United Nations A/CN.9/630/Add.2

General Assembly

Distr.: General
26 April 2007

Original: English

United Nations Commission on International Trade Law
Fortieth session
Vienna, 25 June-12 July 2007

Possible future work on electronic commerce

Comprehensive reference document on elements required to establish a favourable legal framework for electronic commerce: sample chapter on international use of electronic authentication and signature methods

Note by the Secretariat*

Addendum

The annex to the present note contains part of a sample chapter (part one, chap. II, sects. A and B) of a comprehensive reference document dealing with legal issues related to the international use of electronic authentication and signature methods.

* Submission of this document by the secretariat of the United Nations Commission on International Trade Law was delayed owing to shortage of staff.

V.07-82827 (E) 250507 250507

Annex

Contents

Part One
Electronic signature and authentication methods

[…]

II. Legal treatment of electronic authentication and signatures

1. 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;[1] or contractual agreements.[2]

2. 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 inter-bank 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.

3. 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 communications, time and place of dispatch or receipt of data

---

[1] 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 28 March 2007.

[2] 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 28 March 2007.

messages, security procedures for gaining access to the network and authentication or signature methods to be used by the parties.[3] Within the limits of the contractual freedom under applicable law, such rules and agreements are usually self-enforcing.

4. 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

5. 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**.[4]

1. Minimalist approach

6. Some jurisdictions recognize all technologies for electronic signature, following a policy of technological neutrality.[5] This approach is also called minimalist, since 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.

7. The UNCITRAL Model Law on Electronic Commerce[6] 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:

> "(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."

---

[3] 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.

[4] 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.

[5] For example, Australia and New Zealand.

[6] See note […] [United Nations publication, Sales No. E.99.V.4].

8. 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 provide 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.

9. 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.[7]

10. Except in Europe, where legislation has been primarily influenced by directives issued by the European Union,[8] most countries that have legislated in relation to electronic commerce have used the Model Law on Electronic Commerce as their template.[9] The Model Law has also served as a basis for the domestic

---

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

[8] In particular, Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (see note […]) [*Official Journal of the European Communities*, L 13]. 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 (Directive on electronic commerce) (*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.

[9] 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 civilies, 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*

harmonization of e-commerce legislation in countries organized on a federal basis, such as Canada[10] and the United States of America.[11] With very few exceptions,[12] 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,[13] which was adopted in 2001, and the more recent United Nations Convention on the Use of Electronic Communications in International Contracts[14] (which was adopted by the General Assembly on 23 November 2005 and has been opened for signature since 16 January 2006) follow the same approach, although the UNCITRAL Model Law on Electronic Signatures contains some additional language (see below, paras. […]-[…]).

---

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 Great Britain and Northern Ireland 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.

[10] 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 12 April 2007). 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 (the 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.chlc.ca/en/cls/index.cfm?sec=4&sub=4b>, accessed on 7 February 2007.

[11] In the United States of America, 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 7 February 2007). 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 the state of 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 7 February 2007.

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

[13] See note […] [United Nations publication, Sales No. E.02.V.8].

[14] See note […] [General Assembly resolution, 60/21, annex].

11. When legislation adopts the minimalist approach, the issue of whether electronic signature equivalence has been proven 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 test are considered valid; hence, the test embodies the principle of technological neutrality.

12. 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 the time when the data message was communicated.

2. Technology-specific approach

13. 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.[15] 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 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, businessmen are in most cases free to choose among a wide range of methods to achieve integrity and authenticity of

---

[15] 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 28 March 2007. 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 public key infrastructure (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 Russian Federation, Law on Electronic Digital Signature (2002).

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.

14. 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".[16] Rather than facilitating the growth of electronic commerce and the use of electronic authentication techniques, such an approach may have an opposite effect. Technology specific legislation risks fixing requirements before a particular technology matures.[17] 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.

15. 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 authentication arena 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, 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);[18]

(b) **Limited Government interference**. The Government might decide to establish a voluntary or mandatory high-level authentication authority. In this case,

---

[16] Stewart Baker and Matthew Yeo, in collaboration with the secretariat of the International Telecommunication Union, "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 www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html, accessed on 12 April 2007.

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

[18] 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.

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;[19]

(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.[20] Identity management systems (see paras. […]-[…] 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

16. 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).[21] 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 required 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.

17. 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. […]-[…]). 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.

---

[19] Ibid., where Singapore is cited as an example.

[20] Ibid., where China and Malaysia are cited as examples.

[21] Aalberts and van der Hof, *Digital Signature Blindness* … (see note […]), para. 3.2.2.

18. The first jurisdictions to have passed legislation adopting the two-tiered approach include Singapore[22] and the European Union.[23] They were followed by a number of others.[24] 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.[25]

19. 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, etc.).[26] Moreover, it was suggested that two-tier laws should explicitly give effect to contractual agreements concerning the use and recognition of electronic signatures, so as to ensure that

---

[22] 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.

