UNITED
NATIONS

A

General Assembly

Distr.
LIMITED

A/CN.9/WG.IV/WP.82
29 June 1999

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Working Group on Electronic Commerce
Thirty-fifth session
Vienna, 6-17 September 1999

DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

Note by the Secretariat

CONTENTS

V.99-85656

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 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 (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 UNCITRAL Model Law on Electronic Commerce. 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, para. 3 and 5) and expressed its confidence that more progress could be accomplished by the Working Group at its forthcoming sessions.

10. 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. They are intended to reflect the decisions made by the Working Group at its thirty-fourth session. Newly revised provisions are indicated by underlining.

11. 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

12. 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 Draft Directive — Draft Directive of the European Parliament and of the Council on a common framework for electronic signatures, 1999 (7015/99);

- GUIDEC International Chamber of Commerce, "General Usage for International Digitally Ensured Commerce", 1997.

I. GENERAL REMARKS

13. 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.

14. 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.

15. 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).

16. 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. Two newly added articles reflecting provisions contained in the Model Law have been included - articles 1 (Sphere of application) and 4 (Interpretation). Transactions involving consumers have not been specifically excluded from the sphere of application of the Uniform Rules, but the footnote from the Model Law has been included in the text of draft article 1 to clarify that the Uniform Rules are not intended to override any provision of national law dealing with consumer protection issues.

17. 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.

18. 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, paras. 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.

19. In view of this 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 placed in square brackets. Remarks addressing possible amendment of the definition are included under article 2. Draft articles 6, 7 and 8 include the relevant parts of that definition as alternative substantive provisions. The purpose of this alternative 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 specific proposals are dealt with under respective articles.

20. This revised draft of the Uniform Rules extends their application beyond the situation where there are legal form requirements or where the law provides for consequences in the absence of certain conditions, such as signature or original. As such, the scope of the Uniform Rules is potentially wider than that of the Model Law, although draft article 6 does include the form requirement of article 7 of the Model Law. The Working Group may wish to consider this broader application for the Uniform Rules.

II. DRAFT ARTICLES ON ELECTRONIC SIGNATURES

Article 1. Sphere of application

These Rules apply to electronic signatures used in the context of commercial* relationships and do not override any law intended for the protection of consumers.

* 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.9/457, paras. 53-64

Remarks

21. Draft article 1 was originally proposed at the thirty-fourth session of the Working Group as paragraph (1) to an article dealing with party autonomy (draft article E, A/CN.9/457, paras. 55, 60). As this provision more properly deals with issues of scope of the Uniform Rules it has been included in this draft as a separate article under the heading "Sphere of application". As agreed by the Working Group (A/CN.9/457, para 64), draft article 1 includes a footnote which repeats the definition of "commercial" in article 1 of the Model Law on Electronic Commerce and adopts the wording of footnote** to the Model Law on the question of consumers. The words "electronic signatures used in the context of" have been added to the article to define more precisely the subject matter of the Uniform Rules.

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.9/457, 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

Definition of "electronic signature"

22. The definition of electronic signature has been revised 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"

23. 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" has been revised to include 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 this revision on the basis that it is part of the definition of an "electronic signature" in subparagraph (a).

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

25. 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 holder (and therefore potentially unauthorised) 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 10. In particular, the application of those parts of draft article 9 which deal with responsibility for compromise of signature devices could be uncertain.

26. 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 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.

27. 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 paragraph (2) of draft article 9 which provides for joint control. This issue also arises in relation to the definition of "signature holder" below.

28. In subparagraph (b)(iii) the phrase "reasonable assurance" has been changed to "reliable assurance" to maintain consistency with the terminology of article 8 of the Model Law.

Definition of "certificate"

29. A definition of "certificate" has been included 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 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 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, pp6-9.

30. 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 holder, but rather identify the signature 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" 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"

31. A definition of "data message" has been included 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"

32. 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(2), as noted at para. 27.

Definition of "information certifier"

33. 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 issue of certificates as an incidental part of the business of an entity should also be covered.

