UNITED
NATIONS

A

General Assembly

Distr.
LIMITED

A/CN.9/WG.IV/WP.73
12 December 1997

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Working Group on Electronic Commerce
Thirty-second session
Vienna, 19-30 January 1998

DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

Note by the Secretariat

CONTENTS

V.97-29151

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 work to be carried out by the Working Group at its thirty-first session could involve the preparation of draft rules on certain aspects of the above-mentioned topics. The Working Group was requested to provide the Commission with sufficient elements for an informed decision to be made as to the scope of the uniform rules to be prepared. As to a more precise mandate for the Working Group, 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). As to the desirability and feasibility of preparing uniform rules on issues of digital signatures and certification authorities, 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 it had not made a firm decision as to the form and content of such work, it 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). With respect to the issue of incorporation by reference, the Working Group concluded that no further study by the Secretariat was needed, since the fundamental issues were well known and it was clear that many aspects of battle-of-forms and adhesion contracts would need to be left to applicable national laws for reasons involving, for example, consumer protection and other public-policy considerations. The Working Group was of the opinion that the issue should be dealt with as the first substantive item on its agenda, at the beginning of its next session (A/CN.9/437, para. 155).

3. The Commission expressed its appreciation for the work already accomplished by the Working Group at its thirty-first session, 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").

4. 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. 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.

5. As an additional item to be considered in the context of future work in the area of electronic commerce, it was suggested that the Working Group might need to discuss, at a later stage, the issues of jurisdiction, applicable law and dispute settlement on the Internet. The Commission was informed that a colloquium on the issues of jurisdiction and applicable law on the Internet would take place in June 1997 under the auspices of the Hague Conference on Private International Law. The Commission was also informed that an international conference convened by the OECD in November 1997 would attempt to develop a coordinated approach to the issues of electronic commerce among interested Governments, intergovernmental organizations, non-governmental organizations and private sector groups. The Commission expressed the hope that those two events could be attended and reported upon by the Secretariat. [2]

6. This note contains revised draft provisions to be considered for possible inclusion in the Uniform Rules. These provisions deal with digital signatures, other electronic signatures, certification authorities and related legal issues. They were prepared pursuant to the deliberations and decisions of the Working Group at its thirty-first session, as reflected in the report of that session (A/CN.9/437) and also pursuant to the deliberations and decisions of the Commission at its thirtieth session, as reproduced above. In particular, the draft provisions are based on the working assumption adopted by the Working Group that its work in the area of digital signatures would take the form of draft statutory provisions (A/CN.9/437, para. 27). They are also intended to reflect the decision made by the Working Group at its previous session that possible uniform rules in the area of digital signatures should be derived from article 7 of the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law") and should be considered as setting out a manner in which a reliable method could be used "to identify a person" and "to indicate that person's approval" of the information contained in a data message. More generally, pending a final decision as to the relationship between the Model Law, the Uniform Rules and possible rules on incorporation by reference (see A/CN.9/437, paras. 151-155), the draft provisions are intended to be consistent with the principles expressed, and the terminology used, in the Model Law (A/CN.9/437, para. 26).

7. This note does not deal with the issues of jurisdiction, applicable law and dispute settlement on the Internet, the formation and performance of contracts in an electronic environment, or with any other issue that may need to be considered by the Working Group at a future session. An oral report will be presented to the Working Group regarding the

colloquium on the issues of jurisdiction and applicable law on the Internet, which was held in June 1997 under the auspices of the Hague Conference on Private International Law and the international conference convened by the OECD in November 1997 (see above, para. 5).

8. In the preparation of this note, the Secretariat was assisted by a group of experts, comprising both experts invited by the Secretariat and experts designated by interested governments and international organizations.

I. GENERAL REMARKS

9. 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.

10. 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.

11. 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).

II. DRAFT PROVISIONS ON DIGITAL SIGNATURES, OTHER ELECTRONIC SIGNATURES, CERTIFICATION AUTHORITIES AND RELATED LEGAL ISSUES

CHAPTER I. SPHERE OF APPLICATION AND GENERAL PROVISIONS

12. 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. In particular, the Working Group might wish to make proposals to the Commission as to whether uniform rules on digital signatures should constitute a separate legal instrument or whether they should be incorporated in an extended version of the Model Law, for example as a new part III of the Model Law.

13. If the Uniform Rules are prepared as a separate instrument or as an addition to the Model Law, it is submitted that they will need to incorporate provisions along the lines of articles 1 (Sphere of application), 2(a),(c) and (e) (Definitions of "data message", "originator" and "addressee"), 3 (Interpretation), 7 (Signature) and 13 (Attribution of data messages) of the Model Law. While those articles are not reproduced in this note, it should be noted that the

draft provisions of the Uniform Rules have been prepared by the Secretariat based on the assumption that such provisions would form part of the Uniform Rules. With respect to the sphere of application of the Uniform Rules, it should be borne in mind that under article 1 of the Model Law, transactions involving consumers, while not the focus of the Uniform Rules, would not be excluded from their sphere of application unless the law applicable to consumer transactions in the enacting State conflicted with the Uniform Rules (see A/CN.9/WG.IV/WP.71, paras. 49-50).

