UNITED NATIONS

A

General Assembly

Distr.
LIMITED
A/CN.9/WG.IV/WP.84

8 December 1999
ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Working Group on Electronic Commerce
Thirty-sixth session
New York, 14-25 February 2000

DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

Note by the Secretariat

CONTENTS

INTRODUCTION

1. The Commission, at its twenty-ninth session (1996), decided to place the issues of digital signatures and certification authorities on its agenda. The Working Group on Electronic Commerce was requested to examine the desirability and feasibility of preparing uniform rules on those topics. It was agreed that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference. [1/]

2. At its thirtieth session (1997), the Commission had before it the report of the Working Group on the work of its thirty-first session (A/CN.9/437). The Working Group indicated to the Commission that it had reached consensus as to the importance of, and the need for, working towards harmonization of law in that area. While no firm decision as to the form and content of such work had been reached, the Working Group had come to the preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules at least on issues of digital signatures and certification authorities, and possibly on related matters. The Working Group recalled that, alongside digital signatures and certification authorities, future work in the area of electronic commerce might also need to address: issues of technical alternatives to public-key cryptography; general issues of functions performed by third-party service providers; and electronic contracting (A/CN.9/437, paras. 156-157).

3. The Commission endorsed the conclusions reached by the Working Group, and entrusted the Working Group with the preparation of uniform rules on the legal issues of digital signatures and certification authorities (hereinafter referred to as "the draft Uniform Rules on Electronic Signatures" or "the Uniform Rules"). With respect to the exact scope and form of the Uniform Rules, the Commission generally agreed that no decision could be made at this early stage of the process. It was felt that, while the Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging electronic-commerce practice, the Uniform Rules should be consistent with the media-neutral approach taken in the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law"). Thus, the Uniform Rules should not discourage the use of other authentication techniques. Moreover, in dealing with public-key cryptography, the Uniform Rules might need to accommodate various levels of security and to recognize the various legal effects and levels of liability corresponding to the various types of services being provided in the context of digital signatures. With respect to certification authorities, while the value of market-driven standards was recognized by the Commission, it was widely felt that the Working Group might appropriately envisage the establishment of a minimum set of standards to be met by certification authorities, particularly where cross-border certification was sought. [2/]

4. The Working Group began the preparation of the Uniform Rules at its thirty-second session on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.73).

5. At its thirty-first session (1998), the Commission had before it the report of the Working Group on the work of its thirty-second session (A/CN.9/446). It was noted that the Working Group, throughout its thirty-first and thirty-second sessions, had experienced manifest difficulties in reaching a common understanding of the new legal issues that arose from the increased use of digital and other electronic signatures. It was also noted that a consensus was still to be found as to how those issues might be addressed in an internationally acceptable legal framework. However, it was generally felt by the Commission that the progress realized so far indicated that the draft Uniform Rules on Electronic Signatures were progressively being shaped into a workable structure. The Commission reaffirmed the decision made at its thirtieth session as to the feasibility of preparing such Uniform Rules and expressed its confidence that more progress could be accomplished by the Working Group at its thirty-third session on the basis of the revised draft prepared by the Secretariat (A/CN.9/WG.IV/WP.76). In the context of that discussion, the Commission noted with satisfaction that the Working Group

had become generally recognized as a particularly important international forum for the exchange of views regarding the legal issues of electronic commerce and for the preparation of solutions to those issues. [3/]

6. At its thirty-second session (1999), the Commission had before it the report of the Working Group on the work of its thirty-third (July 1998) and thirty-fourth (February 1999) sessions (A/CN.9/454 and 457). The Commission expressed its appreciation for the efforts accomplished by the Working Group in its preparation of draft Uniform Rules on Electronic Signatures. While it was generally agreed that significant progress had been made at those sessions in the understanding of the legal issues of electronic signatures, it was also felt that the Working Group had been faced with difficulties in the building of a consensus as to the legislative policy on which the Uniform Rules should be based.

7. A view was expressed that the approach currently taken by the Working Group did not sufficiently reflect the business need for flexibility in the use of electronic signatures and other authentication techniques. As currently envisaged by the Working Group, the Uniform Rules placed excessive emphasis on digital signature techniques and, within the sphere of digital signatures, on a specific application involving third-party certification. Accordingly, it was suggested that work on electronic signatures by the Working Group should either be limited to the legal issues of cross-border certification or be postponed altogether until market practices were better established. A related view expressed was that, for the purposes of international trade, most of the legal issues arising from the use of electronic signatures had already been solved in the Model Law. While regulation dealing with certain uses of electronic signatures might be needed outside the scope of commercial law, the Working Group should not become involved in any such regulatory activity.

8. The widely prevailing view was that the Working Group should pursue its task on the basis of its original mandate (see above, para. 3). With respect to the need for uniform rules on electronic signatures, it was explained that, in many countries, guidance from UNCITRAL was expected by governmental and legislative authorities that were in the process of preparing legislation on electronic signature issues, including the establishment of public key infrastructures (PKI) or other projects on closely related matters (see A/CN.9/457, para. 16). As to the decision made by the Working Group to focus on PKI issues and PKI terminology, it was recalled that the interplay of relationships between three distinct types of parties (i.e., key holders, certification authorities and relying parties) corresponded to one possible PKI model, but that other models were conceivable, e.g., where no independent certification authority was involved. One of the main benefits to be drawn from focusing on PKI issues was to facilitate the structuring of the Uniform Rules by reference to three functions (or roles) with respect to key pairs, namely, the key issuer (or subscriber) function, the certification function, and the relying function. It was generally agreed that those three functions were common to all PKI models. It was also agreed that those three functions should be dealt with irrespective of whether they were in fact served by three separate entities or whether two of those functions were served by the same person (e.g., where the certification authority was also a relying party). In addition, it was widely felt that focusing on the functions typical of PKI and not on any specific model might make it easier to develop a fully media-neutral rule at a later stage (ibid., para. 68).

9. After discussion, the Commission reaffirmed its earlier decisions as to the feasibility of preparing such uniform rules (see above, paras. 3 and 5) and expressed its confidence that more progress could be accomplished by the Working Group at its forthcoming sessions. [4/]

10. The Working Group proceeded with the preparation of the draft Uniform Rules at its thirty-fifth session (Vienna, September 1999) on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.82). The report of that session is contained in document A/CN.9/465.

11. This note contains the revised draft provisions prepared pursuant to the deliberations and decisions of the Working Group, and also pursuant to the deliberations and decisions of the Commission at its thirty-second session, as reproduced

above (see above, paras. 6 to 9). Newly revised provisions are indicated by underlining. For ease of reference, a consolidated text of the draft provisions is attached as Annex I to this note.

12. In line with the applicable instructions relating to the stricter control and limitation of United Nations documents, the explanatory remarks to the draft provisions have been kept as brief as possible. Additional explanations will be provided orally at the session.

References to national legislation and other texts

13. For information and comparison, references to national legislation and other texts are included under this heading in smaller font for a number of articles. References to national legislation have been included on the basis of those statutes of which the Secretariat is aware and which are available for reference. References to other texts are included on the basis that they were concluded by international organizations or are widely known and publicly available. Abbreviations refer to the following legislation and texts:

- Germany: Digital Signature Law 1997 (Article 3, Information and Communication Services Act, approved 13/6/97; in force 1/8/97);
- Illinois: USA, Electronic Commerce Security Act 1998 (1997 Illinois House Bill 3180; 5 Ill. Comp. Stat. 175, enacted August 1998);
- Minnesota: USA, Electronic Authentication Act (Minnesota Statutes §325, enacted May 1997);
- Missouri: USA, Digital Signature Act, 1998 (1998 SB 680, enacted July 1998);
- Singapore: Electronic Transactions Act 1998, Act No 25 of 1998.

- ABA Guidelines: American Bar Association, Science and Technology Section, "Digital Signature Guidelines", 1996;
- EC Directive: Directive of the European Parliament and of the Council on a Community framework for electronic signatures, as adopted on 30 November 1999 (PE-CONS 3625/99);
- GUIDEC: International Chamber of Commerce, "General Usage for International Digitally Ensured Commerce", 1997.

I. GENERAL REMARKS

14. The purpose of the Uniform Rules, as reflected in the draft provisions set forth in part II of this note, is to facilitate the increased use of electronic signatures in international business transactions. Drawing on the many legislative instruments already in force or currently being prepared in a number of countries, these draft provisions aim at preventing disharmony in the legal rules applicable to electronic commerce by providing a set of standards on the basis of which the legal effect of digital signatures and other electronic signatures may become recognized, with the possible assistance of certification authorities, for which a number of basic rules are also provided.

15. Focused on the private-law aspects of commercial transactions, the Uniform Rules do not attempt to solve all the questions that may arise in the context of the increased use of electronic signatures. In particular, the Uniform Rules do not deal with aspects of public policy, administrative law, consumer law or criminal law that may need to be taken into account by national legislators when establishing a comprehensive legal framework for electronic signatures.

16. Based on the Model Law, the Uniform Rules are intended to reflect in particular: the principle of media-neutrality; an approach under which functional equivalents of traditional paper-based concepts and practices should not be discriminated

against; and extensive reliance on party autonomy. They are intended for use both as minimum standards in an "open" environment (i.e., where parties communicate electronically without prior agreement) and as default rules in a "closed" environment (i.e., where parties are bound by pre-existing contractual rules and procedures to be followed in communicating by electronic means).

17. In considering the draft provisions proposed for inclusion in the Uniform Rules, the Working Group may wish to consider more generally the relationship between the Uniform Rules and the Model Law. This draft of the Uniform Rules has been prepared on the basis that they will constitute a separate legal instrument.

18. The Working Group may wish to consider whether a preamble should clarify the purpose of the Uniform Rules, namely to promote the efficient utilization of electronic communication by establishing a security framework and by giving written and electronic messages equal status as regards their legal effect.

19. At the thirty-third session of the Working Group, doubts were expressed as to the appropriateness of using the terms "enhanced" or "secure" to describe signature techniques that were capable of providing a higher degree of reliability than "electronic signatures" in general (A/CN.9/454, para. 29). The Working Group concluded that, in the absence of a more appropriate term, "enhanced" should be retained. At the thirty-fourth session (A/CN.9/457, para. 39), it was suggested that the definition of "enhanced electronic signature" might need to be reconsidered, together with the general architecture of the Uniform Rules, once the purpose of dealing with two categories of electronic signatures had been clarified, particularly as regards the legal effects of both types of electronic signatures. It was suggested that dealing with enhanced electronic signatures offering a high degree of reliability was justified only if the Uniform Rules were to provide a functional equivalent to specific uses of handwritten signatures. Since this was likely to prove particularly difficult at the international level and be of limited relevance to international commercial transactions, the additional benefit to be expected from using an "enhanced electronic signature" as opposed to a mere "electronic signature" might need to be clarified. At the thirty-fifth session of the Working Group, support was expressed in favour of retaining the notion of "enhanced electronic signature", which was described as particularly apt to provide certainty with respect to the use of a certain type of electronic signatures, namely digital signatures implemented through public-key infrastructure (PKI). In response, it was pointed out that the notion of "enhanced electronic signature" made the structure of the Uniform Rules unnecessarily complex. In addition, the notion of "enhanced electronic signature" would lend itself to misinterpretation by suggesting that various layers of technical reliability might correspond to an equally diversified range of legal effects. Widespread concern was expressed that an enhanced electronic signature would be considered as if it were a distinct legal concept, rather than just a description of a collection of technical criteria, the use of which made a method of signing particularly reliable. While postponing its final decision as to whether the Uniform Rules would rely on the notion of "enhanced electronic signature", the Working Group generally agreed that, in preparing a revised draft of the Uniform Rules for continuation of the discussion at a future session, it would be useful to introduce a version of the draft articles that did not rely on that notion (A/CN.9/465, para. 66).