[23] Like the Electronic Transactions Act of Singapore, the European Union Directive on electronic signatures (see note […]), 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).

[24] For example, Mauritius and Pakistan. For details of the respective statutes, see note [9] above.

[25] UNCITRAL Model Law on Electronic Signatures (see note […]), 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.

[26] Baker and Yeo, "Background and issues concerning authentication…" (see note [16]).

global contract-based authentication models do not run afoul of national legal requirements.

B. Evidentiary value of electronic signature and authentication methods

20. 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

21. 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.

22. 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,[27] 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.

---

[27] United Nations publication, Sales No. E.99.V.11, available at http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf.

23. 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.

24. 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.[28] Some countries expressly refer to the use of codes, passwords or other means of identification as factors that create a presumption of authorship.[29] 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.[30]

25. 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.[31] In addition, several countries that have implemented the Model Law on Electronic Commerce have not included any specific provision based on article 13.[32] 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."[33]

---

[28] 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 [9] above.

[29] Mexico (see note [9] above), art. 90, para. I.

[30] For example, the Uniform Electronic Transactions Act of the United States (see note [10]) 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".

[31] Australia (sect. 15, para. 1); essentially in the same manner, India (sect. 11); Pakistan (sect. 13, subsect. 2); Slovenia (art. 5); the British crown dependency of the Isle of Man (sect. 2); and Hong Kong SAR of China (sect. 18). For details of the respective statutes, see note [9] above.

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

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

26. 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."[34] 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."[35] According to the commentary on the United States Act, therefore:

> "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

---

[34] United States, Uniform Electronic Transactions Act (1999) (see note [11]), 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".

[35] Ibid. 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."

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."[36]

27. 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".[37]

28. 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, as evidence in civil proceedings.[38] Courts in the United States have dismissed arguments that e-mail messages were inadmissible as evidence because they were unauthenticated and parol evidence.[39] The courts have found instead that e-mails obtained from the plaintiff during the discovery process were self-authenticating, since "the production of documents during discovery from the parties' own files is sufficient to justify a finding of self-authentication".[40] The courts tend to take into account all available evidence and do not reject electronic records as being prima facie inadmissible.

29. 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-mails as evidence in court proceedings, on the grounds that e-mails do not offer adequate guarantees of integrity.[41] 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 defendants were 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

---

[36] Ibid., official comments on section 9.

[37] Ibid., paragraph 6 of the official comments on section 9.

[38] *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.

[39] *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.

[40] *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.

[41] 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 11 September 2003.

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,[42] 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.[43] 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 to that person.[44] 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.[45]

2. Ability to meet legal signature requirements

30. In some countries, the courts have been inclined to interpret signature requirements liberally. As previously indicated (see introduction, paras. […]-[…]), 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.[46] 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 satisfied statutory signature requirements.[47] A

---

[42] 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 25 August 2003; 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 2 February 2007.

[43] 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 25 August 2003.

[44] 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 25 August 2003.

[45] 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 25 August 2003.

[46] *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.

[47] *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.

person's "deliberate choice to type his name at the conclusion of all e-mails" has been considered to be valid authentication.[48] The readiness of the United States courts to accept that e-mails and names typed therein are capable of satisfying writing requirements[49] 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".[50] 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 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".[51]

31. 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-mails may therefore constitute "documents", and names typed on the e-mails may be "signatures".[52] 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 "[t]he fact that the document is created electronically as opposed to as a hard copy can make no difference."[53] 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.[54] In other cases courts have suggested that they might

---

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

[49] *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.

[50] 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-mails as such could not validly record the terms of a contract, but because there was no indication that the authors of the e-mails and the persons mentioned therein were employees of the defendant.

[51] *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.

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

[53] *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).

[54] *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

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".[55] 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.[56]

32. 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.[57] 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.[58]

33. 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 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[59] and the

---

(January)) (United Kingdom, All England Direct Law Reports (Digests)).

[55] *Mehta v. J. Pereira Fernandes S.A.* (see note [55]).

[56] *Mehta v. J. Pereira Fernandes S.A.* (see note [55]), 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]".

[57] 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 avril 2003, *Sté Chalets Boisson c/ M. X.*, available at www.juriscom.net/jpt/visu.php?ID=239, accessed on 12 September 2003).

[58] France, Conseil d'État, 28 décembre 2001, N° 235784, *Élections municipales d'Entre-Deux-Monts*, available at www.rajf.org/article.php3?id_article=467, accessed on 12 September 2003.

[59] 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 www.jurpc.de/rechtspr/19980009.htm, accessed on 12 September 2003.

Federal Court (*Bundesgerichtshof*)[60] 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.[61] 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.[62]

34. 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,[63] 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.[64]

35. 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

---

[60] 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 12 September 2003.

[61] Ibid.

[62] In a decision on a case referred to it by the Bundesgerichtshof of Germany (Federal Court of Justice) (see note [62]), the Gemeinsamer Senat der obersten Gerichtshöfe des Bundes (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 ("*hinreichend zuverlässig*") 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 12 September 2003.