14. As to the question of party autonomy, the mere reference to article 4 (Variation by agreement) of the Model Law may not suffice to provide a satisfactory solution, in view of the fact that article 4 establishes a distinction between those provisions of the Model Law that may be freely varied by contract and those provisions that should be regarded as mandatory unless variation by agreement is authorized by the law applicable outside the Model Law. With respect to electronic signatures, the practical importance of "closed" networks makes it necessary to provide wide recognition of party autonomy. However, public policy restrictions on freedom of contract, including laws protecting consumers from overreaching contracts of adhesion, may also need to be taken into consideration. The Working Group may thus wish to include in the Uniform Rules a provision along the lines of article 4(1) of the Model Law to the effect that, except as otherwise provided by the Uniform Rules or other applicable law, electronic signatures and certificates issued, received or relied upon in accordance with procedures agreed among the parties to a transaction are given the effect specified in the agreement. In addition, the Working Group might consider establishing a rule of interpretation to the effect that, in determining whether a certificate, an electronic signature or a data message verified with reference to a certificate, is sufficiently reliable for a particular purpose, all relevant agreements involving the parties, any course of conduct among them, and any relevant trade usage should be taken into account.

15. In addition to the above-mentioned provisions, 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 digital communication by establishing a security framework and by giving written and digital messages equal status as regards their legal effect (see A/CN.9/WG.IV/WP.71, para. 51).

CHAPTER II. ELECTRONIC SIGNATURES

Section I. Secure electronic signatures

Article 1. Definitions

For the purposes of these Rules:

(a) "Signature" means any symbol used, or any security procedure adopted by [or on behalf of] a person with the intent to identify that person and to indicate that person's approval of the information to which the signature is appended;

(b) "Electronic signature" means [a signature] [data] in electronic form in, or attached to, or logically associated with, a data message [and used by [or on behalf of] a person with the intent to identify that person and to indicate that person's approval of the contents of the data message] [and used to satisfy the conditions in [article 7 of the UNCITRAL Model Law on Electronic Commerce]];

(c) "Secure electronic signature" means an electronic signature which

(i) is a digital signature under article 4 and meets the requirements set forth in article 5; or

(ii) as of the time it was made, can otherwise be verified to be the signature of a specific person through the application of a security procedure that is: uniquely linked to the person using it; capable of promptly, objectively and automatically identifying that person; created in a manner or using a means under the sole control of the person using it; and linked to the data message to which it relates in a manner such that if the message is altered the electronic signature is invalidated; or

(iii) [as between parties involved in generating, sending, receiving, storing or otherwise processing data messages in the ordinary course of their business,] is commercially reasonable under the circumstances, previously agreed to, and properly applied, by the parties.

References

A/CN.9/437, paras. 29-50 and 90-113 (draft articles A, B and C);
A/CN.9/WG.IV/WP.71, paras. 52-60.

Remarks

16. Draft article 1 is intended to reflect the decision reached by the Working Group at its thirtieth session that, consistent with media neutrality in the Model Law, the Uniform Rules should not discourage the use of any technique that would provide a "method as reliable as appropriate" as an alternative to handwritten and other paper-based signatures in compliance with article 7 of the Model Law. While the Uniform Rules may focus on issues of digital signatures, a more general approach should also be taken, and issues relevant to other electronic signature techniques could also be considered (see A/CN.9/437, para. 22).

17. Through a definition of "signature" and "electronic signature" in subparagraphs (a) and (b), the scope of the Uniform Rules is thus delineated in broad terms to cover all techniques that might be applied to provide the functional equivalent of a handwritten signature, as understood in article 7 of the Model Law. It should be noted that the definition of "signature", which merely restates article 7(1)(a) of the Model Law in the form of a definition, is not intended to replace or otherwise affect any definition of "signature" or "handwritten signature" that might exist outside the Uniform Rules (e.g., in domestic legislation or case

law). That definition is intended mostly to serve as a basis for the subsequent definitions of "electronic signature" and "secure electronic signature". It may also serve as a useful reference in countries where no definition of "signature" currently exists.

18. The three levels of definition set forth in draft article 1 (i.e., "signature", "electronic signature" and "secure electronic signature") are intended to provide the Working Group with an analytic tool, and to reflect a distinction which has become familiar in draft legislation in a number of countries. However, depending on the contents of the Uniform Rules, not all three definitions may be necessary. Should the Working Group decide to focus on one legal effect of electronic signatures (i.e., recognition as a functional equivalent to handwritten signatures), only one category of "electronic signatures" might need to be considered. The notions currently defined as "electronic signature" and "secure electronic signature" could thus be merged into one legal category, irrespective of the number and variety of techniques that would be considered under that legal category.

19. The main definition to be relied upon for the purposes of delineating the scope of the Uniform Rules is that currently embodied in subparagraph (c) under the heading "secure electronic signature". As a matter of drafting, it may be noted that the word "secure" is not intended to indicate that any given technique may, in fact or in law, provide absolute security. It is merely intended to qualify a higher level of trustworthiness of an electronic signature by reference to a set of criteria which, once met, would entail certain legal effects.