20. In view of that discussion of the need for a category of "enhanced electronic signatures", this revised draft of the Uniform Rules includes an alternative approach for discussion by the Working Group. The definition of "enhanced electronic signature" in draft article 2(b) has been maintained in square brackets but is not used in any of the substantive provisions of the Uniform Rules. Where appropriate, the relevant parts of that definition have been inserted in the corresponding provisions. The purpose of this approach is to assist the Working Group in deciding whether the references to both electronic and enhanced electronic signatures should be eliminated so that the Uniform Rules would deal only with a single category of electronic signature. Remarks addressing possible amendment of the definition are included under article 2. Remarks addressing specific proposals are dealt with under respective articles.

21. As agreed by the Working Group at its thirty-fifth session, this revised draft of the Uniform Rules is based on the assumption that the reference to situations "where the law requires a signature" is not limited to cases where an electronic signature is used to meet a mandatory requirement of law that certain documents be signed for validity purposes. Since the

law contains very few such requirements with respect to documents used for commercial transactions, the practical result of such misinterpretation would be to reduce unduly the scope of the Uniform Rules. Consistent with the interpretation of the words "the law" adopted by the Commission in paragraph 68 of the Guide to Enactment of the Model Law (under which "the words 'the law' are to be understood as encompassing not only statutory or regulatory law but also judicially-created law and other procedural law"), the Uniform Rules (and the Model Law) are intended to cover very broadly the use of electronic signatures, since most documents used in the context of commercial transactions are likely to be faced, in practice, with the requirements of the law of evidence regarding proof in writing (A/CN.9/465, para. 67).

II. DRAFT ARTICLES ON ELECTRONIC SIGNATURES

Article 1. Sphere of application

These Rules apply where electronic signatures are used in the context* of commercial** activities. They do not override any rule of law intended for the protection of consumers.

* The Commission suggests the following text for States that might wish to extend the applicability of these Rules:

"These Rules apply where electronic signatures are used, except in the following situations: [...]."

** The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

References to UNCITRAL documents

A/CN.9/465, paras. 36-42;
A/CN.9/WG.IV/WP.82, para. 21;
A/CN.9/457, paras. 53-64.

Remarks

22. The opening words of draft article 1 have been revised to ensure consistency with article 1 of the Model Law (see A/CN.9/465, para. 38). Footnote * is intended to reflect the same policy as adopted in the context of the Model Law, under which "nothing in the Model Law should prevent an enacting State from extending the scope of the Model Law to cover uses of electronic commerce outside the commercial sphere" (Guide to Enactment of the Model Law, para. 26). The Working Group at its thirty-fifth session decided that such policy should also apply with respect to electronic signatures (ibid., para. 39).

Article 2. Definitions

For the purposes of these Rules:

(a) "Electronic signature" means [data in electronic form in, affixed to, or logically associated with, a data message, and] [any method in relation to a data message] that may be used to identify the signature holder in relation to the data message and indicate the signature holder's approval of the information contained in the data message;

[(b) "Enhanced electronic signature" means an electronic signature in respect of which it can be shown, through the use of a [security procedure] [method], that the signature:

(i) is unique to the signature holder [for the purpose for][within the context in] which it is used;

(ii) was created and affixed to the data message by the signature holder or using a means under the sole control of the signature holder [and not by any other person];

[(iii) was created and is linked to the data message to which it relates in a manner which provides reliable assurance as to the integrity of the message";]]

(c) "Certificate" means a data message or other record which is issued by an information certifier and which purports to ascertain the identity of a person or entity who holds a particular [key pair] [signature device];

(d) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(e) "Signature holder" [device holder] [key holder] [subscriber] [signature device holder] [signer] [signatory] means a person by whom, or on whose behalf, an enhanced electronic signature can be created and affixed to a data message;

(f) "Information certifier" means a person or entity which, in the course of its business, engages in [providing identification services] [certifying information] which [are][is] used to support the use of [enhanced] electronic signatures.

References to UNCITRAL documents

A/CN.9/465, para. 42;
A/CN.9/WG.IV/WP.82, paras. 22-33;
A/CN.9/457, paras. 22-47; 66-67; 89; 109;
A/CN.9/WG.IV/WP.80, paras. 7-10;
A/CN.9/WG.IV/WP.79, para. 21;
A/CN.9/454, para. 20;
A/CN.9/WG.IV/WP.76, paras. 16-20;
A/CN.9/446, paras. 27-46 (draft article 1), 62-70 (draft article 4), 113-131 (draft article 8), 132-133 (draft article 9);
A/CN.9/WG.IV/WP.73, paras. 16-27, 37-38, 50-57, and 58-60;
A/CN.9/437, paras. 29-50 and 90-113 (draft articles A, B and C); and

A/CN.9/WG.IV/WP.71, paras. 52-60.

Remarks

23. The Working Group at its thirty-fifth session decided to postpone consideration of the definitions contained in draft article 2 until it had completed its review of the substantive provisions of the Uniform Rules (A/CN.9/465, para. 42).

Definition of "electronic signature"

24. The definition of electronic signature has been drafted in accordance with the decision of the Working Group at its thirty-fourth session (A/CN.9/457, paras. 23-32). The words in square brackets "[any method in relation to a data message]" are included in order to align the language of the definition in the Uniform Rules with that of article 7 of the Model Law.

Definition of "enhanced electronic signature"

25. At its thirty-fifth session, the Working Group discussed whether the notion of "enhanced electronic signature" should be used in the Uniform Rules. Support was expressed in favour of retaining the notion of enhanced electronic signature, which was described as particularly apt to provide certainty with respect to the use of a certain type of electronic signatures, namely digital signatures implemented through public-key infrastructure (PKI). In response, it was pointed out that the notion of "enhanced electronic signature" made the structure of the Uniform Rules unnecessarily complex. In addition, the notion of "enhanced electronic signature" would lend itself to misinterpretation by suggesting that various layers of technical reliability might correspond to an equally diversified range of legal effects. Widespread concern was expressed that an enhanced electronic signature would be considered as if it were a distinct legal concept, rather than just a description of a collection of technical criteria, the use of which made a method of signing particularly reliable. While postponing its final decision as to whether the Uniform Rules would rely on the notion of "enhanced electronic signature", the Working Group generally agreed that, in preparing a revised draft of the Uniform Rules for continuation of the discussion at a future session, it would be useful to introduce a version of the draft articles that did not rely on that notion (A/CN.9/465, para. 66).

26. In accordance with the decision of the Working Group at its thirty-fourth session (A/CN.9/457, para. 39), the definition of "enhanced electronic signature" includes in subparagraph (b)(iii) the language in square brackets as a necessary link between the enhanced signature on the data message and the information contained in the data message, in the form of an integrity function. The Working Group may wish to consider whether integrity should be included as an integral part of the definition of an enhanced electronic signature or whether, as a concept, it is more relevant to the idea of an original, as in article 8 of the Model Law and draft article 7 of these Uniform Rules. The wording previously included as subparagraph (ii), "can be used to identify objectively the signature holder in relation to the data message", has been omitted from the current draft on the basis that it is part of the definition of an "electronic signature" in subparagraph (a).

27. In the opening words of subparagraph (b), the reference to use of a "method", as an alternative to the use of a "security procedure", is intended to align more closely the terminology with that of the Model Law.

28. In subparagraph (b)(ii) the words "and not by any other person" have been placed in square brackets as their inclusion raises a number of issues. First, including those words in the definition of enhanced electronic signature may suggest that any signature that is not created and affixed by the signature device holder (and therefore potentially unauthorized) is not an enhanced electronic signature. This interpretation may have the effect of excluding such signatures from the scope of some articles of the Uniform Rules including, for example, draft articles 8, 9 and 11. In particular, the application of those parts of draft article 9 which deal with responsibility for compromise of signature devices could be uncertain.

29. Secondly, the inclusion of those words would require that, in order for a security procedure or method to be an enhanced electronic signature, it must be able to show that the signature was actually created and affixed by the signature device holder. Since for some technologies this may not be possible, including such a requirement may suggest the need for the use of a personal identifier, such as the use of biometrics or some other such technique, in conjunction with the use of the signature device.

30. A further issue which the Working Group may wish to consider in the context of subparagraph (b)(ii) is the relationship between the requirement for "sole control" and draft article 9, which provides for obligations of "each" signature device holder. This issue also arises in relation to the definition of "signature holder" below.

31. In subparagraph (b)(iii) the phrase "reliable assurance" is intended to maintain consistency with the terminology of article 8 of the Model Law.

Definition of "certificate"

32. A definition of "certificate" may be needed in the Uniform Rules for reasons of completeness. This definition is based upon the definition in A/CN.9/WG.IV/WP.79 of an "identity certificate", although no longer described in these Uniform Rules as an "identity certificate". The Working Group may wish to consider whether the words in square brackets, "or other significant characteristics", can be deleted for the following reason. The concept of identity may be more than a reference to the name of the signature device holder, and may refer to other significant characteristics, such as position or authority, either in combination with a name or without reference to the name. On that basis, it would not be necessary to distinguish between identity and other significant characteristics, nor to limit the Uniform Rules to those situations in which only identity certificates which named the signature device holder were used. For an alternative view of the meaning of "identity" see "Background Paper on Electronic Authentication Technologies and Issues", Joint OECD-Private Sector Workshop on Electronic Authentication, California, 2-4 June 1999, pages 6-9.

33. The Working Group may wish to consider whether the words "confirm the identity" is appropriate, on the basis that the certificate may not actually confirm the identity of the signature device holder, but rather identify the signature device holder by following certain procedures and certify that that identity is linked to the signature device or public key listed in the certificate. To ensure that the Uniform Rules are technology-neutral, the Working Group may also wish to consider the use of a technology-neutral formulation such as "signature device" or "signature creation device"as an alternative to the words "key pair", since "key pair" refers specifically to digital signatures. Use of the phrase "key pair" in relation to the definition of "certificate" may be appropriate in situations where certificates are only used in a digital signature context.

Definition of "data message"

34. A definition of "data message" may be needed in the draft Uniform Rules for reasons of completeness. The Working Group may wish to consider the need for inclusion of this definition in the context of the relationship of the Uniform Rules to the Model Law.

Definition of "signature holder"

35. The Working Group did not conclude its discussion on the definition of "signature holder" at its thirty-fourth session (A/CN.9/457, para. 47). The revised definition now includes, in square brackets, a number of terms which the Working Group considered may be more appropriate than "signature holder". This definition may need to be reviewed in the context of subparagraph (b)(ii) of the definition of "enhanced electronic signature" above and draft article 9, as noted at para. 30.

In view of a proposal made at the thirty-fifth session of the Working Group, the term "signature holder" has been replaced throughout this note by the term "signature device holder" (see A/CN.9/465, paras. 78-82).

Definition of "information certifier"

36. This definition was not considered by the Working Group at its previous session and remains unchanged. However, in view of earlier discussions (A/CN.9/457, para. 109), the Working Group may wish to consider whether the words "in the course of its business" in the definition of "information certifier" should be interpreted as implying that certification-related activities should be the exclusive business activity of an information certifier or whether, in order to embrace situations such as those where credit card companies would issue certificates, the issuance of certificates as an incidental part of the business of an entity should also be covered. Taking into account a suggestion made at the thirty-fifth session of the Working Group, the term "information certifier" has been replaced throughout the remainder of the Uniform Rules, by the term "supplier of certification services" (A/CN.9/465, para. 125). The Working Group may wish to make a decision as to which terminology should be used.

