United Nations A/CN.9/630

General Assembly

Distr.: General
25 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*

1. 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).

2. In 2005, the Commission 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 the Commission 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

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

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

V.07-82774 (E) 170507 180507

(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.

3. There was support for the view that the task of legislators and policymakers, in particular in developing countries, might be greatly facilitated if the Commission 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 the Commission to identify areas in which it might itself undertake future harmonization work. However, there were also concerns that the range of issues identified was too wide and that the scope of the comprehensive reference document might need to be reduced. The Commission eventually agreed to ask its 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]

4. The annex to the present note contains the introductory part of a sample chapter dealing with legal issues related to the international use of electronic authentication and signature methods (henceforth referred to as the "sample chapter"). The addenda to the present note discuss the legal treatment of electronic authentication and signatures and legal problems arising out of their international use.

5. The Commission may wish to consider the structure, level of detail, nature of discussion and type of advice provided in the sample chapter and consider whether it would be desirable and useful for the Secretariat to prepare other chapters following the same model, to deal with other issues that the Commission may wish to select from among those proposed earlier (see para. 2 above). Alternatively, the Commission may wish to request that the Secretariat continue to follow closely legal developments in the relevant areas, with a view to making appropriate suggestions in due course. In that case, the Commission may wish to consider whether the Secretariat should be requested to publish the sample chapter, with whatever amendments the Commission may consider appropriate, as a stand-alone publication.

---

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

Annex

Contents

Foreword

The present document 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 (see below, paras. […]-[…]).* 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 electronic signature and authentication methods (see below, paras. […]-[…]).

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 document pays 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.

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 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

---

* All cross references in this document and its addenda, as well as all cross references in their footnotes, will be finalized when the final document is issued in consolidated form.

[1] United States of America, Federal Rules of Evidence, rule 901, subdivision (a): "The

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 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

---

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).

[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 Q.B. 574, 114 E.R. 1366 (United Kingdom, Law Reports, Queen's Bench)

[10] Lord Denning in *Goodman v. Eban* [1954] Q.B.D. 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 "[f]or the prevention of many fraudulent practices which are commonly endeavoured to be upheld by perjury 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 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] through 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,

---

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 a price of $500 or more is not enforceable by way of action or defence 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).

[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 7 February 2007.

[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).

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 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

---

[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. Italy also follows the same rule, although less explicitly (see Civil Code of Italy, articles 1326 and 1350).

[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 mai 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 sein privé"*) (see *Recueil Dalloz*, *Preuve*, no. 638).

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 the 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 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 permit 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).[33] 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

---

[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).

[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. 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.

by someone else; and the fact that, and the time when, a person has been at a given place.[34]

8. It should be noted, however, that even though the 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 sufficient assurance of the authenticity of the documents 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 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 therefore 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

---

[34] Ibid.

[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).

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;

(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]

(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.

---

[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 especially chapter III, section D, on the concept of witnessing.

[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 especially part 2, chapter II, on policy objectives of writing and signature requirements.

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.

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 or 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.

---

[39] United Nations, *Treaty Series*, vol. 527, No. 7625. Available at the apostille section on the website of the Hague Conference on Private International Law at http://hcch.e-vision.nl/index_en.php?act=text.display&tid=37, accessed on 7 February 2007.

[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.

Part One

Electronic signature and authentication methods

I. Definition and methods of electronic signature and authentication

A. General remarks on terminology

15. The terms “electronic authentication” or “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 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 the combination of different technologies are becoming increasingly popular, such as, for instance, in the case of the combined use of passwords and TLS/SSL (transport layer security/secure sockets layer), 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. […]-[…]).

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 inconsistent use of terminology. Expressions that were traditionally used with a particular connotation under national laws started to be used 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. […]-[…]), the notions of

---

[41] See 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., available at www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html.

[42] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001* (see note [33]), part two, para. 33.

"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 of 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 (see paras. […]-[…] above). 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 4 April 2007.

[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 4 April 2007).

[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 4 April 2007).

[46] *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (see note [33]).

[47] *UNCITRAL Model Law on Electronic Signatures* (see note [33]).

(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, UNCITRAL's 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. […]-[…]) 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 (see paras. […]-[…]).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 of a person whose relationship with the originator or with any agent of the

---

[48] *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (see note [33]), article 7, subparagraph 1 (b).

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 in the electronic environment do not coincide, the various techniques mentioned earlier (see above, para. [16] and the more detailed discussion in paras. […]-[…] 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 "guarantee the integrity of the contents."[49] 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.[50]

---

[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 4 April 2007.

[50] Ibid.