20. Aimed at providing a basis for the legal effects to be derived from the use of electronic signatures, subparagraph (c) is also intended to reflect the "dual approach" adopted by the Working Group at its previous session. The "dual approach" stemmed from the two alternatives under debate, namely the establishment of criteria for a governmental authorization of certification authorities and the recognition of operation criteria for certification authorities functioning outside a governmentally-implemented public-key infrastructure. The Working Group came to the conclusion that those two alternatives might not be mutually exclusive. The difference between the two situations might reside in the modalities under which legal effect might be given to digital signatures in one or the other case. In the case of governmentally-authorized (or "licensed") certification authorities, the fulfilment of the applicable operation criteria by a certification authority would constitute a prerequisite for the authorization of that certification authority, which, in turn, would be a condition for the recognition of the legal effectiveness of the certificates issued by that certification authority. In the second situation, a certification authority would not need to demonstrate that the operation criteria were met prior to beginning to function. However, if the certificates it issued were to be challenged (e.g., in a judicial dispute or arbitration), the adjudicating body would need to assess the trustworthiness of the certificate by determining whether it had been issued by a certification authority meeting those criteria (see A/CN.9/437, para. 48).

21. In addition to allowing for the operation of both licensed and non-licensed certification authorities, subparagraph (c) further opens the sphere of application of the Uniform Rules to cover authentication devices that would operate without requiring reliance on any kind of certification authority or other "trusted third party". The reference to the "secure" status thus allows to introduce both licensing schemes through which enacting States might establish the

quality and reliability of digital signatures, and market-driven practices that might rely on other forms of electronic signatures.

22. Under subparagraph (c)(i), the secure status would be presumed under the Uniform Rules if a digital signature was applied in conformity with a public-key infrastructure established by the enacting State. In the absence of, or in addition to, such a public-key infrastructure, any kind of electronic signature (i.e., digital and other electronic signatures applied with or without the intervention of certification authorities or other trusted third parties) could be granted secure status, provided that minimum requirements were met. With a view to providing a basic standard against which the quality of such electronic signatures might be assessed, subparagraph (c)(ii) lists four criteria: uniqueness, identification, reliability, and linkage with the information being signed.

23. The requirement that a secure electronic signature be "uniquely linked" to the person applying it is intended to ensure that there is no reasonable likelihood that more than one person would produce the same signature absent fraud or other improper conduct. The requirement of uniqueness could also presumably be satisfied by a biometric-based signature that would incorporate certain attributes unique to the signer, such as a fingerprint or a retinal scan. This requirement would also be satisfied with respect to a digital signature where the key pair used by the signer was randomly generated and of sufficient key length, so that the likelihood of anyone else generating the same key pair would be extremely remote.

24. A secure signature should be such that it can be used to identify the signer. This does not mean that the signature itself must consist of or include the signer's name. Identification by reference to other sources of information would be sufficient. Thus, for example, a digital signature may identify the signer by reference to a certificate issued by a certification authority. The main requirement is that the identification process must be relatively prompt, objective, and automatic. Thus, for example, while a handwritten signature is presumably capable of identifying the signer, such identification cannot normally be made promptly or automatically, and is frequently not an objective determination. In many cases, the signature itself is not readable. Even where it is readable, that signature may ultimately be capable of identifying the signer, but the timing and certainty of the identification process may not always satisfy the requirements of electronic commerce. Thus, a handwritten signature may not always be reliably identified as the signature of a particular individual (in the absence of an admission of that fact or a witness to the signing) without the testimony of an expert in handwriting analysis who has compared admitted signatures of the purported signer with the signature in question. In such a case, the result is unlikely to be prompt or automatic, and the conclusion of the expert is in many respects subjective rather than objective. By contrast, the use of a personal identification number (PIN) in an automatic teller machine provides the bank with an automatic, objective, and prompt identification of a specific person that is tied to a specific address and a specific account number when the funds are withdrawn. Such a person is not in a position to deny that the request for funds contains his or her signature (although that person may deny having signed the request; that is the subject of the reliability requirement).

25. In addition to identifying a person as the signer of a message, the procedure used to sign the message must provide a reasonably reliable assurance that the person identified as the signer is in fact the person who signed the message. A security procedure that requires the use of a manner or means that is under the sole control of the person creating the signature may satisfy such a reliability requirement. The use of a trusted third party may also provide the requisite level of reliability. There may also exist other means by which this requirement can be met. The Working Group may wish to discuss other approaches through which an acceptable level of reliability can be assured.

26. A secure signature must be linked to the data message being signed, in such a manner that if the message is changed the signature is invalidated. Such a linkage may be regarded as a crucial requirement for a secure signature, since otherwise the signature could be simply excised from one data message and pasted onto another.

27. Subparagraphs (c)(i) and (ii) are intended to apply in the absence of a pre-existing contractual arrangement regarding electronic signatures between the originator and the addressee of the data message being signed. However, consistent with the approach taken in the Model Law, the Uniform Rules may need to reaffirm the validity of contractual schemes with respect to authentication of data messages. Subparagraph (c)(iii) thus validates closed-system agreements. The Working Group may wish to discuss whether the wording between square brackets ("as between parties involved in generating, sending, receiving, storing or otherwise processing data messages in the ordinary course of their business,"), which mirrors wording used in the Model Law, is needed to limit the effect of party autonomy to business uses of electronic signatures, to the exclusion of transactions involving consumers (see A/CN.9/437, para. 24).