References to national legislation and other texts

ABA Guidelines

Part 1: Definitions

1.5 Certificate

A message which at least

(1) identifies the certification authority issuing it,
(2) names or identifies its subscriber,
(3) contains the subscriber's public key,
(4) identifies the operational period, and
(5) is digitally signed by the certification authority issuing it.

1.6 Certification Authority

A person who issues a certificate.

1.27 Relying party

A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

1.30 Signer

A person who creates a digital signature for a message.

1.31 Subscriber

A person who

(1) is the subject named or identified in a certificate issued to such person, and
(2) holds a private key that corresponds to a public key listed in that certificate.

EC Directive

Article 2

Definitions

For the purpose of this Directive:

1. "electronic signature" means data in electronic form attached to, or logically associated with, other electronic data and which serves as a method of authentication.
2. "advanced electronic signature" means an electronic signature which 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;
3. "signatory" means a person who holds a signature creation device and acts either on their own behalf or on the behalf of the natural or legal person or entity he represents;

4. "signature-creation data" means unique data such as codes or private cryptographic keys, which is used by the signatory in creating an electronic signature;
5. "signature-creation device" means configured software or hardware used to implement the signature-creation data;
6. "secure-signature-creation device" is a signature-creation device that meets the requirements laid down in Annex III;
7. "signature-verification data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying the electronic signature;
8. "signature-verification device" means configured software or hardware used to implement the signature-verification data;
9. "certificate" means an electronic attestation which links a signature-verification data to a person, and confirms the identity of that person;
10. "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service provider who fulfils the requirements laid down in Annex II;
11. "certification-service provider" means an entity or a natural or legal person who issues certificates or provides other services related to electronic signatures;
[...].

GUIDEC

VI. Glossary of terms
2. Certificate
A message ensured by a person, which message attests to the accuracy of facts material to the legal efficacy of the act of another person.

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

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

14. Subscriber
A person who is the subject of a certificate.

Germany

§2 Definitions
(1) A digital signature within the meaning of this law is a seal on digital data created with a private signature key, which seal allows, by use of the associated public key to which a signature key certificate of a certifier or of the Authority under § 3 is affixed, the owner of the signature key and the unforged character of the data to be ascertained.
(2) A certifier within the meaning of this law is a natural or legal person which attests to the attribution of public signature keys to natural persons and holds a license therefor under § 4;
(3) A certificate within the meaning of this law is a digital attestation concerning the attribution of a public signature key to a natural person to which a digital signature is affixed (signature key certificate), or a special digital attestation which refers unmistakably to a signature key certificate and contains further information (attribute certificate).

Illinois

Article 5. Electronic records and signature generally
Section 5-105. Definitions
“Certificate” means a record that at a minimum: (a) identifies the certification authority issuing it, (b) names or otherwise identifies its subscriber, or a device or electronic agent under the control of the subscriber; (c) contains a public key that corresponds to a private key under the control of the subscriber; (d) specifies its operational period; and (e) is digitally signed by the certification authority issuing it.

“Certification authority” means a person who authorizes and causes the issuance of a certificate.

“Electronic signature” means a signature in electronic form attached to or logically associated with an electronic record.

“Signature device” means unique information, such as codes, algorithms, letters, numbers, private keys, or personal identification numbers (PINS), or a uniquely configured physical device, that is required, alone or in conjunction with other information or devices, in order to create an electronic signature attributable to a specific person.

Singapore

Part 1. Section 2. Interpretation
“certificate” means a record issued for the purpose of supporting digital signatures which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;

"certification authority" means a person who or an organisation that issues a certificate;

"electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record;

"key pair", in an asymmetric cryptosystem, means a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates;

"private key" means the key of a key pair used to create a digital signature;

"public key" means the key of a key pair used to verify a digital signature;

"subscriber" means a person who is the subject named or identified in a certificate issued to him and who holds a private key that corresponds to a public key listed in that certificate.

Article 3. [Technology neutrality] [Equal treatment of signatures]

None of the provisions of these Rules shall be applied so as to exclude, restrict, or deprive of legal effect any method [of electronic signature] [that satisfies the requirements referred to in article 6(1) of these Rules] [which 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] [or otherwise meets the requirements of applicable law].

References to UNCITRAL documents

A/CN.9/465, paras. 43-48;
A/CN.9/WG.IV/WP.82, para. 34;
A/CN.9/457, paras. 53-64.

Remarks

37. Draft article 3 is intended to reflect some of the drafting suggestions made in the context of the thirty-fifth session of the Working Group (A/CN.9/465, paras. 47-48). In the context of its discussion of draft article 3, the Working Group may wish to decide whether the Uniform Rules should make it clear that any method being used or contemplated for purposes other than creating the functional equivalent of a legally significant handwritten signature (i.e., a method meeting the requirements of draft article 6 or otherwise meeting the requirements of applicable law) does not fall within the scope of the Uniform Rules.

Article 4. Interpretation

(1) In the interpretation of these Uniform Rules, regard is to be had to their international origin and to the need to promote uniformity in their application and the observance of good faith.

(2) Questions concerning matters governed by these Uniform Rules which are not expressly settled in them are to be settled in conformity with the general principles on which these Uniform Rules are based.

References to UNCITRAL documents

A/CN.9/465, paras. 49-50;
A/CN.9/WG.IV/WP.82, para. 35.

Remarks

38. The substance of draft article 4 has been generally agreed upon by the Working Group at its thirty-fifth session (A/CN.9/465, para. 50).

Article 5. [Variation by agreement] [Party autonomy] [Freedom of contract]

These Rules may be derogated from or [their effect may be] varied by agreement, unless otherwise provided in these Rules or in the law of the enacting State.

References to UNCITRAL documents

A/CN.9/465, paras. 51-61;
A/CN.9/WG.IV/WP.82, paras. 36-40;
A/CN.9/457, paras. 53-64.

Remarks

39. The text of draft article 5 reflects a proposal which was widely supported by the Working Group at its thirty-fifth session (A/CN.9/465, para. 59), to the effect of ensuring the freedom of the parties, as among themselves, to derogate from or vary the provisions of these Rules. This autonomy provision relates only to these Rules, and is not intended to affect *ordre public* or mandatory laws applicable to contracts, such as provisions relating to unconscionable contracts.

40. The wording in square brackets has been included as a possible formulation following more closely the wording of article 6 of the United Nations Convention on Contracts for the International Sale of Goods (hereinafter referred to as "the Sales Convention"), as suggested by the Working Group (ibid., para. 61).

Article 6. [Compliance with requirements for signature] [Presumption of signing]

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if [a method] [an electronic signature] is used which 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.

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

Variant A

(3) It is presumed that [a method] [an electronic signature] is reliable for the purpose of satisfying the requirement referred to in paragraph (1) if that method ensures that:

(a) the data used for the creation of an electronic signature are unique to the holder of the signature [creation] device within the context in which they are used;

(b) the holder of the signature [creation] device [has] [had at the relevant time] sole control of that device;

(c) the electronic signature is linked to the [information] [the data message or the part of that message] to which it relates [in a manner which guarantees the integrity of that information];

(d) the holder of the signature [creation] device is objectively identified within the context [in which the device is used][of the data message].

Variant B

(3) In the absence of proof to the contrary, the use of an electronic signature is presumed to prove:

(a) that the electronic signature meets the standard of reliability set out in paragraph (1);

(b) the identity of the alleged signer; and

(c) that the alleged signer approved the information to which the electronic signature relates.

(4) The presumption in paragraph (3) applies only if:

(a) the person who intends to rely on the electronic signature notifies the alleged signer that the electronic signature is being relied upon [as equivalent to the hand-written signature of the alleged signer][as proof of the elements listed in paragraph (3)]; and

(b) the alleged signer fails to notify promptly the person who issues a notification under subparagraph (a) of the reasons for which the electronic signature should not be relied upon [as equivalent to the hand-written signature of the alleged signer][as proof of the elements listed in paragraph (3)].

Variant C

(3) In the absence of proof to the contrary, the use of an electronic signature is presumed to prove:

(a) that the electronic signature meets the standard of reliability set out in paragraph (1);

(b) the identity of the alleged signer; and

(c) that the alleged signer approved the information to which the electronic signature relates.

[(4)][(5)] The provisions of this article do not apply to the following: [...].

References to UNCITRAL documents

A/CN.9/465, paras. 62-82;

A/CN.9/WG.IV/WP.82, paras. 42-44;
A/CN.9/457, paras. 48-52;
A/CN.9/WG.IV/WP.80, paras. 11-12.

Remarks

41. Paragraphs (1) and (2), and the last paragraph of draft article 6 introduce provisions drawn from article 7(1)(b), 7(2), and 7(3) of the Model Law, respectively. Wording inspired by article 7(1)(a) of the Model Law is already included in the definition of "electronic signature" under draft article 2(a). However, draft article 2(a) describes a method that "may" be used to fulfil the functions of a signature identified in article 7(1)(a) of the Model Law. Should the Working Group wish to emphasize that the main goal of paragraph (1) is to deal with the case where any type of electronic signature (including "non-enhanced" methods of authentication) is used for signing purposes (i.e., with intent to create a functional equivalent to a hand-written signature), the Working Group may find it more appropriate to reproduce the entire text of article 7(1) of the Model Law. Paragraph (1) could read as follows:

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

"(a) [a method] [an electronic signature] 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] [electronic signature] 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".

42. A suggestion was made at the thirty-fifth session of the Working Group that a provision might need to be included in draft article 6 along the following lines: "The legal consequences of the use of a signature shall apply equally to the use of electronic signatures" (see A/CN.9/465, para. 74). The Working Group may wish to discuss the extent to which this notion of equivalence between handwritten and electronic signatures should be further expressed in the body of the Uniform Rules or whether it might be sufficient (and more consistent with the Model Law) to indicate in the guide to enactment (to be prepared at a later stage) that, in interpreting paragraph (1), it should be borne in mind that the purpose of that provision was to ensure that, where any legal consequence would have flowed from the use of a handwritten signature, the same consequence should flow from the use of a reliable electronic signature.

43. As indicated in the report of the thirty-fifth session of the Working Group (A/CN.9/465, para. 64), paragraph (1), to the extent it reproduces article 7(1) of the Model Law, deals with the determination of what constitutes a reliable method of signature in the light of the circumstances. Such a determination can only be made under article 7 of the Model Law by a court or other trier of fact intervening *ex post*, possibly long after the electronic signature has been used. In contrast, the benefit expected from the Uniform Rules in favour of certain techniques, which are recognized as particularly reliable, irrespective of the circumstances in which they are used, is to create certainty (through either a presumption or a substantive rule), at or before the time any such technique of electronic signature is used (*ex ante*), that using such a recognized technique will result in legal effects equivalent to those of a handwritten signature. That is the purpose of paragraph (3).

44. Variant A of paragraph (3) is based on language proposed and discussed at the thirty-fifth session of the Working Group (A/CN.9/465, paras. 78-82) for expressing objective criteria of technical reliability of electronic signatures. In subparagraph (c), the necessary linkage between the signature and the information being signed has been expressed so as to avoid the implication that the electronic signature could apply only to the full contents of a data message. In fact, the information being signed, in many instances, will be only a portion of the information contained in the data message.

45. In discussing Variants B and C, the Working Group may wish to clarify, as a matter of policy, whether the Uniform Rules, in establishing criteria of "reliability" of an electronic signature, should deal exclusively with the issues of technical reliability envisaged under Variant A or whether other factors should be taken into account, as an alternative or as an addition to Variant A.