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 Draft 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.
1a. "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.
2. "signatory" means a person who holds a signature creation device and acts either on their own behalf or on the behalf of the person or the entity they represent.
3. "signature creation data" means unique data such as codes or private cryptographic keys, which is used by the signatory in creating an electronic signature.
3a. "signature creation device" means a configured software or hardware device to implement the signature creation data.
3b. "secure signature creation device" is a signature creation device that meets the requirements of Annex III.
4. "signature verification data" means data, such as codes or public cryptographic keys, which is used in verifying the electronic signature.
4a. "signature verification device" means a configured software or hardware device to implement the signature verification data.
4b. "certificate" means an electronic attestation which links a signature verification data to a person, and confirms the identity of that person.
5. [...]
6. "certification service provider" means a person who or entity which issues certificates or provides other services related to electronic signatures.

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).

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.

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. [Non-discrimination] [Technology neutrality]

[None of the provisions of these Rules shall be applied] [The provisions of these Rules shall not be applied] so as to exclude, restrict, or deprive of legal effect any method [of signature] that satisfies the requirements of *[article 7 of the UNCITRAL Model Law on Electronic Commerce]*.

References to UNCITRAL documents

A/CN.9/457, paras. 53-64

Remarks

34. Draft article 2 was originally proposed at the thirty-fourth session of the Working Group as paragraph (3) to an article dealing with party autonomy (draft article E, A/CN.9/457, paras. 55, 60). As paragraph (3) dealt with the issues of non-discrimination and technology neutrality, rather than party autonomy, it has been included in this draft as a separate article under the alternative headings of "Non-discrimination" and "Technology neutrality". The words "exclude, restrict or deprive of legal effect" have replaced the original words "exclude, restrict or discriminate against" to more precisely describe the purpose and object of this provision. The reference to article 7 of the Model Law on Electronic Commerce would be a reference to that Model Law as enacted in national 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 in electronic commerce.

(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.

Remarks

35. Draft article 3 repeats article 3 of the Model Law on Electronic Commerce, with addition of the words "in electronic commerce", and is included here for reasons of completeness. The Working Group may wish to consider the question of whether the Uniform Rules should now be completed as a text which does not form part of the Model Law, although retaining a clear link to the Model Law. Should the Working Group so decide, article 3 may provide guidance to interpretation of the Uniform Rules by courts and other national or local authorities. The expected effect of article 3 would be to promote interpretation of the uniform text, once incorporated in local legislation, by reference to its international character and origins, rather than by reference only to the concepts of local law.

Article 5. Variation by agreement

Variant A

> [By agreement, whether express or implied, parties are free to derogate from or vary any aspect of these Rules.] [Any aspect of these Rules may be derogated from or varied by agreement, whether express or implied,] except to the extent such derogation or variation would adversely affect rights of third parties.

Variant B

(1) These Rules do not affect any right that may exist to modify by agreement any rule of law referred to in articles 6 and 7.

(2) Any aspect of articles 9 to 12 of these Rules may be derogated from or varied by agreement, whether express or implied, except to the extent that such derogation or variation would adversely affect rights of third parties.

References to UNCITRAL documents

A/CN.9/457, paras. 53-64

Remarks

36. Variant A of draft article 5 reflects the decision of the Working Group at its thirty-fourth session to include, for future discussion, a provision ensuring the freedom of the parties to agree among themselves that they could derogate from or vary the provisions of these Rules, for the purposes only of transactions between the agreeing parties. Such agreement, however, cannot affect the rights of parties not party to that agreement, that is, third parties. 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.

37. Variant B recognizes that the provisions of draft articles 6 and 7 of the Uniform Rules, which are based on articles 7 and 8 of the Model Law, include references to requirements of law which may be mandatory requirements of national law and not subject to modification by agreement. Paragraph (1) allows for variation by agreement where such mandatory requirements of national law may be so modified. As such, it repeats the wording of article 4(2) of the Model Law, which deals with the same question.

38. Paragraph (2) of Variant B preserves complete party autonomy with respect to draft articles 9 to 12. This provision is drafted on the basis that draft articles 9 to 12 would be rules of substantive law that would apply in the absence of agreement to derogate from or vary the application of these provisions as between contracting parties. Parties would be free to modify or opt out of these provisions. Paragraph (2) is intended to ensure that any such agreement should not operate to the detriment of third parties, but is not intended to have the effect of invalidating any part of the agreement between the parties.

39. Provisions dealing with cross-border recognition would not be subject to variation by agreement, except as specifically provided in those provisions.

40. The Working Group may wish to consider the formulation of draft article 5 and the issues it raises in respect of the satisfaction of what may be mandatory requirements of law in draft articles 6 and 7. The Working Group may also wish to consider how the principle of party autonomy should apply to draft articles 9 to 12. The provision could establish, for example, default rules which apply in the absence of contrary agreement between contracting parties ("opt out") or could establish rules which parties can agree to apply ("opt in").

