRAL Model Law on Electronic Signatures, for example, requires the signatory to "exercise reasonable care to avoid unauthorized use of its signature creation data".[301] A similar duty exists under most domestic laws, although with some variations. In some cases, the law subjects the signatory to a strict obligation to ensure exclusive control over the signature creation device and prevent its unauthorized use,[302] or makes the signatory solely responsible for safe-keeping the signature creation device.[303] Often, however, this obligation is qualified as a duty to keep adequate control over the signature creation device or to take adequate measures to keep control over it,[304] to act diligently to avoid unauthorized use,[305] or to exercise reasonable care to avoid unauthorized use of its signature device.[306]

(d) Failure to suspend or revoke a certificate

227. The certification services provider could also incur liability for failing to suspend or revoke a compromised certificate. For a digital signature infrastructure to function properly and enjoy trust, it is critical that a mechanism be in place to determine in real time whether a particular certificate is valid, or whether it has been suspended or revoked. Whenever a private key is compromised, for example, revocation of the certificate is the primary mechanism by which a signatory can protect itself from fraudulent transactions initiated by impostors who may have obtained a copy of their private key.

228. As a consequence, the speed with which the certification services provider revokes or suspends a signatory's certificate following a request from the signatory is critical. The lapse of time between a signatory's request to revoke a certificate, the actual revocation and the publication of the notice of revocation could allow an impostor to enter into fraudulent transactions. Consequently, if the certification services provider unreasonably delays posting a revocation to a certificate revocation list, or fails to do so, both the signatory and the defrauded relying party could suffer significant damages in reliance upon an allegedly valid certificate. Furthermore, as part of their

[301] Article 8, subparagraph 1 (*a*).

[302] Argentina, *Ley de firma digital (2001)*, article 25 (*a*); Colombia, *Ley 527 sobre comercio electrónico*, article 39, paragraph 3; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 53 (*d*); Panama, *Ley de firma digital (2001)*, article 37, paragraph 4; Russian Federation, Federal Law on Electronic Digital Signature (2002), clause 12, paragraph 1; and Turkey, Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (2005), article 15 (*e*).

[303] Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 21.

[304] Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 24; and Viet Nam, Law on Electronic Transactions, article 25, paragraph 2 (*a*).

[305] Bolivarian Republic of Venezuela, *Ley sobre mensajes de datos y firmas electrónicas*, article 19.

[306] Cayman Islands, Electronic Transactions Law, 2000, section 39 (*a*); Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 17 (*b*); India, Information Technology Act, 2000, section 42, paragraph 1; Mauritius, Electronic Transactions Act 2000, section 35, paragraph 1 (*a*) and (*b*); Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99 (II); Singapore, Electronic Transactions Act (chapter 88), section 39; and Thailand, Electronic Transactions Act (2001), section 27, paragraph 1.

certification services, certification services providers may offer to maintain online depositories and certificate revocation lists that will be accessible by relying parties. Maintaining this database involves two basic risks: the risk that the repository or certificate revocation list might be inaccurate, thereby providing erroneous information upon which the recipient will rely to its detriment; and the risk that the repository or certificate revocation list will be unavailable (e.g. because of system failure), thereby interfering with the ability of signatories and relying parties to complete transactions.

229. As indicated earlier, the UNCITRAL Model Law on Electronic Signatures assumes that the certification services provider may issue various levels of certificates with varying degrees of reliability and security. Accordingly, the Model Law does not require a certification services provider to always make available a revocation system, which may not be commercially reasonable for certain types of low-value certificate. Instead, the Model Law only requires the certification services provider to provide "reasonably accessible means" that enable a relying party to ascertain from the certificate, inter alia, whether means exist for the signatory to give notice that the signature creation data have been compromised and whether a timely revocation service is offered;[307] where a timely revocation service is offered, the certification services provider is obliged to ensure its availability.[308]