46. Variant B results from a proposal made at the thirty-fifth session of the Working Group (A/CN.9/465, paras. 74-75). If adopting Variant B implies the elimination of any linkage between a given level of technical reliability, on the one hand, and the legal consequences that would result from the use of electronic signatures, on the other hand, the effect of paragraphs (3) and (4) would be to create, in favour of any technique that might be used to produce an electronic signature, what has sometimes been referred to as a "low level presumption", i.e., a presumption that could be easily rebutted by the purported signer through a mere declaration. The Working Group may wish to decide, as a matter of policy, whether the exchange of notices contemplated in Variant B can realistically be imposed on users of electronic signatures, and whether such an exchange of notices would result in the expected level of user-friendliness and pre-determined certainty as to the legal effects of electronic signatures.

47. Variant C results from a proposal made at the thirty-fifth session of the Working Group (A/CN.9/465, para. 76). Contrary to Variant B, it does not offer a mechanism for easy rebuttal of the presumption it creates. In view of the fact that "proof to the contrary" might require detailed and costly investigations of the various technical devices and procedures involved in the creation of the electronic signature, the effect of Variant C would be to create a very strong presumption as to the legal effectiveness of any technique used to produce an electronic signature.

References to national legislation and other texts

EC Directive

Article 5
Legal Effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

(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.

2. Member States shall 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.

Singapore

Part V. Secure electronic records and signatures
Secure electronic signature

17. If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —

(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 such that if the record was changed the electronic signature would be invalidated,

such signature shall be treated as a secure electronic signature.

Presumptions relating to secure electronic records and signatures

18. [...]

(2) In any proceedings involving a secure electronic signature, it shall be presumed, unless evidence to the contrary is adduced, that —

(a) the secure electronic signature is the signature of the person to whom it correlates; and

(b) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

[Article 7. Presumption of original

(1) A data message is presumed to be in its original form where, in relation to that data message, [a method] [an electronic signature] [within article 6] is used which:

(a) provides 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

(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;

(2) The provisions of this article do not apply to the following: [...].]

References to UNCITRAL documents

A/CN.9/465, paras. 83-89;
A/CN.9/WG.IV/WP.82, para. 45;
A/CN.9/457, paras. 48-52;
A/CN.9/WG.IV/WP.80, paras. 13-14.

Remarks

48. The text of draft article 7 results from the decision made by the Working Group at its thirty-fifth session (A/CN.9/465, para. 89). The purpose of draft article 7 is to confirm the connection with article 8 of the Model Law and the requirement of integrity. As currently drafted, paragraph (1) does not imply any linkage between the function of preserving the integrity of the information and the signature function under draft article 6. The independence of the two articles, which may apply cumulatively or separately to various authentication techniques, is based on a recognition of the fact that, in a paper-based environment, the corresponding two functions can also be conceived as separate.

Article 8. Satisfaction of articles 6 and 7

Variant A

(1) *[The organ or authority specified by the enacting State as competent]* may determine which methods satisfy the requirements of articles 6 and 7.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

Variant B

(1) One or more methods of electronic signature may be determined as satisfying the requirements of articles 6 and 7.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

References to UNCITRAL documents

A/CN.9/465, paras. 90-98;
A/CN.9/WG.IV/WP.82, para. 46;
A/CN.9/457, paras. 48-52;
A/CN.9/WG.IV/WP.80, para. 15.

Remarks

49. The purpose of draft article 8 is to make it clear that an enacting State may designate an organ or authority that will have the power to make determinations on what specific technologies may benefit from the presumptions established in draft articles 6 and 7. As decided by the Working Group at its thirty-fifth session, draft article 8 should not be interpreted in a manner that would prohibit users, for example, from using techniques which had not been determined to satisfy draft articles 6 and 7, if that was what they had agreed to do, as among themselves. Parties should also be free to show, before a court or an arbitral tribunal, that the method of signature they had chosen to use did satisfy the requirements of draft articles 6 and 7, even though not the subject of a prior determination to that effect. Draft article 8 should not be seen as making a recommendation to States as to the only means of achieving recognition of signature technologies, but rather as indicating the limitations that should apply if States wished to adopt such an approach. These points might need to be clearly explained, possibly in a guide to the enactment of the Uniform Rules (see A/CN.9/465, para. 93).

50. The purpose of both Variants A and B is to encourage States to ensure that determinations made under paragraph (1) conform with international standards where applicable, thus facilitating harmonization of practices with respect to enhanced electronic signatures and cross-border use and recognition of signatures. Variant A refers to a possible intervention by the State in the designation of an organ or authority competent to assess the technical reliability of signature techniques (irrespective of whether that organ is established as a public or private entity). Variant B, in order not to over-emphasize the role of the State in making the determinations referred to in paragraph (1), leaves it open whether any organ or authority set up to assess the technical reliability of signature techniques should be established by the State (either as a State organ or as a private entity) or purely industry-based.

51. A proposal made in the context of the thirty-fifth session of the Working Group (namely, that "any determination made should take into account not only whether certain methods satisfied the requirements of draft articles 6 and 7 but also the degree or extent to which those requirements were met"), has not been reflected in the revised version of draft article 8. The Working Group may wish to clarify whether it is envisaged that a requirement such as the use of a handwritten signature (or the production of an original document) could be met only in part with respect to a document processed in an electronic environment, which would seem to depart from the functional-equivalence approach taken throughout the preparation of the Model Law and the Uniform Rules. If the intent of the Working Group is merely to indicate that an electronic signature (or a method ensuring integrity) does not necessarily apply to the entire contents of a data message but should be capable of applying only to a chosen part of the information contained in a given message, that indication may easily be provided in the guide to enactment.

Article 9. Responsibilities of the signature device holder

(1) Each signature device holder shall:

(a) Exercise reasonable care to avoid unauthorized use of its signature device;

(b) Notify appropriate persons without undue delay if:

(i) the signature device holder knows that the signature device has been compromised; or

(ii) the circumstances known to the signature device holder give rise to a substantial risk that the signature device may have been compromised;

(c) [Where a certificate is used to support the signature device,] [Where the signature device involves the use of a certificate,] exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signature device holder which are relevant to [the life-cycle of the] certificate, or which are to be included in the certificate.

(2) A signature device holder shall be liable for its failure to satisfy the requirements of paragraph (1).

References to UNCITRAL documents

A/CN.9/465, paras. 99-108;
A/CN.9/WG.IV/WP.82, paras. 50-55;
A/CN.9/457, paras. 65-98;
A/CN.9/WG.IV/WP.80, paras. 18-19.

Remarks

52. The substance of draft article 9 has been largely approved by the Working Group at its thirty-fifth session. In paragraph (1), the reference to "each" holder has been introduced to reflect the general view that, in certain cases, it might be unfair to provide that each holder of the device was liable for the entire loss that might have resulted from unauthorized use of the device (e.g., in case of unauthorized use of a corporate signature device held by a number of employees). Accordingly, each holder should only be liable to the extent that it had personally failed to meet the requirements in paragraph (1) (see A/CN.9/465, para. 105).

53. Paragraph (2) is based on the conclusion reached by the Working Group at its thirty-fifth session that it might be difficult to achieve consensus as to what consequences might flow from the liability of the signature device holder. Depending on the context in which the electronic signature was used, such consequences might range, under existing law, from the signature device holder being bound by the contents of the message to liability for damages. Accordingly, paragraph (2) merely establishes the principle that the signature device holder should be held liable for failure to meet the requirements of paragraph (1), and leaves it to the law applicable outside the Uniform Rules in each enacting State to deal with the legal consequences that would flow from such liability (ibid., para. 108). Another view was that a rule based on a test of foreseeability of damage (along the lines of article 74 of the Sales Convention, and restating a basic rule which

would apply under readily applicable law in many countries) should have been introduced in draft article 9 (ibid., para. 107).

References to national legislation and other texts

Paragraph (1)(a) - material representations

ABA Guidelines

4.2 Subscriber's obligations
All material representations made by the subscriber to a certification authority, including all information known to the subscriber and represented in the certificate, must be accurate to best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the certification authority.

GUIDEC

VII. Ensuring a message
7. Representations to a Certifier
A subscriber must accurately represent to a certifier all facts material to the certificate.

Illinois

Article 20. Duties of subscribers
Section 20-101 Obtaining a certificate
All material representations knowingly made by a person to a certification authority for purposes of obtaining a certificate naming such person as a subscriber must be accurate and complete to best of such person's knowledge and belief.

Section 20-105 Acceptance of a certificate
[...]
(b) By accepting a certificate, the subscriber listed in the certificate represents to any person who reasonably relies on information contained in the certificate, in good faith and during its operational period, that:
(1) the subscriber rightfully holds the private key corresponding to public key listed in the certificate;
(2) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and
(3) all information in the certificate that is within the knowledge of the subscriber is true.

Singapore

Part IX. Duties of subscribers
Obtaining certificate
37. All material representations made by the subscriber to a certification authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in the certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the certification authority.

Paragraph (1)(b) - notification

ABA Guidelines

4.4 Initiating suspension or revocation
A subscriber who has accepted a certificate must request the issuing certification authority to suspend or revoke the certificate if the private key corresponding to the public key listed in the certificate has been compromised.

Illinois

Article 20. Duties of subscribers
Section 20-110 Revocation of a certificate
Except as otherwise provided by another applicable rule of law, if the private key corresponding to the public key listed in a valid certificate is lost, stolen, accessible to an unauthorized person, or otherwise compromised during the operational period of the certificate, a subscriber who has learned of the compromise

must promptly request the issuing certification authority to revoke the certificate and publish notice of revocation in all repositories in which the subscriber previously authorized the certificate to be published, or otherwise provide reasonable notice of the revocation.

Section 10-125 Creation and control of signature devices
Except as otherwise provided by another applicable rule of law, whenever the creation, validity, or reliability of an electronic signature created by a qualified security procedure under [...] is dependent upon the secrecy or control of a signature device of the signer:

(1) the person generating or creating the signature device must do so in a trustworthy manner;

(2) the signer and all other persons that rightfully have access to such signature device must exercise reasonable care to retain control and maintain the secrecy of the signature device, and to protect it from any unauthorised access, disclosure, or use, during the period when reliance on a signature created by such device is reasonable;

(3) in the event that the signer, or any other person that rightfully has access to such signature device, knows or has reason to know that the secrecy or control of any such signature device has been compromised, such person must make a reasonable effort to promptly notify all persons that such person knows might foreseeably be damaged as a result of such compromise, or where an appropriate publication mechanism is available [...], to publish notice of the compromise and a disavowal of any signatures created thereafter.

Singapore

Initiating suspension or revocation
40. A subscriber who has accepted a certificate shall as soon as possible request the issuing certification authority to suspend or revoke the certificate if the private key corresponding to the public key listed in the certificate has been compromised.

Paragraph (1)(c) - unauthorized use

ABA Guidelines

4.3 Safeguarding the private key
During the operational period of a valid certificate, the subscriber shall not compromise the private key corresponding to a public key listed in such certificate, and must also avoid compromise during any period of suspension.

GUIDEC

VII. Ensuring a message
6. Safeguarding an Ensuring Device
If a person ensures a message by means of a device, the person must exercise, at a minimum, reasonable care to prevent unauthorised use of the device.

Illinois

Section 10-125 Creation and control of signature devices
Except as otherwise provided by another applicable rule of law, whenever the creation, validity, or reliability of an electronic signature created by a qualified security procedure under [...] is dependent upon the secrecy or control of a signature device of the signer:

(1) the person generating or creating the signature device must do so in trustworthy manner;

(2) the signer and all other persons that rightfully have access to such signature device must exercise reasonable care to retain control and maintain the secrecy of the signature device, and to protect it from any unauthorized access, disclosure, or use, during the period when reliance on a signature created by such device is reasonable;

(3) in the event that the signer, or any other person that rightfully have access to such signature device, knows or has reason to know that the secrecy or control of any such signature device has been compromised, such person must make a reasonable effort to promptly notify all persons that such person knows might foreseeably be damaged as a result of such compromise, or where an appropriate publication mechanism is available [...] to publish notice of the compromise and a disavowal of any signature created thereafter.