General remarks regarding draft articles 6-8

41. In the context of a discussion at its thirty-fourth session of the scope of the Uniform Rules (A/CN.9/457, paras. 48-52), the Working Group decided to focus upon rules for technologies which were currently being used in commercial transactions, such as digital techniques within a public key infrastructure (PKI). Accordingly, it was agreed that the Working Group should focus its discussion on draft articles F to H (in this draft, articles 9 to 12) in the context of PKI. Discussion on draft articles A to D (in this draft, articles 2, 6, 7 and 8) was deferred until a later time when articles F to H had been reviewed. It was pointed out that draft article B (in this revision, article 6 - Compliance with requirements for signature), in particular, might serve an important function in defining the scope of application of articles F to H. In addition, it was suggested that article E (in this draft, article 5 - Variation by agreement), which dealt with the principle of party autonomy, would be important to any consideration of the obligations of the parties in articles F to H.

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

Variant A

(1) Where, in relation to a data message, an enhanced electronic signature is used, it is presumed that the data message is signed.

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

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

(4) Paragraphs (2) and (3) apply 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.

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

Variant B

(1) Where, in relation to a data message, [a method] [an electronic signature] is used which:

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

[(b) can be used to objectively identify the signature holder in relation to the data message; and]

(c) 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];

it is presumed that the data message is signed.

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

(3) Paragraph (2) 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.

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

References to UNCITRAL documents

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

Remarks

Variant A

42. Variant A establishes that where an enhanced electronic signature is used in relation to a data message, the data message can be presumed to be signed. Paragraph (2) restates the principle of article 7 of the Model Law that an electronic signature can satisfy a requirement of law for a signature, provided that it meets certain conditions of reliability. The Working Group will recall that paragraph 58 of the Guide to Enactment of the Model Law sets out factors that may be taken into account in determining the appropriate level of reliability. Paragraph (3), which provides that an enhanced electronic signature meets those conditions and establishes a shortcut to satisfaction of the requirements of article 7 of the Model Law, has been included in this draft in square brackets. The Working Group may wish to consider whether this provision is still necessary in view of paragraph (1).

Variant B

43. The purpose of Variant B is to establish a presumption of signing and satisfaction of a requirement of law for a signature in the context of a single category of electronic signature. Accordingly, it makes no reference to "enhanced electronic signature". Paragraph (1) of Variant B establishes that where a method is used in relation to a data message and that method satisfies certain requirements, the data message can be presumed to be signed. That method is required to satisfy the conditions set forth in the definition of "enhanced electronic signature" in draft article 2(b), with the exception of the reference to integrity in subparagraph (b)(iii). Paragraph (1)(b) appears in square brackets, as it would be required only if the opening words of paragraph (1) refer to "a method" rather than to "an electronic signature".

44. The Working Group may wish to consider whether these Rules should be limited in their application to situations where there are legal form requirements or where the law provides for consequences in the absence of certain conditions, such as writing or a signature. It should be recalled that what is meant by form requirements was discussed in the preparation of the Model Law. Paragraph 68 of the Guide to Enactment of the Model Law notes that the use of the phrase "the law" in the Model Law is to be understood as encompassing not only statutory or regulatory law, but also judicially-created law and other procedural law. Thus the phrase "the law" also covers rules of evidence. Where the law does not stipulate a requirement for a particular condition, but provides for consequences in the absence of the condition, for example writing or signature, this is also to be included within the concept of "the law" as used in the Model Law.

References to national legislation and other texts

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) Where, in relation to a data message, [an enhanced electronic signature is used] [an electronic signature [a method] is used which 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], it is presumed that the data message is an original.

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

References to UNCITRAL documents

A/CN.9/457, paras. 48-52
A/CN.9/WG.IV/WP.80, paras. 13-14

Remarks

45. The purpose of draft article 7 is to confirm the connection with article 8 of the Model Law and the requirement of integrity. Paragraph (1) sets out two alternatives. The first provides that the use of an enhanced electronic signature, as defined in draft article 2(b), will establish a presumption that the data message is an original. The second alternative is that where an electronic signature or a method is used which provides a reliable assurance of integrity, the data message can be presumed to be an original. Although an original form does not always require a signature, the use of a form of electronic signature, whether enhanced or not, may be used to verify the integrity of the data message or record.