Article 2 Presumptions

(1) With respect to a data message authenticated by means of a secure electronic signature, it is rebuttably presumed that:

(a) the data message has not been altered since the time the secure electronic signature was affixed to the data message;

(b) the secure electronic signature is the signature of the person to whom it relates; and

(c) the secure electronic signature was affixed by that person with the intention of signing the message.

(2) With respect to a data message authenticated by means of an electronic signature other than a secure electronic signature, nothing in these Rules affects existing legal or evidentiary rules regarding the burden of proving the authenticity and integrity of a data message or an electronic signature.

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

[(4) The presumptions in paragraph (1) may be rebutted by:

(a) evidence indicating that a security procedure used to verify an electronic signature is not to be generally recognized as trustworthy, due to advances in technology, the way in which the security procedure was implemented, or other reasons;

(b) evidence indicating that the security procedure agreed to between the parties under article 1(c)(iii) was not implemented in a trustworthy manner; or

(c) evidence relating to facts of which the relying party was aware which would suggest that reliance on the security procedure was not reasonable. The commercial reasonableness of a security procedure agreed upon by the parties under article 1(c)(iii) is to be determined in light of the purposes of the procedure and the commercial circumstances at the time the parties agreed to adopt the procedure, including the nature of the transaction, sophistication of the parties, volume of similar transactions engaged in by either or both of the parties, availability of alternatives offered to but rejected by the party, cost of alternative procedures, and procedures in general use for similar types of transactions.]

References

A/CN.9/437, paras. 43, 48 and 92.

Remarks

28. Draft article 2 focuses on the legal effects flowing from recognition of the "secure electronic signature" status. At its previous session, the Working Group discussed the possibility that certain issues of electronic signatures (e.g., liability of certification authorities, and attribution of digitally-signed messages) might be dealt with by way of presumptions (see A/CN.9/437, paras. 58, 70, and 120-121).

29. The concept of a secure electronic signature, and the rebuttable presumptions that flow from that status may be regarded as critical to enabling a viable system of electronic commerce. With paper-based transactions, a number of indicators can be used by a relying party to determine whether the document is authentic and the signature genuine. These include the use of paper (sometimes with water marks, coloured backgrounds, or other indicators of reliability) to which the message is affixed, the use of letterhead, handwritten signatures, or delivery in sealed envelopes via a trusted third party (such as postal services). With electronic communications, however, none of these factors of reliability are present. All that can be communicated is a set of electronic impulses that are in all respects identical, and can easily be copied or modified. Thus, in many cases it is important for the addressee and for any other party relying on an electronic communication to know, at the time of receipt or reliance, whether the message is authentic, whether the integrity of its contents has been preserved, and whether it will be able to establish both of those facts in the event of a subsequent dispute (e.g., to establish in court the non-repudiation of a data message). To that end, the existence

of rebuttable presumptions with respect to secure signatures may provide such assurances to relying parties thereby enabling them to engage in commercial activities with confidence that their transactions will be easier to enforce if that should become necessary.

30. The effect of the presumptions in draft article 2 should be distinguished from the effect of attribution under draft article 3. The presumptions in draft article 2 are designed to ease the burden of proving the source of an electronic message when the recipient has verified the apparent source of the message by use of a secure electronic signature. The person to whom the signature relates is thus required to prove that, notwithstanding the addressee's verification of the secure electronic signature and reliance on the security procedure, the signature was not that of that person. As a justification for establishing such a presumption, it may be noted that the evidence necessary to prove who actually sent the message is normally in the possession of the person to whom the signature relates. For example, in the case of a digital signature, the person to whom the signature relates is ordinarily in a better position than any other relying party to prove that the private key was stolen, copied, compromised, or used without authority by a third person. In a typical situation, the recipient of the message will have no evidence other than the security procedure used with which to prove that the person to whom the signature relates did, in fact, send the message. However, under draft article 3, even if the party to whom the signature relates can establish that it did not send the message in question, it may nevertheless be liable for losses caused to the recipient who reasonably relied if the requirements of draft article 3 are met.

31. Consistent with the approach taken in article 7 of the Model Law, paragraph (1) does not create a presumption that the data message bearing a secure electronic signature constitutes a legally binding obligation. Paragraph (1) merely presumes that the secure electronic signature was affixed by the purported signer with the intention of signing the message. If there is evidence that the person whose signature was affixed was the victim of mistake, misrepresentation, duress, or other invalidating cause, the message may be denied legal effect, but the burden of raising these issues rests with the person denying the legal effect of the data message.

32. Paragraph (2) makes it clear that, in the absence of a secure electronic signature, nothing in the Uniform Rules changes the ordinary rules of evidence about the burden of proving the source of a message. Paragraph (3) is modelled on similar provisions in the Model Law. It is intended to facilitate the exclusion of certain situations from the benefit of draft article 2 in cases where a legitimate interest would require such an exclusion by the enacting State. For example, enacting States may decide that the presumptions established in draft article 2 do not apply in the area of criminal law. Paragraph (4) lists a number of ways in which the presumption established in paragraph (1) may be rebutted. The Working Group may wish to discuss whether such an illustrative provision is needed in the text of the Uniform Rules or whether it should be considered in the context of a guide or commentary.