Paragraph (2) - liability

Minnesota

325K.12 Representations and duties upon accepting certificates
Subd.4 Indemnification by subscriber
By accepting a certificate, a subscriber undertakes to indemnify the issuing certification authority for loss or damage caused by issuance or publication of a certificate in reliance on:

(1) a false and material representation of fact by the subscriber;
(2) the failure by the subscriber to disclose a material fact if the representation or failure to disclose was made either with intent to deceive the certification authority or a person relying on the certificate, or with gross negligence. The indemnity provided in this section may not be disclaimed or contractually limited in scope. However, a contract may provide consistent, additional terms regarding the indemnification.

Singapore

Part IX. Duties of subscribers
Control of private key
39. (1) By accepting a certificate issued by a certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such certificate and prevent its disclosure to a person not authorized to create the subscriber's digital signature.
(2) Such duty shall continue during the operational period of the certificate and during any period of suspension of the certificate.

Article 10. Responsibilities of a supplier of certification services

(1) A supplier of certification services shall:

(a) act in accordance with the representations it makes with respect to its practices;

(b) exercise due diligence to ensure the accuracy and completeness of all material representations made by the supplier of certification services that are relevant to the life-cycle of the certificate or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain:

(i) the identity of the supplier of certification services;

(ii) that the person who is identified in the certificate holds, at the relevant time, the signature device referred to in the certificate;

(iii) the method used to identify the signature device holder;

(iv) any limitations on the purposes or value for which the signature device may be used; and

(v) whether the signature device is valid and has not been compromised;

(d) Provide a means for signature device holders to give notice that a signature device has been compromised and ensure the operation of a timely revocation service;

(e) Utilize trustworthy systems, procedures and human resources in performing its services.

(2) In determining whether and the extent to which any systems, procedures and human resources are trustworthy for the purposes of subparagraph (e) of paragraph (1), regard shall be had to the following factors:

(a) financial and human resources, including existence of assets within the jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the supplier of certification services regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and

(h) the degree of discrepancy between the law applicable to the conduct of the supplier of certification services and the law of the enacting State.

(3) A certificate shall state:

(a) the identity of the supplier of certification services;

(b) that the person who is identified in the certificate holds, at the relevant time, the signature device referred to in the certificate;

(c) that the signature device was effective at or before the date when the certificate was issued;

(d) any limitations on the purposes or value for which the certificate may be used; and

(e) any limitation on the scope or extent of liability which the supplier of certification services accepts to any person.

Variant X

(4) A supplier of certification services shall be liable for its failure to satisfy the requirements of paragraph (1).

(5) Liability of the supplier of certification services may not exceed the loss which the supplier of certification services foresaw or ought to have foreseen at the time of its failure in the light of facts or matters which the supplier of certification services knew or ought to have known to be possible consequences of the supplier of certification services' failure to [fulfil the obligations [duties] in][satisfy the requirements of] paragraph (1).

Variant Y

(4) A supplier of certification services shall be liable for its failure to satisfy the requirements of paragraph (1).

(5) In assessing the loss, regard shall be had to the following factors:

(a) the cost of obtaining the certificate;

(b) the nature of the information being certified;

(c) the existence and extent of any limitation on the purpose for which the certificate may be used;

(d) the existence of any statement limiting the scope or extent of the liability of the supplier of certification services; and

(e) any contributory conduct by the relying party.

Variant Z

(4) If damage has been caused as a result of the certificate being incorrect or defective, a supplier of certification services shall be liable for damage suffered by either:

(a) a party who has contracted with the supplier of certification services for the provision of a certificate; or

(b) any person who reasonably relies on a certificate issued by the supplier of certification services.

(5) A supplier of certification services shall not be liable under paragraph (2):

(a) if, and to the extent, it included in the certificate a statement limiting the scope or extent of its liability to any relevant person; or

(b) if it proves that it [was not negligent][took all reasonable measures to prevent the damage].

References to UNCITRAL documents

A/CN.9/465, paras. 123-142 (draft article 12);
A/CN.9/WG.IV/WP.82, paras. 59-68 (draft article 12);
A/CN.9/457, paras. 108-119;
A/CN.9/WG.IV/WP.80, paras. 22-24.

Remarks

54. Draft article 10 (formerly draft article 12) has been revised in accordance with decisions of the Working Group at its thirty-fifth session.

55. The substance of paragraph (1) has been found largely acceptable by the Working Group at its previous session, subject to minor drafting changes. Paragraph (2) results from a proposal made at that session to the effect that the characteristics of a supplier of certification services as described in draft article 13 should be taken into account not only in respect of foreign entities but should equally apply to domestic suppliers of certification services (A/CN.9/465, para. 136).

56. Paragraph (3) results from a proposal, which was also met with considerable interest by the Working Group at its previous session, under which draft article 12 should establish an additional rule setting out the minimum contents of a certificate (ibid., para. 135). While the elements to be contained in a certificate are listed in a separate paragraph, it is doubtful whether paragraph (1)(c) and paragraph (3) should be kept as separate provisions. The Working Group may wish

to clarify whether those two lists should be merged, presumably in subparagraph (1)(c), which could open with wording along the following lines: "indicate in each certificate ...".

57. Paragraphs (4) and (5) deal with the liability of the supplier of certification services.

58. In Variants X and Y, paragraph (4) establishes a rule that the supplier of certification services is responsible for its failure to observe the obligations or duties in paragraph (1), but leaves it up to national law to determine what the consequences of that failure might be.

59. Paragraph (5) of Variant X establishes a rule of foreseeability of damage based upon article 74 of the Sales Convention, This paragraph operates to limit the quantum of any liability of the supplier of certification services which might arise from paragraphs (1) and (2). In Variant Y, paragraph (5) is based on a suggestion made at the thirty-fifth session of the Working Group (A/CN.9/465, para. 140), according to which the Uniform Rules, without interfering with the operation of domestic law, might provide a list of factors to be taken into consideration when applying domestic law to suppliers of certification services.

60. Variant Z was not discussed during the thirty-fifth session of the Working Group. It originates in a feeling, which was widely expressed at the thirty-fourth session of the Working Group (A/CN.9/457, para. 115), that it would be appropriate to create a uniform rule that went beyond merely referring to the applicable law and established a general rule of liability for negligence, subject to possible contractual exemptions (provided that the limitation would not be grossly unfair) and subject to the supplier of certification services exonerating itself by demonstrating that it had fulfilled the obligations under paragraph (1). Paragraph (4) of Variant Z deals with the question of to whom the supplier of certification services may be liable. Paragraph (5) provides a rule permitting the supplier of certification services to rely on any limitation of liability set out in the certificate or to show that it was not negligent or took reasonable measures to prevent the damage occurring (A/CN.9/WG.IV/WP.82, para. 67).

References to national legislation and other texts

Paragraphs (1), (2) and (3) - general duties

ABA Guidelines

3 Certification Authorities

3.1 Certification authority must use trustworthy systems

A certification authority must utilize trustworthy systems in performing its services**.**

3.2 Disclosure

(1) A certification authority must disclose any material certification practice statement, as well as notice of the revocation or suspension of a certification authority certificate.

(2) A certification authority must use reasonable efforts to notify any persons who are known to be or foreseeably will be affected by the revocation or suspension of its certification authority certificate.

(3) [...]

(4) In the event of an occurrence which materially and adversely affects a certification authority's trustworthy system or its certification authority certificate, the certification authority must use reasonable efforts to notify any persons who are known to be or foreseeably will be affected by that occurrence, or act in accordance with procedures specified in its certification practice statement.

3.7 Certification authority's representations in certificate

By issuing a certificate, a certification authority represents to any person who reasonably relies on certificate or a digital signature verifiable by the public key listed in the certificate, that the certification authority, in accordance with any applicable certification practice statement of which the relying person has notice, has confirmed that

(1) the certification authority has complied with all applicable requirements of these Guidelines in issuing certificate, and if the certification authority has published the certificate or otherwise made it available to such reasonably relying person, that the subscriber listed in the certificate has accepted it,

(2) the subscriber identified in the certificate holds the private key corresponding to the public key is listed in the certificate,

(3) [...]
(4) the subscriber's public key and private key constitute a functioning key pair, and
(5) all information in the certificate is accurate, unless the certification authority has stated in the certificate or incorporated by reference in the certificate that the accuracy of specified information is not confirmed.

Further, the certification authority represents that there are no known, material facts omitted from the certificate which would, if known, adversely affect the reliability of its representations under this Guideline.

3.9 Suspension of certificate at subscriber's request
Unless a contract between the certification authority and the subscriber provides otherwise, a certification authority must suspend a certificate as soon as possible after a request by a person whom the certification authority reasonably believes to be
(1) the subscriber listed in the certificate,
(2) a person duly authorized to act for that subscriber, or
(3) a person acting on behalf of that subscriber, who is unavailable.

3.10 Revocation of certificate at subscriber's request
The certification authority which issued a certificate must revoke it at the request of the subscriber listed in it, if the certification authority has confirmed
(1) that person requesting revocation is the subscriber listed in the certificate to be revoked, or
(2) if the requester is acting as an agent, that the requester has sufficient authority to effect revocation.

3.11 Revocation or suspension without the subscriber's consent
A certification authority must suspend or revoke a certificate, regardless of whether the subscriber listed in the certificate consents, if the certification authority confirms that
(1) a material fact represented in the certificate in false,
(2) a material prerequisite to issuance of the certificate was not satisfied, or
(3) the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability.
Upon affecting such a suspension, or revocation, the certification authority must promptly notify the subscriber listed in the suspended or revoked certificate.

3.12 Notice of suspension or revocation
Promptly upon suspending or revoking a certificate, a certification authority must publish notice of the suspension or revocation if the certificate was published, and otherwise must disclose the fact of suspension or revocation on inquiry by a relying party.

EC Directive

Annex II Requirements for certification service providers issuing qualified certificates
Certification service providers must:
(a) demonstrate the reliability necessary for offering certification services;
(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
(e) employ personnel which possesses the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the processes supported by them;
(g) take measures against forgery of certificates, and, in cases where the certification-service provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
(j) not store or copy signature-creation data of the person to whom the certification-service provider provided key management services;
(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature, inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third parties relying on the certificate;
(l) use trustworthy systems to store certificates in a verifiable form so that
- only authorised persons can make entries and changes,
- information can be checked for authenticity,

- certificates are publicly available for retrieval only in those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

GUIDEC

VIII Certification

2. Accuracy of representations in certificate

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

3. Trustworthiness of a certifier

A certifier must:

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

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

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

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

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

4. Notice of Practices and Problems

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

(a) any material certification practice statement, and

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

8. Suspension of public key certificate by request

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

9. Revocation of public key certificate by request

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

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

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

10. Suspension or revocation of public key certificate without consent

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

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

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

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

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

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

Germany

§5 Issuance of certificates

(1) The certifier shall reliably identify persons who apply for a certificate. It shall confirm the attribution of a public signature key to an identified person by a signature key certificate and shall maintain access to such, as well as to attribute certificates, at all times and for everyone over publicly accessible telecommunications channels in a verifiable manner and with the agreement of the signature key owner.

(2) Upon request of an applicant, the certifier shall record information concerning the applicant's power of representation for a third party or its professional or other licensing in the signature key certificate or in an attribute certificate, insofar as such licensing or the consent of the third party that the power of representation be recorded is reliably demonstrated.

(3) Upon request of an applicant, the certifier shall record a pseudonym in the certificate in place of the applicant's name.