[63] 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).

[64] Colombia, Juzgado Segundo Promiscuo Municipal Rovira Tolima, *Juan Carlos Samper v. Jaime Tapias*, 21 julio 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-mails 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 2 February 2007).

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) Apostilles*

36. It has been stated that the spirit and letter of the Convention Abolishing the Requirement of Legalisation for Foreign Public Documents, done at The Hague on 5 October 1961, did not constitute an obstacle to the usage of modern technology.[65] The First International Forum on e-Notarization and e-Apostilles endorsed this conclusion and noted that the application and operation of the Convention could be further improved by relying on such technologies.[66] An interpretation of the Convention in the light of the principle of functional equivalence would permit competent authorities both to keep electronic registries and to issue electronic Apostilles, in order to enhance further international legal assistance and government services.

37. In April 2006, 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 e-APP, the Hague Conference and the 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).[67]

(b) Seals

38. Some jurisdictions have already abolished the requirement for seals on the ground that sealing is no longer relevant in today's context. An attested

---

* This section would be further developed in a final version of the comprehensive reference document.

65 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" (The Hague, 2003).

66 Conclusions adopted at the First International Forum on e-Notarization and e-Apostilles, held in Las Vegas, United States, on 30 and 31 May 2005, available at http://www.hcch.net/upload/concl_forum.pdf, accessed on 7 February 2007.

67 The e-APP is designed to use already existing and widely used technology. The suggested technology is based on Portable Document Format (PDF) with embedded Extensible Markup Language (XML). More information may be found at http://hcch.e-vision.nl/index_en.php?act=text.display&tid=37, under "Second International Forum on e-Notarization and e-Apostilles", held in Washington, D.C., from 27 to 29 May 2006.

(i.e. witnessed) signature has been substituted.[68] 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.[69] 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.[70]

39. A number of countries have also 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 in legislation, leaving the technical details of the form of the electronic seal to be separately determined.[71]

40. The United States Uniform Real Property Electronic Recording Act[72] 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 be contained in the stamp, impression or seal must be attached to, or logically associated with, the document or signature in an electronic fashion.[73] Thus, the notarial stamp or impression that is required under

---

[68] 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).

[69] 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.

[70] 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.

[71] 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), which defines an "electronic seal" as the form of identification issued by the association of 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 4 April 2007).

[72] 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 7 February 2007. It has been adopted in Arizona, Delaware, the District of Columbia, Kansas, North Carolina, Texas, Virginia and Wisconsin (see http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-urpera.asp, accessed on 7 February 2007).

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.

(c) Notarization*

41. There are three principal United States statutes dealing with notarization: the Uniform Electronic Transactions Act, the Electronic Signatures in Global and National Commerce Act (E-sign)[74] and the Uniform Real Property Electronic Recording Act.[75] 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.

42. In Austria, the cyberDOC electronic document archive, an independent company jointly established by the Austrian Chamber of Civil Law Notaries and Siemens AG, provides notaries with an electronic archive that includes authentication functions.[76] Austrian notaries are obliged under the law to record and store all notarial deeds perfected after 1 January 2000 in this archive.

(d) Attestation

43. It has been argued that traditional witnessing processes, such as attestation, 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 computer screen, capable of being read by a human being, of what is allegedly in the memory. When the witness sees the signatory pressing the keyboard, the witness will not know with certainty what is actually happening. Therefore, it would be possible to ensure that the screen display corresponds to the contents of the computer memory and that the signatory's keystrokes correspond to his or her intentions only if the computer has been evaluated to effect a trusted path by trusted evaluation criteria.[77]

44. However, a secure electronic signature would be able to perform a similar function 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

---

* This section would be further developed in a final version of the comprehensive reference document.

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

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

[75] See note [74].

[76] See Österreichische Notariatskammer (Austrian Chamber of Civil Law Notaries), available at http://www.notar.at/de/portal/einrichtungen/cyberdocgmbhcokg/, accessed on 7 February 2007.

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

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.[78]

45. 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, as long as it "adequately identifies the witness and adequately indicates that the signature or seal has been witnessed"; and "is as reliable as is appropriate given the purpose for which, and the circumstances in which, the witness's signature is required."[79]

46. 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 signs the electronic document with their secure electronic signature.[80] 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 that person's secure electronic signature.[81] 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 that person's 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 that person's secure electronic signature.[82] 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.[83]

---

[78] 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".

[79] New Zealand, Electronic Transactions Act (see note [9]), section 23, available at http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes, accessed on 4 April 2007.

[80] Canada, Personal Information Protection and Electronic Documents Act (see note [72]), part 2, section 46.

[81] Ibid., section 45.

[82] Ibid., section 44.

[83] 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.landregistry.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc, accessed on 7 April 2007. The project is scheduled to be implemented in tranches from 2006 to 2009.