Article 3. Attribution

(1) Variant A Subject to [article 13 of the UNCITRAL Model Law on Electronic Commerce], the originator of a data message on which the originator's secure electronic signature is affixed is [bound by the content] [deemed to be the signer] of the message in the same manner as if the message had existed in a [manually] signed form in accordance with the law applicable to the content of the message.

Variant B As between the holder of a private key and any third party who relies on a digital signature which can be [verified][authenticated] by using the corresponding certified public key, the digital signature [is presumed to be that of the holder] [satisfies the conditions set forth in [article 7(1) of the UNCITRAL Model Law on Electronic Commerce]].

(2) Paragraph (1) does not apply if

(a) the [originator] [holder] can establish that the [secure electronic signature] [private key] was used without authorization and that the [originator] [holder] could not have avoided such use by exercising reasonable care; or

(b) the relying party knew or should have known, had it sought information from the [originator] [certification authority] or otherwise exercised reasonable care, that the [secure electronic] [digital] signature was not that of the [originator] [holder of the private key].

References

A/CN.9/437, paras. 118-124 (draft article E);
A/CN.9/WG.IV/WP.71, paras. 64-65.

Remarks

33. At its previous session, the Working Group generally felt that no attempt should be made to restate in the context of the Uniform Rules the principles set forth in article 13 of the Model Law (see A/CN.9/437, paras. 119-120). However, it was also felt that the relationship between the Uniform Rules and articles 7 and 13 of the Model Law needed to be clarified. To that effect, Variant A of paragraph (1), which reflects a principle that was found generally acceptable by the Working Group at its previous session (see A/CN.9/437, para. 120), is worded in broad terms to encompass both digital signatures and alternative techniques that may be used for producing a secure digital signature.

34. Variant B creates a presumption that a digital signature fulfils the requirements for a "reliable method" under article 7 of the Model Law. The Working Group may wish to consider whether such a presumption should be extended to cover not only digital signatures

but also other instances where a secure electronic signature is used. Should the Working Group wish to limit the scope of the provision to digital signatures, draft article 3 would need to be relocated accordingly.

35. The Working Group may wish to discuss whether draft article 3 might be used to deal more precisely with the question of when a person can be held accountable for the content of a data message where that message was not in fact sent by that person, and the message is communicated in an open environment (i.e., without a prior agreement being made directly between the originator and the recipient of the message (or in the context of "system rules") as to the procedure to be applied for determining the attribution of the data message). While article 13(3)(a) of the Model Law deals with that issue where "a procedure previously agreed to by the originator" is used, the Model Law does not deal expressly with the open environment. Given the high level of security inherent in secure electronic signatures, the Working Group may wish to consider whether a general rule might be established to the effect that the recipient of a data message who reasonably relies on a secure electronic signature is entitled to regard that message as being that of the originator.

36. As an example of a provision to that effect, the Working Group may wish to consider the following wording:

> Except as provided by other applicable law, a secure electronic signature is attributable to the person to whom it appears to relate, whether or not authorized by that person, if:
>
> (a) the electronic signature resulted from acts of a person that obtained the access numbers, codes, computer programs, or other information necessary to create the signature from a source under the control of the purported signer, creating the appearance that it came from that person;
>
> (b) the access occurred under circumstances resulting from a failure to exercise reasonable care by the purported signer; and
>
> (c) The recipient relied in good faith to its detriment on the apparent source of the data message.

The effect of such wording is to allocate the risk of loss between the two interested parties, i.e., the purported originator who did not actually sign the message in question, and the recipient who relied on the message in good faith pursuant to a commercially reasonable security procedure. The risk of loss is put on the purported originator only in the situation where the message bears the signature of the purported originator as a result of the purported originator's fault. Such a situation may occur where the signature was created by a person who obtained the necessary information from a source under the control of the purported originator and where such access occurred under circumstances resulting from a failure to exercise reasonable care by the purported originator. In such a case, if the recipient reasonably relies on the message, the purported originator will be bound. In all other cases, the risk of loss will fall on the recipient notwithstanding any reasonable reliance. The

reference to "other applicable law" in the opening words may be necessary to exclude consumer transactions from the scope of the suggested rule.

Section II. Digital signatures

Article 4. Definition

For the purposes of these Rules,

Variant A "digital signature" means a type of an electronic signature consisting of a transformation of a data message using a message digest function and an asymmetric cryptosystem such that any person having the initial untransformed data message and the signer's public key can accurately determine:

(a) whether the transformation was created using the signer's private key that corresponds to the signer's public key; and

(b) whether the initial data message has been altered since the transformation was made.