(4) The certifier shall take measures so that data for certificates cannot be forged or falsified in a way which is not visible. It shall furthermore take steps so that the confidentiality of private signature keys is guaranteed. Private signature keys may not be stored by a certifier.

(5) It shall use reliable personnel for the exercise of certification activities, and shall use technical components in accordance §14 for making signature keys accessible and creating certificates. This also applies to technical components which make possible the verification of certificates under para. 1, sentence 2.

§6 Duty of instruction

The certifier shall instruct the applicant under § 5 para. 1 concerning the measures necessary to contribute to secure digital signatures and their reliable verification. It shall instruct the applicant concerning which technical components fulfil the requirements of § 14, paras. 1 and 2, as well as concerning the attribution of digital signatures created with a private signature key. It shall point out to the applicant that data with digital signatures may need to be re-signed before the security value of an available signature decreases with time.

§8 Blocking of certificates

(1) A certifier shall block a certificate if a signature key owner or his representative so request, if the certificate was issued based on false information under § 7, if the certifier has ended its activities and they are not continued by another certifier, or if the Authority orders blocking under § 13, para. 5, sentence 2. The blocking shall indicate the time from which it applies. Retroactive blocking is not permitted.

Illinois

Article 15. Effect of a digital signature

Section 15-301. Trustworthy services

Except as conspicuously set forth in its certification practice statement, a certification authority and a person maintaining a repository must maintain its operation and perform its services in a trustworthy manner.

Section 15-305. Disclosure

(a) For each certificate issued by a certification authority with the intention that it will be relied upon by third parties to verify digital signature created by subscribers, a certification authority must publish or otherwise make available to the subscriber and all such relying parties:

(1) its certification practice statement, if any, applicable thereto; and

(2) its certificate that identifies the certification authority as a subscriber and that contains the public key corresponding to the private key used by the certification authority to digitally sign the certificate (its "certification authority certificate").

(b) In the event of an occurrence that materially and adversely affects a certification authority's operations or system, its certification authority certificate, or any other aspect of its ability to operate in a trustworthy manner, the certification authority must act in accordance with procedures governing such an occurrence specified in its certification practice statement, or in the absence of such procedures, must use reasonable efforts to notify any persons that the certification authority knows might foreseeably be damaged as a result of such occurrence.

Section 15-310. Issuance of a certificate

A certification authority may issue a certificate to a prospective subscriber for the purpose of allowing third parties to verify digital signatures created by the subscriber only after:

(1) the certification authority has received a request for issuance from the prospective subscriber, and

(2) the certification authority has:

(A) complied with all of the relevant practices and procedures set forth in its applicable certification practice statement, if any; or

(B) in the absence of a certification practice statement addressing these issues, confirmed in a trustworthy manner that:

(i) the prospective subscriber is the person to be listed in the certificate to be issued;

(ii) the information in the certificate to be issued is accurate; and

(iii) the prospective subscriber rightfully holds a private key capable of creating a digital signature, and the public key to be listed in the certificate can be used to verify a digital signature affixed by such private key.

Section 15-315. Representations upon issuance of certificate

(a) By issuing a certificate with the intention that it will be relied upon by third parties to verify digital signatures created by the subscriber, a certification authority represents to the subscriber, and to any person who reasonably relies on information contained in the certificate, in good faith and during its operational period, that:

(1) the certification authority has processed, approved, and issued, and will manage and revoke if necessary, the certificate in accordance with its applicable certification practice statement stated or incorporated by reference in the certificate or of which such person has notice, or in lieu thereof, in accordance with this Act or the law of the jurisdiction governing issuance of the certificate;

(2) the certification authority has verified the identity of the subscriber to the extent stated in the certificate or its applicable certification practice statement, or in lieu thereof, that the certification authority has verified the identity of the subscriber in a trustworthy manner;

(3) the certification authority has verified that the person requesting the certificate holds the private key corresponding to the public key listed in the certificate; and

(4) except as conspicuously set forth in the certificate or its applicable certification practice statement, to the certification authority's knowledge as of the date the certificate was issued, all other information in the certificate is accurate, and not materially misleading.

(b) If a certification authority issued the certificate subject to the laws of another jurisdiction, the certification authority also makes all warranties and representations, if any, otherwise applicable under the law governing its issuance.

Section 15-320. Revocation of a certificate

(a) During the operational period of a certificate, **t**he certification authority that issued the certificate must revoke the certificate in accordance with the policies and procedures governing revocation specified in its applicable certification practice statement, or in the absence of such policies and procedures, as soon as possible after:

(1) receiving a request for revocation by the subscriber named in the certificate, and confirming that the person requesting revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation;

(2) receiving a certified copy of an individual subscriber's death certificate, or upon confirming by other reliable evidence that the subscriber is dead;

(3) being presented with documents effecting a dissolution of a corporate subscriber, or confirmation by other evidence that the subscriber has been dissolved or has ceased to exist;

(4) being served with an order requiring revocation that was issued by a court of competent jurisdiction; or

(5) confirmation by the certification authority that:

(A) a material fact represented in the certificate is false,

(B) a material prerequisite to issuance of the certificate was not satisfied,

(C) the certification authority's private key or system operations were compromised in a manner materially affecting the certificate's reliability, or

(D) the subscriber's private key was compromised.

(b) Upon effecting such a revocation, the certification authority must notify the subscriber and relying parties in accordance with the policies and procedures governing notice of revocation specified in its applicable certification practice statement, or in the absence of such policies and procedures, promptly notify the subscriber, promptly publish notice of the revocation in all repositories where the certification authority previously caused publication of the certificate, and otherwise disclose the fact of revocation on inquiry by a relying party.

Singapore

Part VIII

Duties of Certification Authorities

Trustworthy system

27. A certification authority must utilise trustworthy systems in performing its services.

Disclosure

28. (1) A certification authority shall disclose —

(a) its certificate that contains the public key corresponding to the private key used by that certification authority to digitally sign another certificate (referred to in this section as a certification authority certificate);

(b) any relevant certification practice statement;

(c) notice of the revocation or suspension of its certification authority certificate; and

(d) any other fact that materially and adversely affects either the reliability of a certificate that the authority has issued or the authority's ability to perform its services.

(2) In the event of an occurrence that materially and adversely affects a certification authority's trustworthy system or its certification authority certificate, the certification authority shall —

(a) use reasonable efforts to notify any person who is known to be or foreseeably will be affected by that occurrence; or

(b) act in accordance with procedures governing such an occurrence specified in its certification practice statement.

Issuing of certificate

29. (1) A certification authority may issue a certificate to a prospective subscriber only after the certification authority —

(a) has received a request for issuance from the prospective subscriber; and

(b) has —

(i) if it has a certification practice statement, complied with all of the practices and procedures set forth in such certification practice statement including procedures regarding identification of the prospective subscriber; or

(ii) in the absence of a certification practice statement, complied with the conditions in subsection (2).

(2) In the absence of a certification practice statement, the certification authority shall confirm by itself or through an authorised agent that -

(a) the prospective subscriber is the person to be listed in the certificate to be issued;

(b) if the prospective subscriber is acting through one or more agents, the subscriber authorised the agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(c) the information in the certificate to be issued is accurate;

(d) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(e) the prospective subscriber holds a private key capable of creating a digital signature; and

(f) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

Representations upon issuance of certificate

30. (1) By issuing a certificate, a certification authority represents to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate that the certification authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.

(2) In the absence of such certification practice statement, the certification authority represents that it has confirmed that —

(a) the certification authority has complied with all applicable requirements of this Act in issuing the certificate, and if the certification authority has published the certificate or otherwise made it available to such relying person, that the subscriber listed in the certificate has accepted it;

(b) the subscriber identified in the certificate holds the private key corresponding to the public key listed in the certificate;

(c) the subscriber's public key and private key constitute a functioning key pair;

(d) all information in the certificate is accurate, unless the certification authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed; and

(e) the certification authority has no knowledge of any material fact which if it had been included in the certificate would adversely affect the reliability of the representations in paragraphs (a) to (d).

(3) Where there is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person has notice, subsection (2) shall apply to the extent that the representations are not inconsistent with the certification practice statement.

Suspension of certificate

31. Unless the certification authority and the subscriber agree otherwise, the certification authority that issued a certificate shall suspend the certificate as soon as possible after receiving a request by a person whom the certification authority reasonably believes to be —

(a) the subscriber listed in the certificate;

(b) a person duly authorised to act for that subscriber; or

(c) a person acting on behalf of that subscriber, who is unavailable.

Revocation of certificate

32. A certification authority shall revoke a certificate that it issued —

(a) after receiving a request for revocation by the subscriber named in the certificate; and confirming that the person requesting the revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation;

(b) after receiving a certified copy of the subscriber's death certificate, or upon confirming by other evidence that the subscriber is dead; or

(c) upon presentation of documents effecting a dissolution of the subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

Revocation without subscriber's consent

33. (1) A certification authority shall revoke a certificate, regardless of whether the subscriber listed in the certificate consents, if the certification authority confirms that —

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

(b) a requirement for issuance of the certificate was not satisfied;

(c) the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability;

(d) an individual subscriber is dead; or

(e) a subscriber has been dissolved, wound-up or otherwise ceased to exist.

(2) Upon effecting such a revocation, other than under subsection (1)(d) or (e), the certification authority shall immediately notify the subscriber listed in the revoked certificate.

Notice of suspension

34. (1) Immediately upon suspension of a certificate by a certification authority, the certification authority shall publish a signed notice of the suspension in the repository specified in the certificate for publication of notice of suspension.

(2) Where one or more repositories are specified, the certification authority shall publish signed notices of the suspension in all such repositories.

Notice of revocation

35. (1) Immediately upon revocation of a certificate by a certification authority, the certification authority shall publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation.

(2) Where one or more repositories are specified, the certification authority shall publish signed notices of the revocation in all such repositories.

Paragraphs (4) and (5) - liability

ABA Guidelines

3.14 Liability of complying certification authority

A certification authority that complies with these Guidelines and any applicable law or contract is not liable for any loss which

(1) is incurred by the subscriber of a certificate issued by that certification authority, or any other person, or

(2) is caused by reliance upon a certificate issued by the certification authority, upon a digital signature verifiable with reference to a public key listed in a certificate, or upon information represented in such a certificate or repository.

EC Directive

Article 6 Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-creation data given or identified in the certificate;

(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service provider generates them both;

unless the certification-service provider proves that he has not acted negligently.

2. As a minimum Member States shall ensure that a certification-service provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service provider shall not be liable for damages arising from use of a qualified certificate which exceeds the limitations placed on it.

4. Member States shall ensure that a certification-service provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties. The certification-service provider shall not be liable for damages arising from this maximum limit being exceeded.

5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

Missouri

Section 17.1

By specifying a recommended reliance limit in a certificate, the issuing certification authority and the accepting subscriber recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.

Section 17.2

Unless a licensed certification authority waives application of this subsection, a licensed certification authority is:

(1) Not liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with all material requirements of sections 1 to 27 of this act;

(2) Not liable in excess of the amount specified in the certificate as its recommended reliance limit for either:

(a) A loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or

(b) Failure to comply with section 10 of this act in issuing the certificate;

(3) Liable only for direct, compensatory damages in any action to recover a loss due to reliance on the certificate, which damages do not include:

(a) Punitive or exemplary damages;

(b) Damages for lost profit, savings or opportunity; or

(c) Damages for pain or suffering.

Singapore

Liability limits for licensed certification authorities

45. Unless a licensed certification authority waives the application of this section, a licensed certification authority -

(a) shall not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the licensed certification authority complied with the requirements of this Act;

(b) shall not be liable in excess of the amount specified in the certificate as its recommended reliance limit for either -

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or

(ii) failure to comply with sections 29 and 30 in issuing the certificate.

