United Nations A/CN.9/630/Add.3

General Assembly

Distr.: General
16 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 (part two, chap. I, sects. A and B) of a sample chapter of a comprehensive reference document dealing with legal issues related to the international use of electronic authentication and signature methods.

V.07-82259 (E) 090507 100507

Annex

Contents

Part Two

Cross-border use of electronic signature and authentication methods

I. Legal recognition of foreign electronic authentication and signature methods

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

A. International impact of domestic laws

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

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

1. International obstacles created by conflicting domestic approaches

4. Technology-neutral approaches, especially those which incorporate a "reliability test", tend to resolve legal incompatibilities. International legal instruments adopting this approach include the UNCITRAL Model Law on Electronic Commerce, article 7, paragraph 1 (b),[1] and the United Nations Convention on the Use of Electronic Communications in International Contracts, article 9, paragraph 3.[2] Under this approach, an electronic signature or authentication method that can both identify the signatory and indicate the signatory's intention in respect of the information contained in the electronic communication will fulfil signature requirements, provided it meets several criteria. In the light of all the circumstances, including any agreement between the originator and the addressee of the data message, the signature or authentication method must

[1] See note [...] [United Nations publication, Sales No. E.99.V.4].
[2] See note [...] [General Assembly resolution 60/21, annex].

be shown to be as reliable as is appropriate for the purpose for which the data message is generated or communicated. Alternatively, by itself or in conjunction with other evidence, it must be shown to have fulfilled these purposes.

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

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

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

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

9. Second, technology-specific legislation, particularly legislation that favours digital signatures, which is also the case in the two-tiered approach, is likely to give rise to a patchwork of conflicting technical standards and licensing requirements that will make the use of electronic signatures across borders very difficult. A system in which each country prescribes its own standards may also prevent parties from entering into mutual recognition and cross-certification agreements.[3] Indeed, a

[3] Stewart Baker and Matthew Yeo, in collaboration with the secretariat of the International Telecommunication Union, “Background and issues concerning authentication and the ITU”,

major remaining problem relating, in particular, to digital signatures is that of cross-border recognition. The Working Party on Information Security and Privacy (WPSIP) of the Organization for Economic Cooperation and Development (OECD) (hereinafter OECD WPSIP) has noted that although the approach adopted by most jurisdictions appears to be non-discriminatory, differences in local requirements will continue to engender interoperability problems.[4] For the purposes of the present study, the following weaknesses noted by OECD WPSIP may be relevant:

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

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

(c) **Acceptance of credentials**.[5] In some cases, the acceptance of the credentials issued by other entities was cited as a barrier to interoperability. As such, OECD WPSIP suggests that consideration could be given to the possibility of developing a set of best practices or guidelines for issuing credentials for authentication purposes. Work may already be under way in several jurisdictions on this issue that could provide useful input to any initiatives of OECD WPSIP in this regard;

(d) **A range of authentication methods in use**. OECD WPSIP found that in virtually all OECD member States, a range of authentication solutions was in use.

---

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.

[4] Organization for Economic Cooperation and Development, Working Party on Information Security and Privacy, *The Use of Authentication across Borders in OECD Countries* (DSTI/ICCP/REG(2005)4/FINAL), http://www.oecd.org/dataoecd/1/10/35809749.pdf, accessed on 2 February 2007.

[5] A credential is a token given to prove that an individual or a specific device has gone through an authentication process. Credentials that are bound to the user are essential for identification purposes. Bearer credentials may be sufficient for some forms of authorization. Examples are a valid driving licence, a person's social security number or other identification number, or smart cards. Centre for Democracy and Technology, "Privacy principles for authentication systems", http://tprc.org/papers/2003/183/CDTauthenticationTPRC.pdf, accessed on 12 April 2007; see also Centre for Democracy and Technology, Authentication Privacy Principles Working Group, "Interim report on privacy principles for authentication systems", http://www.cdt.org/privacy/authentication/030513interim.pdf, accessed on 12 April 2007.

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

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

2. Emerging consensus

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

12. The divergent policies may also reflect different assumptions about how authentication technologies will emerge. One scenario, the so-called “universal authentication paradigm”,[7] assumes that the principal purpose of authentication technologies will be to verify identities and attributes among persons who have no pre-existing relationship with each other and whose common use of technology is not the subject of contractual agreement. Therefore, the authentication or signature technology should confirm the identity or other attributes of a person to a potentially unlimited number of persons and for a potentially unlimited number of purposes. This model stresses the importance of technical standards and of the operational requirements of certification services providers when trusted third

---

[6] See note […] [Background and issues concerning authentication and the ITU].