Variant B (a) "digital signature" means a numerical value, which is affixed to a data message and which, using a known mathematical procedure associated with the originator's private cryptographic key, makes it possible to determine that this numerical value has only been obtained with the originator's private key;

(b) The mathematical procedures used for generating digital signatures under these Rules are based on public-key encryption. When applied to a data message, those mathematical procedures operate a transformation of the message such that a person having the initial message and the originator's public key can accurately determine:

(i) whether the transformation was operated using the private key that corresponds to the originator's public key; and

(ii) whether the initial message was altered after the transformation was made.

References

A/CN.9/437, paras. 30-38 (draft article A);
A/CN.9/WG.IV/WP.71, paras. 18-45 and 55-56.

Remarks

37. The differences between Variants A and B are mostly of a drafting nature. While Variant B reflects the conclusions reached by the Working Group at its previous session (see A/CN.9/437, para. 32), Variant A provides simpler wording, building upon the definition of "electronic signature". In both Variants, "digital signature" is defined without reference to "certification authorities" or "certificates".

38. No attempt has been made to provide definitions of "private key", "public key", "key pair" or other concepts relating to public-key cryptography. While suggestions for additional definitions were made at the previous session of the Working Group, a note of caution was struck about introducing a large number of definitions in uniform rules of a statutory nature, which might be contrary to the legislative tradition in many countries. The Working Group may wish to discuss the extent to which additional definitions might be necessary (see A/CN.9/437, para. 29).

Article 5. Effects

(1) Where all or any portion of a data message is signed with a digital signature, the digital signature is regarded as a secure electronic signature with respect to such portion of the message if:

(a) the digital signature was created during the operational period of a [valid] certificate and is verified by reference to the public key listed in the certificate; and

(b) the certificate is considered as accurately binding a public key to a person's identity because:

(i) the certificate was issued by a certification authority licensed [accredited] by ... *[the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities]*; or

(ii) the certificate was otherwise issued by a certification authority in accordance with standards issued by ... *[the enacting State specifies the organ or authority competent to issue recognized standards for the operation of licensed certification authorities]*.

(2) Where all or any portion of a data message is signed with a digital signature that does not meet the requirements set forth in paragraph (1), the digital signature is regarded as a secure electronic signature with respect to such portion of the message if sufficient evidence indicates that the certificate accurately binds the public key to the holder's identity.

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

References

A/CN.9/437, paras. 43, 48 and 92.

Remarks

39. Digital signatures, if properly implemented, should constitute secure electronic signatures. However, a question is to determine when the implementation of a digital signature has been done in a manner such that it is entitled to secure status. Not all digital signatures verifiable with reference to a certificate are secure, especially where there is uncertainty as to whether the identification or authentication of the holder or the public key is accurate. The primary factors that determine whether a digital signature is secure include: (1) whether the certification authority has properly identified the holder; (2) whether the certification authority has properly authenticated the holder's public key; (3) whether the holder's private key has been compromised; and (4) whether the process is trustworthy (e.g., whether the public key algorithm and the key length used are appropriate).

40. Paragraph (1) sets forth two basic criteria for determining when a digital signature qualifies as a secure electronic signature. The first criterion requires that the signature be created during the operational period of a valid certificate and be verified by reference to the public key listed in the certificate. The operational period of a certificate normally begins at the time it is issued and ends upon the earlier of expiration, revocation or suspension.

41. The second step involves providing assurance that the certificate itself accurately identifies a person as the holder of the private key corresponding to the public key specified in the certificate. The trustworthiness of the certificate may be assessed by reference to standards, procedures, and other requirements specified by authorities recognized in the enacting State. Such standards may be established through accreditation of certification authorities by third parties, the voluntary licensing of certification authorities, or otherwise require compliance with rules adopted by the enacting State.

42. Alternatively, under paragraph (2), if a court or other trier of fact determines, as a matter of evidence, that the information stated in the certificate is in fact true, then the trustworthiness of the certificate is obvious. At this stage, however, the trier of fact is required to determine on a case-by-case basis whether the certificate was issued by a certification authority that properly identified the holder and authenticated the holder's public key.

43. Consistent with the "dual approach" taken by the Working Group, draft article 5 is intended to provide as much latitude as possible for making a determination as to the trustworthiness of a certificate issued by a certificate authority. This flexibility is particularly important in light of the fact that the use of digital signatures is new and the models for its use as well as its regulation have not yet fully developed. Thus, it is important to facilitate the increased use of digital signatures in electronic commerce, while at the same time establishing the standards necessary to make a presumptive determination as to the reliability of a digitally-signed message.

44. It is also important to note that while one of the options set forth in draft article 5 includes a judicial determination of the accuracy of a certificate, the other option presumes the accuracy of a certificate if it was issued by a certification authority accredited by the enacting State or if it otherwise meets certain standards established by the enacting State. In such a case, a judicial finding of accuracy is not required in order to qualify for a secure electronic signature status. The second option may be helpful to persons engaging in electronic commerce, who would know in advance of acting in reliance on a communication whether such action can be enforced. However, the presumption of accuracy may be rebutted by showing that a certificate issued by such an accredited certification authority is, in fact, not accurate or reliable.

[Article 6. Signature by legal persons

A legal person may identify a data message by affixing to that message the public cryptographic key certified for that legal person. The legal person shall only be regarded as [the originator][having approved the sending] of the message if the message is also digitally signed by the natural person authorized to act on behalf of that legal person.]