Article 8. Determination of [enhanced] electronic signature

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

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

References to UNCITRAL documents

A/CN.9/457, paras. 48-52
A/CN.9/WG.IV/WP.80, para. 15

Remarks

46. 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 qualify as an enhanced electronic signature. The alternative wording in paragraph (1) is to align draft article 8 with the alternatives provided in revised articles 6 and 7. The purpose of paragraph (2) 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.

Article 9. [Responsibilities] [duties] of the signature holder

(1) A signature holder [has a duty to] [shall]:

(a) Exercise due diligence to ensure the accuracy and completeness of all material representations made by the signature holder which are relevant to issuing, suspending or revoking a certificate, or which are included in the certificate.

(b) Notify appropriate persons without undue delay in the event that [it knew its signature had been compromised] [its signature had or might have been compromised];

(c) Exercise due care to retain control and avoid unauthorized use of its signature, as of the time when the signature holder has sole control of the signature device.

(2) If [there are joint holders][more than one person has control] of the [key][signature device], the [obligations] [duties] under paragraph (1) are joint and several.

(3) A signature holder shall be [responsible][liable] for its failure to [fulfil the obligations [duties] in][satisfy the requirements of] paragraph (1).

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

References to UNCITRAL documents

A/CN.9/457, paras. 65-98;
A/CN.9/WG.IV/WP.80, paras. 18-19.

General remarks regarding draft articles 9 and 10

47. The Working Group may wish to consider the relationship between draft articles 9 and 10 in practice. There are a number of possible combinations of the duties in draft article 9 and the consequences of failure to observe those duties in terms of draft article 10. Two of such combinations will serve to illustrate some of the issues to be considered.

48. First, the situation where the signature holder does not breach the duty of exercising reasonable care in draft article 9(1)(c), but nevertheless the signature somehow is compromised. The signature holder does not know of the compromise and so does not notify the information certifier, but is unlikely to be in breach of the duty in draft article 9(1)(b). Under draft article 10, the relying party could not learn of the compromise of the signature by checking information provided by the information certifier, and could rely on the signature. This situation raises a number of questions: Is it reasonable for the relying party to rely in such a situation? Does the relying party bear the risk of reliance? What is the consequence of that reliance for the signature holder? Is the signature holder bound by whatever was signed using the compromised signature?

49. Secondly, the situation where the signature holder does breach the duty of exercising reasonable care in draft article 9(1)(c), and the signature is compromised. The signature holder knows of the compromise and notifies the information certifier. Under draft article 10, the relying party could learn of the compromise of the signature by checking information provided by the information certifier, and then could rely on the signature. The signature holder is thus responsible under draft article 9(3) for failure to observe the duties in paragraph (2) and liable for loss under paragraph (4). In this situation the result is much clearer than in the situation set forth in para. 48.

Remarks

Article 9, paragraph (1)

50. Paragraph (1) of draft article 9 has been revised in accordance with the decisions of the Working Group at its thirty-fourth session (A/CN.9/457, paras. 73-92). The Working Group expressed concern that the duty in subparagraph (a) should be limited to the context of the certification process (A/CN.9/457, para. 92), since otherwise the duty might be widely interpreted to include representations and statements made by the signature holder to a relying party. Since representations or statements made in the context of this relationship should be subject to the law of the underlying contract, subparagraph (a) has been more narrowly drawn to limit the duty to the context of the process of issuing, suspending or revoking a certificate.

51. Subparagraph (b) has been revised to include the two alternative texts agreed by the Working Group (A/CN.9/457, para. 83). The words "or ought to have known" have not been included in this revision on the basis that it would be difficult for the signature holder to satisfy a duty of notification that is based on something it ought to have known, but did not in fact know.

52. Subparagraph (c) refers not only to the obligation to avoid unauthorised use of the signature, but also to the obligation to retain control of the key. The revised provision also refers to the time at which the duty to exercise reasonable care arises. This reflects the prevailing view in the Working Group that, while the duty of the key holder to protect the key should only arise with respect to those key pairs that were effectively protected by a certificate, the duty of the key holder to protect certified keys against misuse should apply retroactively to the time at which the signature holder obtained sole control of the key pair (A/CN.9/457, para. 67).

Paragraph (2)

53. Paragraph (2) has been added to draft article 9 in order to clarify the obligation of due care in the situation where there may be more than one holder of the same key. The Working Group may wish to consider this provision and its relationship with requirements for sole control in article 2.