[7] Ibid.

parties are involved. Another scenario, the so-called "bounded authentication paradigm" advocates that the principal use of authentication and signature technologies will be to verify identities and attributes among persons whose common use of the technology takes place under contractual agreements.[8] Therefore, the authentication technology should confirm the identity or other attributes of the certificate holder only for a set of specifically defined purposes and within a defined community of potentially relying parties who are subject to common terms and conditions for the use of the technology. Under this model, focus is on the legal recognition of the contractual agreements.

13. Despite these discrepancies, some of which still prevail, the findings of OECD WPISP[9] suggest that there now appears to be a growing international consensus on the basic principles that should govern electronic commerce and in particular electronic signature. The following findings are particularly interesting for the present study:

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

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

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

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

---

[8] Ibid.

[9] See note […] [*The Use of Authentication across Borders in OECD Countries*].

Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures[10]).

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

15. As noted above, one of the main obstacles to the cross-border use of electronic signatures and authentication has been a lack of interoperability, due to conflicting or divergent standards or their inconsistent implementation. Various forums have been established to promote standards-based, interoperable PKI as a foundation for secure transactions in electronic commerce applications. They include both intergovernmental[11] and mixed public sector and private sector organizations[12] at a global[13] or regional level.

16. Some of this technical work aims at developing technical standards for the provision of the information necessary for meeting certain legal requirements.[14]

---

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

[11] In the Asia-Pacific region, the Asia-Pacific Economic Cooperation (APEC) forum has developed "Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction eCommerce" (eSecurity Task Group, APEC Telecommunications and Information Working Group, December 2004), http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf, accessed on 12 April 2007. These Guidelines are intended to assist in developing schemes that are potentially interoperable and in reviewing the interoperability of existing schemes. The Guidelines cover classes or types of certificate used in transnational e-commerce only. The Guidelines are not intended to address other certificates, nor are they intended to limit schemes to only issuing certificates covered by the Guidelines.

[12] Within the European Union, the European Electronic Signature Standardization Initiative (EESSI), was created in 1999 by the Information and Communications Technology (ICT) Standards Board to coordinate the standardization activity in support of the implementation of European Union Directive 1999/93/EC on electronic signatures. The ICT Standards Board itself is an initiative of the European Committee for Standardization (CEN), which was created by national standards organizations and two non-profit organizations: the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). EESSI has developed various standards to promote interoperability, but their implementation has been slow, allegedly because of their complexity (Paolo Balboni, "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information and Communications Technology Law*, vol. 13, No. 3, 2004), pp. 211-242, 214.

[13] For example, the Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit, international consortium founded in 1993 to promote the development, convergence and adoption of standards for electronic business. OASIS has established a PKI Technical Committee comprised of PKI users, vendors and experts to address issues related to the deployment of digital certificates technology. The OASIS PKI Technical Committee has developed an action plan that contemplates, inter alia, to develop specific profiles or guidelines that describe how the standards should be used in particular applications so as to achieve PKI interoperability; to create new standards, where needed; and to provide interoperability tests and testing events (OASIS, PKI Technical Committee, "PKI action plan" (February 2004), http://www.oasis-open.org/committees/pki/pkiactionplan.pdf, accessed on 12 April 2007).

[14] For example, the ETSI has developed a standard (TS 102 231) to implement a non-hierarchical structure that, among other things, can address also cross recognition of PKI domains and, therefore, of certificates' validity. Basically, ETSI technical standard TS 102 231 specifies a standard for the provision of information on the status of a provider of certification services

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

1. Place of origin, reciprocity and local validation

17. Place of origin has been a classical factor in affording legal recognition to foreign documents or acts. This is typically done on the basis of reciprocity, so that signatures and certificates of a given country will be given domestic effect to the extent that domestic signatures and certificates are given legal effect in the other country. Another related factor is to subject the domestic effect of the foreign signature and certificate to some form of validation or acknowledgement by a domestic certification services provider, certification authority or regulator. Some of them combine all these factors.[15]