References

A/CN.9/437, paras. 114-117 (draft article D);
A/CN.9/WG.IV/WP.71, paras. 61-63.

Remarks

45. At the previous session, it was widely felt that draft article 6 should be deleted. After discussion, however, the Working Group decided that it should be placed between square brackets, for further consideration at a later session (A/CN.9/437, paras. 115 and 117). While a provision along the lines of draft article 6 may be seen as inappropriately interfering with other bodies of law (e.g., the law of agency, and the provisions of company law dealing with representation of companies by natural persons), it may also be useful at the current stage of development of the Uniform Rules, as a reminder that the Working Group may need to discuss more fully the extent to which the Uniform Rules should validate the operation of "electronic agents" for the purpose of automatically authenticating data messages.

Section III. Other electronic signatures

46. Since no information was communicated to the Secretariat as to how authentication techniques other than digital signatures might be dealt with under the Uniform Rules, no specific provision has been prepared for inclusion in this section. The Working Group may wish to discuss whether such authentication techniques should be dealt with in more detail in the Uniform Rules. Should the Working Group come to the conclusion that such techniques should not be addressed more specifically, the Uniform Rules would still favour the increased use of alternatives to digital signatures, through the principle of non-discrimination embodied

in the definitions of "signature"and "secure electronic signatures", and through the legal status recognized to any authentication technique that would qualify as a "secure electronic signature".

CHAPTER III. CERTIFICATION AUTHORITIES AND RELATED ISSUES

Article 7. Certification authority

(1) For the purposes of these Rules, "certification authority" means:

(a) any person or entity licensed [accredited] by ... *[the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities]* to act in pursuance of these Rules; or

(b) any person who, or entity which, as an ordinary part of its business, engages in issuing certificates in relation to cryptographic keys used for the purposes of digital signatures.

[(2) A certification authority may offer or facilitate registration and time stamping of the transmission and reception of data messages as well as other functions regarding communications secured by means of digital signatures.]

References

A/CN.9/437, paras. 39-50 and 90-97 (draft article B);
A/CN.9/WG.IV/WP.71, paras. 18-45 and 57-58.

Remarks

47. As indicated in the context of draft article 1, the Uniform Rules should provide legal recognition for both the situation where an enacting State wishes to regulate the operation of certification authorities through a public-key infrastructure or other licensing scheme, and the situation where unlicensed certification authorities may operate freely under market-driven practice standards (see above, paras. 17-18).

48. In dealing with licensed certification authorities, paragraph (1) does not attempt to define criteria to be used by enacting States in implementing a public-key infrastructure or other licensing scheme for certification authorities. A reason for not dealing with those criteria may be the strong public policy component of such public-key infrastructures, which may not easily lend themselves to international harmonization by way of model legislative provisions. Should the Working Group engage in more detailed consideration of the criteria to be used in the context of a licensing scheme, it may wish to consider the following factors, to be taken into

account when assessing the trustworthiness of a certification authority: (1) independence (i.e., absence of financial or other interest in underlying transactions); (2) financial resources and financial ability to bear the risk of being held liable for loss; (3) competence of the personnel at the managerial level, expertise in public-key technology and familiarity with proper security procedures; (4) longevity (certification authorities may be required to produce evidence of certification or decryption keys many years after the underlying transaction has been completed, in the context of a lawsuit or property claim); (5) approval of hardware and software; (6) maintenance of an audit trail, and audit by an independent entity; (7) existence of a contingency plan (e.g., "disaster recovery" software or key escrow); (8) personnel selection and management; (9) protection arrangements for the certification authority's own private key; (10) internal security; (11) arrangements for termination of operations, including notice to users; (12) warranties and representations (given or excluded); (13) limitation of liability; (14) insurance; (15) inter-operability with other certification authorities; (16) revocation procedures (in cases where cryptographic keys might be lost or compromised); (17) isolation of the certifying function from any other business that the certification authority might pursue (see A/CN.9/WG.IV/WP.71, para. 44 and A/CN.9/437, para. 45).

49. Paragraph (1)(b) defines "certification authority" without any mention of governmental authorization, by reference to its function as the issuer of certificates. Such a provision, in combination with paragraph (2), is also intended to reflect the fact that, while certification authorities may perform other functions and offer services in addition to issuing certificates, such functions and services are outside the sphere of application of the Uniform Rules and should not be taken into account when dealing with the legal effects of electronic signatures. The Working Group may wish to discuss whether a provision along the lines of paragraph (2), which is mainly descriptive in nature should form part of the Uniform Rules or whether it should rather be expressed in a guide or commentary.

Article 8. Certificate

For the purposes of these Rules, "certificate"means a data message [or other record] which, at least:

(a) identifies the certification authority issuing it;

(b) names or identifies its holder or a device or electronic agent under the control of the holder;

(c) contains a public key which corresponds to a private key under the control of the holder;

(d) specifies its operational period [and existing restrictions, if any, on the scope of use of the public key]; and

(e) is [digitally] signed by the certification authority issuing it.