Paragraph (3)

54. This paragraph has been revised in accordance with decisions of the Working Group at its thirty-fourth session (A/CN.9/457, paras. 93-98). Reference to the "consequences of the [signature holder] failing to fulfil the obligations in paragraph (1)" has been deleted (i) to avoid considerations of whether or not the obligation breached was contractual, and (ii) to avoid any uncertainty that might arise from the use of the phrase "the consequences" which might suggest that all possible consequences were under consideration, without conveying any idea as to the remoteness of those possible consequences from the failure to fulfil the obligation.

Paragraph (4)

55. This paragraph is based upon article 74 of the United Nations Convention on Contracts for the International Sale of Goods and has been included for further consideration by the Working Group. It establishes a rule based upon a test of foreseeability of damage, but is limited to breach of the obligations of the signature holder in paragraph (1). Some concerns were expressed by the Working Group at its thirty-fourth session (A/CN.9/457, paras. 93-98) that the liability which might arise in the context of a contract for the sale of goods was not the same as the liability that might arise from the use of a signature and could not be quantified in the same way. It was also pointed out that a test of foreseeability might not be appropriate in the context of the contractual relationship between the signature holder and the information certifier, although such a test might be appropriate in the context of the relationship between the signature holder and a relying party. The Working Group may wish to consider these issues in its further deliberations on this draft article and, in addition, the relationship of draft article 9 to draft article 10.

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.

Paragraphs (3) and (4) - 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. Reliance on an enhanced electronic signatures

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

(2) In determining whether reliance [is][is not] reasonable, regard shall be had, if appropriate, to:

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

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

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

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

(e) any other relevant factor.

Article 11. Reliance on certificates

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

(2) In determining whether reliance [is][is not] reasonable, 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 list where relevant;

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

(d) [any] [all] other relevant factor[s].

References to UNCITRAL documents

A/CN.9/457, paras. 99-107;
A/CN.9/WG.IV/WP.80, paras. 20-21.

Remarks

56. Draft articles 10 and 11, which deal respectively with the reasonableness of reliance on enhanced electronic signatures and certificates, have been redrafted in accordance with the prevailing view of the Working Group at its thirty-fourth session (A/CN.9/457, para. 107) as to content. Although originally proposed as a single article dealing with both reliance on signatures and reliance on signatures supported by a certificate, the current draft separates these two concepts on the basis that different considerations apply to each situation. The Working Group may wish to consider whether there is a need to include a rule on reliance on certificates in addition to a rule on reliance on signatures and what the considerations that would establish reasonable reliance in each case should be.

57. Some concern was expressed by the Working Group that formulating draft articles 10 and 11 as entitlements to rely might presume certain legal effects, while establishing the factors to be considered in deciding whether reliance could be regarded as reasonable might avoid addressing the issue of what legal effect the signature or certificate might have. An opposing view was that formulating the draft articles as an entitlement to rely added a benefit that was not available under the Model Law, and did not establish legal effect in terms of the validity of the signature. As agreed by the Working Group, the revised draft articles include both a positive and negative form and set out the factors to be taken into consideration in the case of signatures and in the case of certificates.

58. Some concern was also expressed as to the relationship between draft articles 10 and 11 and article 13 of the Model Law and whether draft articles 9, 10 and 11, when read together, would establish a rule on attribution. The Working Group may wish to consider the relationship of draft articles 10 and 11 to draft article 9 and to article 13 of the Model Law.

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 12. [Responsibilities][duties] of an information certifier

(1) [An information certifier is [obliged to[shall]] [*inter alia*]:

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

(b) take reasonable steps to ascertain the accuracy of any facts or information that the information certifier certifies in the certificate, [including the identity of the signature holder];

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

(i) the identity of the information certifier;

(ii) that the person who is [named][identified] in the certificate holds [at the relevant time] the [private key corresponding to the public key][signature device] referred to in the certificate;

[(iii) that the keys are a functioning key pair];

(iv) the method used to identify the signature holder;

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

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

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

(e) exercise due diligence to ensure the accuracy and completeness of all material representations made by the information certifier that are relevant to issuing, suspending or revoking a certificate or which are included in the certificate;

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

Variant X

(2) An information certifier shall be [responsible][liable] for its failure to [fulfil the obligations [duties] in][satisfy the requirements of] paragraph (1).