18. It is not common for domestic laws expressly to deny legal recognition to foreign signatures or certificates, which may confirm the appearance of their non-discriminatory character. In practice, however, many recognition regimes are likely to have some discriminatory impact, even if unintended. The European Union Directive on electronic signatures, for example, generally bans discrimination of foreign qualified certificates (i.e. PKI-based digital signatures). However, this works mainly in favour of certificates issued by certification services providers established within the territory of the States members of the European Union. A certification services provider established in a non-European-Union country has three options to obtain recognition of its certificate in the European Union: fulfil the requirements of the European Union Directive on electronic signatures and obtain accreditation under a scheme established in a member State; establish a cross certification with a certification services provider established in a European Union member State; or operate under the umbrella of a general recognition at the level of international agreement.[16] The manner in which the European Directive regulates

---

(called a “trust service provider”). It adopts a form of a signed list, the “Trust Service Status List” as the basis for presentation of this information. The Trust Service Status List specified by ETSI accommodates the requirement of evidence as to whether the provider of a trust service is or was operating under the approval of any recognized scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place. In order to fulfil that requirement, the Trust Service Status List must contain information from which it can be established whether the certification services provider’s service was, at the time of the transaction, known by the scheme operator and if so what was the status of the service (i.e. whether it was approved, suspended, cancelled, or revoked). The Trust Service Status List contemplated by ETSI technical standard TS 102 231 must therefore contain not only the service’s current status, but also the history of its status. Therefore, the list becomes a combination of valid services (“white list”) and cancelled or revoked services (“black list”) (see http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc, accessed on 4 March 2007).

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

[16] Indeed, under article 7 of the Directive, European Union member States only must ensure that the certificates issued by a certification services provider in a third country are recognized as legally equivalent to certificates issued by a certification services provider established within

international aspects suggests that ensuring conditions for market access abroad of European Union providers of certification services was one of the objectives pursued by the Directive.[17] By cumulating the requirement of substantive equivalence with European Union standards with the additional requirement of "accreditation under a scheme established in a member State", the European Union Directive on electronic signatures effectively requires foreign certification services providers to comply both with their original and with the European Union regime, which is a higher standard than is required from certification services providers accredited in a State member of the European Union.[18]

19. Article 7 of the European Union Directive on electronic signatures has been implemented with some variations.[19] Ireland and Malta, for instance, recognize foreign digital signatures (qualified certificates, under European Union terminology) as equivalent to domestic signatures, as long as other legal requirements are satisfied. In other cases, recognition is subject to domestic verification (Austria, Luxembourg) or a decision of a domestic authority (Czech Republic, Estonia, Poland). This tendency to insist on some form of domestic verification, which is typically justified by a legitimate concern as to the level of reliability of foreign certificates, leads in practice to a system of discrimination of foreign certificates on the basis of their geographic origin.

2. Substantive equivalence

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

21. Paragraph 1 of article 12 of the UNCITRAL Model Law on Electronic Signatures is intended to reflect the basic principle that the place of origin, in and of itself, should in no way be a factor in determining whether and to what extent foreign certificates or electronic signatures should be recognized as capable of being

---

the Community if (a) the certification services provider "fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State"; or (b) a certification services provider established within the Community that fulfils the requirements laid down in the Directive "guarantees" the certificate; or (c) the certificate or the certification services provider "is recognized under a bilateral or multilateral agreement between the Community and third countries or international organisations."

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

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

[19] Ibid., pp. 92-94.

legally effective. Determination of whether, or the extent to which, a certificate or an electronic signature is capable of being legally effective should depend on its technical reliability, rather than the place where the certificate or the electronic signature was issued. Non-discrimination provisions similar to article 12 of the Model Law on Electronic Signatures can also be found in some domestic regimes, such as the United States Electronic Signatures in Global and National Commerce Act 2000.[20] These provisions provide that the place of origin, in and of itself, should not be a factor in determining whether and to what extent foreign certificates or electronic signatures should be recognized as capable of being legally effective in an enacting State. They recognize that the legal effectiveness of a certificate or electronic signature should depend on its technical reliability.[21]

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

23. The Model Law does not require or promote reciprocity arrangements. In fact, the Model Law "contains no specific suggestion" as to "the legal techniques through which advance recognition of the reliability of certificates and signatures complying with the law of a foreign country might be made by an enacting State (e.g. a unilateral declaration or a treaty)".[22] Possible methods to achieve that result that were mentioned during the preparation of the Model Law included, for example, automatic recognition of signatures complying with the laws of another State if the laws of the foreign State required a level of reliability at least equivalent to that required for equivalent domestic signatures. Other legal techniques through which advance recognition of the reliability of foreign certificates and signatures might be made by an enacting State could include unilateral declarations or treaties.[23]

---

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

[21] See *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment*, part two, para. 83.

[22] Ibid., para. 157.

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