Article 11. Reliance on electronic signatures

(1) A person is not entitled to rely on an electronic signature to the extent that it is not reasonable to do so.

(2) [In determining whether reliance is not reasonable,] [In determining whether it was reasonable for a person to have relied on the electronic signature,] regard shall be had, if appropriate, to:

(a) the nature of the underlying transaction that the electronic signature was intended to support;

(b) whether the relying party has taken appropriate steps to determine the reliability of the electronic signature;

(c) whether the relying party took steps to ascertain whether the electronic signature was supported by a certificate;

(d) whether the relying party knew or ought to have known that the electronic signature device had been compromised or revoked;

(e) any agreement or course of dealing which the relying party has with the subscriber, or any trade usage which may be applicable;

(f) any other relevant factor.

Article 12. Reliance on certificates

(1) A person is not entitled to rely on the information in a certificate to the extent that it is not reasonable to do so.

(2) In determining whether reliance is not reasonable,] [In determining whether it was reasonable for a person to have relied on the information in a certificate,] regard shall be had, if appropriate, to:

(a) any restrictions placed upon the certificate;

(b) whether the relying party has taken appropriate steps to determine the reliability of the certificate, including reference to a certificate revocation or suspension list where relevant;

(c) any agreement or course of dealing which the relying party has or had at the relevant time with the supplier of certification services or subscriber or any trade usage which may be applicable;

(d) any other relevant factors.

Variant A

(3) If reliance on the electronic signature is not reasonable in the circumstances having regard to the factors in paragraph (1), a relying party assumes the risk that the signature is not a valid signature.

Variant B

(3) If reliance on the signature is not reasonable in the circumstances having regard to the factors in paragraph (1), a relying party shall have no claim against the signature device holder or the supplier of certification services.

References to UNCITRAL documents

A/CN.9/465, paras. 109-122 (draft articles 10 and 11);
A/CN.9/WG.IV/WP.82, paras 56-58 (draft articles 10 and 11);
A/CN.9/457, paras. 99-107;
A/CN.9/WG.IV/WP.80, paras. 20-21.

Remarks

61. Draft articles 11 and 12, which deal respectively with the reasonableness of reliance on electronic signatures and certificates, have been subject to minor redrafting as a result of the deliberations by the Working Group at its thirty-fifth session. While the prevailing view of the Working Group at its thirty-fourth session was that provisions should be included in the Uniform Rules regarding the obligations of the party who intended to rely on a certificate, doubts were expressed at the thirty-fifth session with respect to the usefulness of the notion of "reliance", which relates both to the message and the signature, and which might raise difficult questions when confronted with the law of obligations and the need to assign risk (see A/CN.9/465, para. 111). The Working Group may wish to decide, as a matter of policy, whether the Uniform Rules should expressly establish obligations binding on the relying parties. If articles 11 and 12 are understood as setting out obligations for the relying parties, the consequences of failure to fulfil those obligations may need to be further examined. If articles 11 and 12 are understood as establishing a mere "code of conduct", without addressing the consequences of failure to follow the conduct indicated (see A/CN.9/465, para. 113), such suggestions for conduct by a relying party might more appropriately be included in explanatory material such as a guide to enactment of the Uniform Rules.

62. Variants A and B, which are both based on the assumption that the Uniform Rules should deal with the legal consequences that might flow from the failure by a relying party to exercise due care in assessing the reliability of an electronic signature (whether such an electronic signature is supported or not by a certificate), are intended to reflect the two proposals made in that respect at the thirty-fifth session of the Working Group (A/CN.9/465, para. 117).

63. The Working Group may wish to further consider the relationship between draft articles 11 and 12, on the one hand, and draft article 6, on the other hand.

References to national legislation and other texts

ABA Guidelines

5.3 Unreliable digital signatures
(1) [...]
(2) Unless otherwise provided by law or contract, a relying party assumes the risk that a digital signature is invalid as a signature or authentication of the signed message, if reliance on the digital signature is not reasonable under the circumstances in accordance with the factors listed in Guideline 5.4 (reasonableness of reliance).

5.4 Reasonableness of reliance
The following factors, among others, are significant in evaluating the reasonableness of a recipient's reliance upon a certificate, and upon digital signatures verifiable with reference to the public key listed in the certificate:
(1) facts which the relying party knows or of which the relying party has notice, including all facts listed in the certificate or incorporated in it by reference,
(2) the value or importance of the digitally signed message, if known,
(3) the course of dealing between the relying person and subscriber and the available indicia of reliability or unreliability apart from the digital signature,
(4) usage of trade, particularly trade conducted by trustworthy systems or other computer-based means.

2.3 Reliance on certificates foreseeable
It is foreseeable that persons relying on a digital signature will also rely on a valid certificate containing the public key by which the digital signature can be verified.

GUIDEC

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

Singapore

Part VI Effect of digital signatures
Unreliable digital signatures
22. Unless otherwise provided by law or contract, a person relying on a digitally signed electronic record assumes the risk that the digital signature is invalid as a signature or authentication of the signed electronic record, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors:

(a) facts which the person relying on the digitally signed electronic record knows or has notice of, including all facts listed in the certificate or incorporated in it by reference;
(b) the value or importance of the digitally signed electronic record, if known;
(c) the course of dealing between the person relying on the digitally signed electronic record and the subscriber and the available indicia of reliability or unreliability apart from the digital signature; and
(d) any usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

Article 13. Recognition of foreign certificates and electronic signatures

[(1) In determining whether, or the extent to which, a certificate [or an electronic signature] is legally effective, no regard shall be had to the place where the certificate [or the electronic signature] was issued, nor to the State in which the issuer had its place of business.]

(2) Certificates issued by a foreign supplier of certification services are recognized as legally equivalent to certificates issued by suppliers of certification services operating under ... *[the law of the enacting State]* if the practices of the foreign suppliers of certification services provide a level of reliability at least equivalent to that required of suppliers of certification services under ... *[the law of the enacting State]*. [Such recognition may be made through a published determination of the State or through bilateral or multilateral agreement between or among the States concerned.]

(3) Signatures complying with the laws of another State relating to electronic signatures are recognized as legally equivalent to signatures under ... *[the law of the enacting State]* if the laws of the other State require a level of reliability at least equivalent to that required for such signatures under ... *[the law of the enacting State]*. [Such recognition may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

(4) In determining equivalence, regard shall be had, if appropriate, [to the factors in paragraph (2) of article 10] [to the following factors:

(a) financial and human resources, including existence of assets within the jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification authority regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and

(h) the degree of discrepancy between the law applicable to the conduct of the certification authority and the law of the enacting State].

(5) Notwithstanding paragraphs (2) and (3), parties to commercial and other transactions may specify that a particular supplier of certification services, class of suppliers of certification services or class of certificates must be used in connection with messages or signatures submitted to them.

(6) Where, notwithstanding paragraphs (2) and (3), parties agree, as between themselves, to the use of certain types of electronic signatures and certificates,[that agreement shall be recognized as sufficient for the purpose of cross-border recognition]. [In determining whether, or the extent to which, an electronic signature or certificate is legally effective, regard shall be had to any agreement between the parties to the transaction in which that signature or certificate is used.]

References to UNCITRAL documents

A/CN.9/465, paras. 21-35;
A/CN.9/WG.IV/WP.82, paras. 69-71;
A/CN.9/454, para. 173;
A/CN.9/446, paras. 196-207 (draft article 19);
A/CN.9/WG.IV/WP.73, para. 75;
A/CN.9/437, paras. 74-89 (draft article I); and
A/CN.9/WG.IV/WP.71, paras. 73-75.

Remarks

64. While there was general support at the thirty-fifth session of the Working Group for the principle of non-discrimination set forth in paragraph (1), doubts were expressed as to whether it was appropriate to refer to the country of origin. The view was expressed that reference to the country of origin resulted in a non-discrimination provision that was too narrow, and left open the possibility that discrimination could occur on a number of other grounds, which would be undesirable. The view was also expressed that, in fact, there might be cases where the country of origin of the signature or certificate was essential to the question of recognition. However, no support was expressed in favour of a proposal to replace the current wording under which "no regard" should be had to the country of origin, by wording to the effect that determination of the legal effect of an electronic signature should not be based "solely" on the country of origin (see A/CN.9/465, paras. 23-24). The Working Group may wish to decide, as a matter of policy, whether a precise statement embodying the principle of non-discrimination should be included in draft article 13 or whether the expression of that principle should be left for a more general reference in a preamble or in a guide to enactment of the Uniform Rules.

65. Paragraphs (2), (3), (4) and (5) were largely agreed upon by the Working Group at its previous session as setting out an appropriate rule on recognition of foreign certificates and signatures (ibid., para. 34). As regards the factors listed in paragraph (4), a cross-reference to draft article 10 might be sufficient if the same factors are used for determining the trustworthiness of systems used by domestic suppliers of certification services. Paragraph (5) reflects a general view in the Working Group that parties to commercial and other transactions should be accorded the right to choose the particular supplier of certification services, class of suppliers of certification services or class of certificates that they wish to use in connection with messages or signatures that they receive. The reference to parties to commercial and other transactions is intended to include government agencies acting in their commercial capacity.

66. Paragraph (6) contains suggestions for expressing the decision made by the Working Group at its thirty-fifth session that draft article 13 should provide for the recognition of agreements between interested parties regarding the use of certain types of electronic signatures or certificates as sufficient grounds for cross-border recognition (as between those parties) of such agreed signatures or certificates (A/CN.9/465, para. 34).

67. The Working Group may wish to decide, as a matter of policy, whether draft article 13 should address both certificates and signatures.

References to national legislation and other texts

EC Directive

Article 7 International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service provider established within the Community if:

(a) the certification-service 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-service provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or

(c) the certificate or the certification-service provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.

Germany

§ 15 Foreign Certificates

(1) Digital signatures which may be checked with a public signature key for which a foreign certificate of another Member State of the European Union or of another contracting State of the Treaty on the European Economic Area exists are equivalent to digital signatures under this law, insofar as they demonstrate an equivalent level of security.

(2) Para. 1 also applies to other States, insofar as supranational or international agreements concerning the recognition of certificates have been concluded.

Illinois

Article 25. State Agency use of electronic signatures and records

Section 25-115. Interoperability

To the extent reasonable under the circumstances, rules adopted by the Department of Central Management Services or a State agency relating to the use of electronic records or electronic signatures shall be drafted in a manner designed to encourage and promote consistency and interoperability with similar requirements adopted by government agencies of other states and the federal government.

Singapore

Part X Regulation of Certification Authorities

Recognition of foreign certification authorities

43. The Minister may by regulations provide that the controller may recognise certification authorities outside Singapore that satisfy the prescribed requirements for any of the following purposes:

(a) the recommended reliance limit, if any, specified in a certificate issued by the certification authority;

(b) the presumption referred to in sections 20(b)(ii) [digital signature to be treated as secure electronic signature in certain circumstances] and 21 [presumption of correctness of certificate if accepted by subscriber].

Annex I. DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

(Consolidated text of draft articles 1 to 13, as considered in part II of this note)

Article 1. Sphere of application

These Rules apply where electronic signatures are used in the context* of commercial** activities and do not override any rule of law intended for the protection of consumers.

* The Commission suggests the following text for States that might wish to extend the applicability of these Rules:

"These Rules apply where electronic signatures are used, except in the following situations: [...]."