230. The regime established by the European Union directive on electronic signatures obliges European Union member States, as "a minimum", to ensure that a certification services provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate, unless the certification services provider proves that it has not acted negligently.[309] Some domestic laws oblige the certification services provider to take measures to prevent certificate forgery[310] or to revoke a certificate immediately upon finding out that information on which the certificate was issued was inaccurate or false.[311]

231. A similar duty may also exist for the signatory and other authorized persons. The UNCITRAL Model Law on Electronic Signatures, for example, requires the signatory to utilize, without undue delay, means made available by the certification service provider, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if the signatory knows that the signature creation data have been compromised or if circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised.[312]

[307] Article 9, subparagraph 1 (*d*), (v) and (vi).

[308] Article 9, subparagraph 1 (*e*).

[309] European Union directive on electronic signatures …, article 6, paragraph 2; see also paragraph (*b*) of annex II to the directive.

[310] Panama, *Ley de firma digital (2001)*, article 49, paragraph 6.

[311] Argentina, *Ley de firma digital (2001)*, article 19 (*e*) (2).

[312] Article 8, subparagraph 1 (*b*), (i) and (ii).

232. Domestic laws often affirm the duty of the signatory to request revocation of the certificate in any circumstance where the secrecy of the signature creation data might have been compromised,[313] although in some cases the law only obliges the signatory to communicate that fact to the certification services provider.[314] The laws of several countries have adopted the formulation in the UNCITRAL Model Law on Electronic Signatures, which places the signatory under an obligation to further notify any person who may reasonably be expected by the signature device holder to rely on or to provide services in support of the electronic signature.[315] Although the consequences of breach of this duty may be implied in a number of legal systems, in some countries the law expressly declares the signatory liable for failure to communicate the loss of control over the private key or failure to request the revocation of the certificate.[316]

Conclusion

233. Wide use of electronic authentication and signature methods may be a significant step towards reducing trade documentation and the related costs in international transactions. While to a very large extent the pace of developments in this area is determined by the quality and security of technological solutions, the law may offer a significant contribution towards facilitating the use of electronic authentication and signature methods.

234. A large number of countries have already taken domestic measures in that direction by adopting legislation that affirms the legal value of electronic communications and sets the criteria for their equivalence to paper-based ones. Provisions regulating electronic authentication and signature methods are often an important component of such laws. The UNCITRAL Model Law on Electronic Commerce has become the single most influential standard for legislation in this area and its wide implantation has helped to promote an important degree of international harmonization. Wide ratification of the United Nations Convention on the Use of Electronic Communications in International Contracts would provide even greater harmonization, by offering a particular set of rules for international transactions.

[313] Argentina, *Ley de firma digital (2001)*, article 25 (*c*); Colombia, *Ley 527 sobre comercio electrónico*, article 39, paragraph 4; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, articles 49 and 53 (*e*); Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 17 (*f*); Mauritius, Electronic Transactions Act 2000, article 36; Panama, *Ley de firma digital (2001)*, article 37, paragraph 5; Singapore, Electronic Transactions Act (chapter 88), section 40; and Russian Federation, Federal Law on Electronic Digital Signature (2002), clause 12, paragraph 1.

[314] India, Information Technology Act, 2000, section 42, paragraph 2; and Turkey, Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (2005), article 15 (*f*) and (*i*).

[315] Cayman Islands, Electronic Transactions Law, 2000, section 31 (*b*); China, Electronic Signatures Law, article 15; Thailand, Electronic Transactions Act (2001), section 27, paragraph 2; and Viet Nam, Law on Electronic Transactions, article 25, paragraph 2 (*b*).

[316] China, Electronic Signatures Law, article 27; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 55; Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 17 (*e*); Panama, *Ley de firma digital (2001)*, article 39; Russian Federation, Federal Law on Electronic Digital Signature (2002), clause 12, paragraph 2; and Venezuela (Bolivarian Republic of), *Ley sobre mensajes de datos y firmas electrónicas*, article 40.