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

Variant Y

(2) Subject to paragraph (3), if the damage has been caused as a result of the certificate being incorrect or defective, an information certifier shall be liable for damage suffered by either:

(a) a party who has contracted with the information certifier for the provision of a certificate; or

(b) any person who reasonably relies on a certificate issued by the information certifier.

(3) An information certifier 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 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.9/457, paras. 108-119;
A/CN.9/WG.IV/WP.80, paras. 22-24

Remarks

59. Draft article 12 has been revised in accordance with decisions of the Working Group at its thirty-fourth session (A/CN.9/457, paras. 108-119).

Paragraph (1)

60. The opening words of paragraph (1) include several alternatives. The first relates to whether the provision should be drafted using the form "is obliged to" or "shall". The second relates to the use of the words "*inter alia*". If that is used, draft article 12 would set forth an open-ended, illustrative list of duties. While such a formulation might appear burdensome to information certifiers, the Working Group was of the view that it would not be inconsistent with the general rule currently applying to information certifiers in many legal systems. If the words "*inter alia*" are omitted, draft article 12 would set forth an exhaustive list of duties of an information certifier, allowing the exact scope of the liability of the information certifier to be determined and avoiding difficulties which might arise with a different formulation in countries in which an information certifier might not be under a general duty of due diligence.

61. As to the specific duties included in paragraph (1), these have been extended to reflect the views of the Working Group (A/CN.9/457, paras. 112-114). With regard to subparagraph (c), the information to be provided through "reasonably accessible means" includes some information which a relying party might reasonably expect to be included on a certificate and other information which could only be obtained by reference to some other source, such as a certificate revocation list. The Working Group might wish to consider whether some of this information should be specified for inclusion in a certificate and whether an additional rule setting out the minimum contents of a certificate should be included in the Uniform Rules.

62. Paragraph (1)(c)(ii) refers both to a "key pair" and to a "signature device". To ensure that the Uniform Rules are technology neutral, the Working Group may wish to consider the use of

a technology neutral formulation such as "signature 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.

63. Paragraph (1)(c)(iii) has been included as proposed at the previous session, but the Working Group may wish to consider whether this is an appropriate requirement. If the public key referred to in the certificate corresponds to the private key held by the signature holder and there is, therefore, a mathematical correspondence between the two keys, it is not clear what additional functionality would be achieved by a requirement that the key pair be "a functioning key pair". It is also uncertain whether the information certifier could provide information, in addition to what is required by paragraph (1)(c)(ii), that would indicate that additional functionality.

Paragraphs (2) and (3)

64. Variant X establishes a rule that the information certifier 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. The words "the consequences of" have been deleted in this revised draft article 12 for the same reasons that were given for their deletion in paragraph (3) of draft article 9. These were (i) to avoid considerations of whether or not the obligation breached was contractual and (ii) to avoid any uncertainty that might arise from the use of "the consequences" which might suggest that all possible consequences were under consideration, without conveying any idea as to the remoteness of those possible consequences from the failure to fulfil the obligation.

65. Following the revision of paragraph (1) to include two variations - an exhaustive list of obligations and an open-ended, illustrative list of obligations - the Working Group may wish to consider whether Variant X would be more appropriate in the case where paragraph (1) was phrased as an exhaustive list, rather than the open-ended alternative.

66. Paragraph (3) of Variant X establishes a rule of foreseeability of damage based upon article 74 of the United Nations Convention on Contracts for the International Sale of Goods, This paragraph operates to limit the quantum of any liability of the information certifier which might arise from paragraphs (1) and (2).

Variant Y

67. It was widely felt in 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 information certifier exonerating itself by demonstrating that it had fulfilled the obligations under paragraph (1). Paragraph (2) of Variant Y deals with the question of to whom the information certifier may be liable. Paragraph (3) provides a rule permitting the information certifier 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.

68. As in the case of Variant X, the Working Group may wish to consider whether a provision such as proposed in Variant Y would be appropriate in the context of an exhaustive list of duties under paragraph (1), but not where the obligations were open-ended. It may also wish to consider whether it needs to be made clear in draft paragraph (2) of Variant Y that the liability of the information certifier is limited to its failure to perform the obligations in paragraph (1).