** The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2. Definitions

For the purposes of these Rules:

(a) "Electronic signature" means [data in electronic form in, affixed to, or logically associated with, a data message, and] [any method in relation to a data message] that may be used to identify the signature device holder in relation to the data message and indicate the signature device holder's approval of the information contained in the data message;

[(b) "Enhanced electronic signature" means an electronic signature in respect of which it can be shown, through the use of a [security procedure] [method], that the signature:

(i) is unique to the signature device holder [for the purpose for][within the context in] which it is used;

(ii) was created and affixed to the data message by the signature device holder or using a means under the sole control of the signature device holder [and not by any other person];

[(iii) was created and is linked to the data message to which it relates in a manner which provides reliable assurance as to the integrity of the message";]]

(c) "Certificate" means a data message or other record which is issued by an information certifier and which purports to ascertain the identity of a person or entity who holds a particular [key pair] [signature device];

(d) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(e) "Signature holder" [device holder] [key holder] [subscriber] [signature device holder] [signer] [signatory] means a person by whom, or on whose behalf, an enhanced electronic signature can be created and affixed to a data message;

(f) "Information certifier" means a person or entity which, in the course of its business, engages in [providing identification services] [certifying information] which [are][is] used to support the use of [enhanced] electronic signatures.

Article 3. [Technology neutrality] [Equal treatment of signatures]

None of the provisions of these Rules shall be applied so as to exclude, restrict, or deprive of legal effect any method [of electronic signature] [that satisfies the requirements referred to in article 6(1) of these Rules] [which 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] [or otherwise meets the requirements of applicable law].

Article 4. Interpretation

(1) In the interpretation of these Uniform Rules, regard is to be had to their international origin and to the need to promote uniformity in their application and the observance of good faith.

(2) Questions concerning matters governed by these Uniform Rules which are not expressly settled in them are to be settled in conformity with the general principles on which these Uniform Rules are based.

Article 5. [Variation by agreement] [Party autonomy] [Freedom of contract]

These Rules may be derogated from or [their effect may be] varied by agreement, unless otherwise provided in these Rules or in the law of the enacting State.

Article 6. [Compliance with requirements for signature] [Presumption of signing]

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if [a method] [an electronic signature] is used which 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.

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

Variant A

(3) It is presumed that [a method] [an electronic signature] is reliable for the purpose of satisfying the requirement referred to in paragraph (1) if that method ensures that:

(a) the data used for the creation of an electronic signature are unique to the holder of the signature [creation] device within the context in which they are used;

(b) the holder of the signature [creation] device [has] [had at the relevant time] sole control of that device;

(c) the electronic signature is linked to the [information] [the data message or the part of that message] to which it relates [in a manner which guarantees the integrity of that information];

(d) the holder of the signature [creation] device is objectively identified within the context [in which the device is used][of the data message].

Variant B

(3) In the absence of proof to the contrary, the use of an electronic signature is presumed to prove:

(a) that the electronic signature meets the standard of reliability set out in paragraph (1);

(b) the identity of the alleged signer; and

(c) that the alleged signer approved the information to which the electronic signature relates.

(4) The presumption in paragraph (3) applies only if:

(ppp) the person who intends to rely on the electronic signature notifies the alleged signer that the electronic signature is being relied upon [as equivalent to the hand-written signature of the alleged signer][as proof of the elements listed in paragraph (3)]; and

(qqq) the alleged signer fails to notify promptly the person who issues a notification under subparagraph (a) of the reasons for which the electronic signature should not be relied upon [as equivalent to the hand-written signature of the alleged signer][as proof of the elements listed in paragraph (3)].

Variant C

(3) In the absence of proof to the contrary, the use of an electronic signature is presumed to prove:

(a) that the electronic signature meets the standard of reliability set out in paragraph (1);

(b) the identity of the alleged signer; and

(c) that the alleged signer approved the information to which the electronic signature relates.

[(4)][(5)] The provisions of this article do not apply to the following: [...].

[Article 7. Presumption of original

(1) A data message is presumed to be in its original form where, in relation to that data message, [a method] [an electronic signature] [within article 6] is used which:

(a) provides 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

(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;

(2) The provisions of this article do not apply to the following: [...].]

Article 8. Satisfaction of articles 6 and 7

Variant A

(1) *[The organ or authority specified by the enacting State as competent]* may determine which methods satisfy the requirements of articles 6 and 7.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

Variant B

(1) One or more methods of electronic signature may be determined as satisfying the requirements of articles 6 and 7.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

Article 9. Responsibilities of the signature device holder

(1) Each signature device holder shall:

(a) Exercise reasonable care to avoid unauthorized use of its signature device;

(b) Notify appropriate persons without undue delay if:

(i) the signature device holder knows that the signature device has been compromised; or
(ii) the circumstances known to the signature device holder give rise to a substantial risk that the signature device may have been compromised;

(c) [Where a certificate is used to support the signature device,] [Where the signature device involves the use of a certificate,] exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signature device holder which are relevant to [the life-cycle of the] certificate, or which are to be included in the certificate.

(2) A signature device holder shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 10. Responsibilities of a supplier of certification services

(1) A supplier of certification services shall:

(a) act in accordance with the representations it makes with respect to its practices;

(b) exercise due diligence to ensure the accuracy and completeness of all material representations made by the supplier of certification services that are relevant to the life-cycle of the certificate or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain:

(i) the identity of the supplier of certification services;

(ii) that the person who is identified in the certificate holds, at the relevant time, the signature device referred to in the certificate;

(iii) the method used to identify the signature device holder;

(iv) any limitations on the purposes or value for which the signature device may be used; and

(v) whether the signature device is valid and has not been compromised;

(d) Provide a means for signature device holders to give notice that a signature device has been compromised and ensure the operation of a timely revocation service;

(e) Utilize trustworthy systems, procedures and human resources in performing its services.

(2) In determining whether and the extent to which any systems, procedures and human resources are trustworthy for the purposes of subparagraph (e) of paragraph (1), regard shall be had to the following factors:

(a) financial and human resources, including existence of assets within the jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(c) the existence of a declaration by the State, an accreditation body or the supplier of certification services regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and

(h) the degree of discrepancy between the law applicable to the conduct of the supplier of certification services and the law of the enacting State.

(3) A certificate shall state:

(a) the identity of the supplier of certification services;

(b) that the person who is identified in the certificate holds, at the relevant time, the signature device referred to in the certificate;

(c) that the signature device was effective at or before the date when the certificate was issued;

(d) any limitations on the purposes or value for which the certificate may be used; and

(e) any limitation on the scope or extent of liability which the supplier of certification services accepts to any person.

Variant X

(4) A supplier of certification services shall be liable for its failure to satisfy the requirements of paragraph (1).

(5) Liability of the supplier of certification services may not exceed the loss which the supplier of certification services foresaw or ought to have foreseen at the time of its failure in the light of facts or matters which the supplier of certification services knew or ought to have known to be possible consequences of the supplier of certification services' failure to [fulfil the obligations [duties] in][satisfy the requirements of] paragraph (1).

Variant Y

(4) A supplier of certification services shall be liable for its failure to satisfy the requirements of paragraph (1).

(5) In assessing the loss, regard shall be had to the following factors:

(a) the cost of obtaining the certificate;

(b) the nature of the information being certified;

(c) the existence and extent of any limitation on the purpose for which the certificate may be used;

(d) the existence of any statement limiting the scope or extent of the liability of the supplier of certification services; and

(e) any contributory conduct by the relying party.

Variant Z

(4) If damage has been caused as a result of the certificate being incorrect or defective, a supplier of certification services shall be liable for damage suffered by either:

(a) a party who has contracted with the supplier of certification services for the provision of a certificate; or

(b) any person who reasonably relies on a certificate issued by the supplier of certification services.

(5) A supplier of certification services shall not be liable under paragraph (2):

(a) if, and to the extent, it included in the certificate a statement limiting the scope or extent of its liability to any relevant person; or

(b) if it proves that it [was not negligent][took all reasonable measures to prevent the damage].

Article 11. Reliance on electronic signatures

(1) A person is not entitled to rely on an electronic signature to the extent that it is not reasonable to do so.

(3) [In determining whether reliance is not reasonable,] [In determining whether it was reasonable for a person to have relied on the electronic signature,] regard shall be had, if appropriate, to:

(a) the nature of the underlying transaction that the electronic signature was intended to support;

(b) whether the relying party has taken appropriate steps to determine the reliability of the electronic signature;

(c) whether the relying party took steps to ascertain whether the electronic signature was supported by a certificate;

(d) whether the relying party knew or ought to have known that the electronic signature device had been compromised or revoked;

(e) any agreement or course of dealing which the relying party has with the subscriber, or any trade usage which may be applicable;

(f) any other relevant factor.

Article 12. Reliance on certificates

(1) A person is not entitled to rely on the information in a certificate to the extent that it is not reasonable to do so.

(2) In determining whether reliance is not reasonable,] [In determining whether it was reasonable for a person to have relied on the information in a certificate,] regard shall be had, if appropriate, to:

(a) any restrictions placed upon the certificate;

(b) whether the relying party has taken appropriate steps to determine the reliability of the certificate, including reference to a certificate revocation or suspension list where relevant;

(c) any agreement or course of dealing which the relying party has or had at the relevant time with the supplier of certification services or subscriber or any trade usage which may be applicable;

(d) any other relevant factors.

Variant A

(3) If reliance on the electronic signature is not reasonable in the circumstances having regard to the factors in paragraph (1), a relying party assumes the risk that the signature is not a valid signature.

Variant B

(3) If reliance on the signature is not reasonable in the circumstances having regard to the factors in paragraph (1), a relying party shall have no claim against the signature device holder or the supplier of certification services.

Article 13. Recognition of foreign certificates and electronic signatures

[(1) In determining whether, or the extent to which, a certificate [or an electronic signature] is legally effective, no regard shall be had to the place where the certificate [or the electronic signature] was issued, nor to the State in which the issuer had its place of business.]

(2) Certificates issued by a foreign supplier of certification services are recognized as legally equivalent to certificates issued by suppliers of certification services operating under ... *[the law of the enacting State]* if the practices of the foreign suppliers of certification services provide a level of reliability at least equivalent to that required of suppliers of certification services under ... *[the law of the enacting State]*. [Such recognition may be made through a published determination of the State or through bilateral or multilateral agreement between or among the States concerned.]

(3) Signatures complying with the laws of another State relating to electronic signatures are recognized as legally equivalent to signatures under ... *[the law of the enacting State]* if the laws of the other State require a level of reliability at least equivalent to that required for such signatures under ... *[the law of the enacting State]*. [Such recognition may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

(4) In determining equivalence, regard shall be had, if appropriate, [to the factors in paragraph (2) of article 10] [to the following factors:

(a) financial and human resources, including existence of assets within the jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification authority regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and

(h) the degree of discrepancy between the law applicable to the conduct of the certification authority and the law of the enacting State].

(5) Notwithstanding paragraphs (2) and (3), parties to commercial and other transactions may specify that a particular supplier of certification services, class of suppliers of certification services or class of certificates must be used in connection with messages or signatures submitted to them.

(6) Where, notwithstanding paragraphs (2) and (3), parties agree, as between themselves, to the use of certain types of electronic signatures and certificates,[that agreement shall be recognized as sufficient for the purpose of cross-border recognition]. [In determining whether, or the extent to which, an electronic signature or certificate is legally effective, regard shall be had to any agreement between the parties to the transaction in which that signature or certificate is used.]

Notes

1/ Official Records of the General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), paras. 223-224.

2/ Ibid., Fifty-second Session, Supplement No. 17 (A/52/17), paras. 249-251.

3/ Ibid., Fifty-third Session, Supplement No. 17 (A/53/17), para. 208.

4/ Ibid., Fifty-fourth Session, Supplement No. 17 (A/54/17), paras. 308-314.