235. International use of electronic authentication and signature methods may also benefit from the adoption of those UNCITRAL standards. In particular, the flexible criteria for functional equivalence between electronic and paper-based signatures contained in the United Nations Convention on the Use of Electronic Communications in International Contracts may provide an international common framework for allowing electronic authentication and signature methods to meet foreign form signature requirements. Nevertheless, some problems may persist, in particular in connection with international use of electronic authentication and signature methods that require the involvement of a trusted third party in the authentication or signature process.

236. The problems that arise in this particular area derive to a very large extent from inconsistency of technical standards or incompatibility of equipment or software, resulting in lack of international interoperability. Efforts to harmonize standards and improve technical compatibility may lead to a solution to the difficulties that exist at present. However, there are also legal difficulties related to use of electronic authentication and signature methods, in particular in connection with domestic laws that either prescribe or favour the use of a particular technology for electronic signatures, typically digital signature technology.

237. Laws that provide for the legal value of digital signatures typically attribute the same legal value to signatures supported by foreign certificates only to the extent that they are regarded as equivalent to domestic certificates. The review done in this study indicates that proper assessment of legal equivalence requires a comparison not only of the technical and security standards attached to a particular signature technology, but also of the rules that would govern the liability of the various parties involved. The UNCITRAL Model Law on Electronic Signatures provides a set of basic common rules governing certain duties of the parties involved in the authentication and signature process that may have an impact on their individual liability. There are also regional texts, such as the European Union directive on electronic signatures, that offer a similar legislative framework for the liability of certification services providers operating in the region. However, neither of those texts addresses all liability issues arising out of the international use of certain electronic authentication and signature methods.

238. It is important for legislators and policymakers to understand the differences between domestic liability regimes and the elements common to them, so as to devise appropriate methods and procedures for recognition of signatures supported by foreign certificates. The domestic laws of various countries may already provide substantially equivalent answers to the various questions discussed in the present publication, for instance because they share a common legal tradition or belong to a regional integration framework. Such countries may find it useful to devise common liability standards or even harmonize their domestic rules, so as to facilitate cross-border use of electronic authentication and signature methods.

كيفية الحصول على منشورات الأمم المتحدة

يمكن الحصول على منشورات الأمم المتحدة من المكتبات ودور التوزيع في جميع أنحاء العالم. استعلم عنها من المكتبة التي تتعامل معها أو اكتب إلى: الأمم المتحدة، قسم البيع في نيويورك أو في جنيف.

如何购取联合国出版物

联合国出版物在全世界各地的书店和经售处均有发售。请向书店询问或写信到纽约或日内瓦的联合国销售组。

HOW TO OBTAIN UNITED NATIONS PUBLICATIONS

United Nations publications may be obtained from bookstores and distributors throughout the world. Consult your bookstore or write to: United Nations, Sales Section, New York or Geneva.

COMMENT SE PROCURER LES PUBLICATIONS DES NATIONS UNIES

Les publications des Nations Unies sont en vente dans les librairies et les agences dépositaires du monde entier. Informez-vous auprès de votre libraire ou adressez-vous à: Nations Unies, Section des ventes, New York ou Genève.

КАК ПОЛУЧИТЬ ИЗДАНИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

Издания Организации Объединенных Наций можно купить в книжных магазинах и агентствах во всех районах мира. Наводите справки об изданиях в вашем книжном магазине или пишите по адресу: Организация Объединенных Наций, Секция по продаже изданий, Нью-Йорк или Женева.

CÓMO CONSEGUIR PUBLICACIONES DE LAS NACIONES UNIDAS

Las publicaciones de las Naciones Unidas están en venta en librerías y casas distribuidoras en todas partes del mundo. Consulte a su librero o diríjase a: Naciones Unidas, Sección de Ventas, Nueva York o Ginebra.

United Nations publication
ISBN: 978-92-1-133663-4
Sales No. E.09.V.4

FOR UNITED NATIONS USE ONLY

Printed in Austria
V.08-55698—February 2009—1,510