References to national legislation and other texts

Article 12 paragraph (1) - 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 Draft 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 secure and immediate revocation service;

(ba) ensure that the date and time, when a certificate is issued or revocated, can be determined;

(c) 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;

(d) employ personnel which possesses the expert knowledge, experience, and qualifications necessary for the offered services, in particular competence at the managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also exercise administrative and management procedures and processes that are adequate and which correspond to recognised standards;

(e) use trustworthy systems and products which are protected against modification and which must ensure the technical and cryptographic security of the processes supported by them;

(f) take measures against forgery of certificates, and, in cases where the certification service provider generates signature creation data, guarantee the confidentiality during the process of generating that data;

(g) maintain sufficient financial resources to operate in conformity with the requirements laid down in this Directive, in particular to bear the risk of liability for damages, for example, by obtaining an appropriate insurance;

(h) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular to provide evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(i) not store or copy signature creation data of the person to whom the certification service provider offered key management services;

(j) before entering into a contractual relationship with a person seeking a certificate from it to support his electronic signature, inform that person by a durable means of communication of the precise terms and conditions for the use of the certificate, including any limitations on the use of the certificate, the existence of a voluntary accreditation and the procedures for complaints and dispute settlement. Such information must be in writing which may be transmitted electronically and in readily understandable language. Relevant parts of this information must also be made available on request to third parties relying on the certificate;

(k) 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 will be apparent to the operator.

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.

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.

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, the 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.

Article 12 paragraphs (2) and (3) - 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 Draft 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 a certificate to the public a certification service provider is liable for damage caused to any person who reasonably relies on the certificate for:

(a) accuracy of all information in the qualified certificate as of the time of issuance,

(b) [...]

(c) assurance that at the time of the issuance of the certificate, the person identified in the qualified certificate held the signature creation data corresponding to the signature verification data given or identified in the certificate;

(d) 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.

1a. 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 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 the qualified certificate limits on the uses of a certain certificate the limit must be recognizable to third parties. The certification service provider shall not be liable for damages arising from a contrary use of a qualified certificate which includes limits on its uses.

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.

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 13. Recognition of foreign certificates and signatures

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

Variant A

(2) Certificates issued by a foreign information certifier are recognized as legally equivalent to certificates issued by information certifiers operating under ... *[the law of the enacting State]* if the practices of the foreign information certifiers provide a level of reliability at least equivalent to that required of information certifiers 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 digital or other 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) Notwithstanding the preceding paragraph, parties to commercial and other transactions may specify that a particular information certifier, class of information certifier or class of certificates must be used in connection with messages or signatures submitted to them.

Variant B

(2) Certificates issued by a foreign information certifier are recognized as legally equivalent to certificates issued by information certifiers operating under [*the law of the enacting State*] if the practices of the foreign information certifier provide a level of reliability at least equivalent to that required of information certifiers under ... *[the law of the enacting State]*.

[(3) The determination of equivalence described in paragraph (2) may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

(4) In the determination of equivalence, regard shall be had to the following factors :

(a) financial and human resources, including existence of assets within 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 enacting State.

References to UNCITRAL documents

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

69. Draft article 13 addresses the matters referred to as "cross-border recognition" at the thirty-first session of the Working Group (see A/CN.9/437, paras. 77-78). Paragraph (1) is based on a proposal made at the thirty-fourth session of the Working Group (A/CN.9/457, para. 120) that the Working Group might like to consider introducing an article to establish that certificates should not be discriminated against on the basis of the place at which they were issued.

70. Variant A is based on a suggestion for a combination of several paragraphs made at the thirty-second session of the Working Group (see A/CN.9/446, paras. 197-204). As such it sets forth the tests that might be applied in the enacting State in order to recognize the certificates issued by foreign information certifiers, as well as the signatures complying with the laws of another State. Paragraph (4) reflects a general view in the Working Group that parties to commercial and other transactions should be accorded the right to choose the particular information certifier, class of information certifiers or class of certificates that they wished to use in connection with messages or signatures that they received. the reference to parties to commercial and other transactions would include government agencies acting in their commercial capacity.

71. Variant B provides an illustrative list of criteria to be taken into account in assessing the reliability of foreign certificates.

References to national legislation and other texts

EC Draft 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 European Community:

(a) if the certification service provider fulfils the requirements laid down in this Directive and has been accredited in the context of a voluntary accreditation scheme established in a Member State of the European Community; or

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

(c) if the certificate or the certification service provider is recognized under the regime of a bilateral or multilateral agreement between the Community and third countries or international organizations.

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 will make proposals where appropriate to achieve the effective implementation of standards and international agreements applicable to certification services. In particular and where necessary, it will submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organizations. 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].

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.