References

A/CN.9/437, paras. 98-113 (draft article C);
A/CN.9/WG.IV/WP.71, paras. 18-45 and 59-60.

Remarks

50. While a certificate may be used for performing a variety of functions and conveying additional information outside the scope of the Uniform Rules, the only function of a certificate addressed by the Uniform Rules is that of linking a public key to a given holder. Such a linkage may be done directly, by naming the holder of the public key in the certificate. It can also be done indirectly by describing certain attributes about the holder (e.g., a purchasing agent with authority to contract for purchases up to a given amount), or by describing a machine, device, or software agent under the control of the holder. Thus, for example, a certificate may be issued to an employee of a corporation specifying only the limits of such employee's purchasing authorization. It might then be used in purchase transactions with trading partners where the identity of the individual employee is not important, but rather the main issues are whether that employee has authority to act on behalf of an identified person (i.e., the employer), and the limit of the employee's purchasing authority. In all cases, however, there is a person, known as the "holder" who controls the private key that corresponds to the public key identified in the certificate and who is the person to whom digitally signed messages verified by reference to the certificate are to be attributed. If no such person is identified, then the certificate cannot be used to verify that a digital signature is that of a specified person.

51. Draft article 8 is intended to reflect the elements regarded by the Working Group as the basic components of a certificate, namely, that a certificate should: be a data message; identify the certification authority; contain the public key of the holder; identify the holder; and be digitally signed by the certification authority (see A/CN.9/437, para. 101). As to whether a certificate should necessarily be in the form of a data message, the Working Group may wish to discuss whether the Uniform Rules should also cover paper-based certificates.

52. At the previous session, the Working Group decided that it might need to consider whether establishing a mandatory rule regarding the minimum information to be provided in a certificate might run counter to applicable law on data protection. It is submitted that, in view of the nature of the elements listed in draft article 8, such potential conflict is avoided.

53. The definition of "certificate" does not distinguish between different levels of security that may be provided that may be provided commercially under the heading of a "certificate". However, in preparing the Uniform Rules, the Working Group may bear in mind that certification authorities typically offer various classes of certificates. At the previous session of the Working Group, various suggestions were made for reflecting in the Uniform Rules the various levels of security that might result from the use of such certificates (see A/CN.9/437, paras. 20, 56, 138 and 145). As an example of such variety, the three classes of "certificates" listed below are reported as being available on the market.

54. Class I certificates confirm that a user's name and electronic-mail address form an unambiguous subject name within the register, or "repository" maintained by the certification authority. They are typically used primarily for browsing on the Internet and for personal electronic mail, with the purpose of modestly enhancing the security of these environments. Class I certificates are not intended to authenticate the identity of the holder. Rather, they represent a simple check of the non-ambiguity of the subject name within the repository, and a limited verification of the electronic mail address. The holder's name contained in a class 1 certificate is considered as non-verified information. These certificates provide a very low level of security. They are not intended for commercial use where proof of identity is required and should not be relied upon for such uses.

55. Class II certificates confirm that the information provided by the holder when applying for the certificate does not conflict with the information accessible in widely recognized consumer databases. Class 2 certificates are typically used for: (1) inter-organizational electronic mail; (2) low-value, low-risk transactions; (3) personal electronic mail; (4) password replacement; (4) software validation; and (5) on-line subscription services. Class 2 certificates provide a certain level of assurance as to the holder's identity, based on an automated, on-line process.

56. Class III certificates provide important assurances as to the identity of the holder, for example by requiring personal (physical) appearance of the holder before an agent of the certification authority, or verification of its identity through appropriate identity documents. The private key corresponding to the public key contained in a Class III certificate must be generated and stored in a trustworthy manner according to the requirements set forth by the certification authority. Class III certificates are used in practice for certain electronic commerce applications such as electronic banking, electronic data interchange (EDI), and membership-based on-line services. Class III certificate processes utilize various procedures to obtain probative evidence of the identity of individual subscribers. These validation procedures provide stronger assurances of an applicant's identity than class II certificates.

57. In the preceding examples, it is clear that only class III certificates would fall within the current scope of the Uniform Rules. The Working Group may wish to discuss whether the scope of the Uniform Rules should be expanded to cover also lower classes of certificates, in which case a decision would need to be made as to the various legal effects that would be attached to the various classes of certificates, in particular with respect to the level of liability that would be imposed on certification authorities with respect to the issuance of low-class certificates. Alternatively, the definition of "certificate" in the uniform Rules might need to be amended to make it clear that lower-level certificates would not be covered by the Uniform Rules.

Article 9. Certification practice statement

For the purposes of these Rules, "certification practice statement" means a statement published by a certification authority that specifies the practices that the certification authority employs in issuing and otherwise handling certificates.

References

A/CN.9/437, paras. 60-62, 70, 110-111 and 149 (draft article J);
A/CN.9/WG.IV/WP.71, para. 89.

Remarks

58. The degree to which any party relying on a certificate can trust the link between a person and a public key, as evidenced by a certificate, depends on several factors. Those factors include the practices and procedures followed by the certification authority in authenticating the holder of the key pair, and the certification authority's operating policy, procedures, and security controls. Certification practice statements are often presented by existing certification authorities as one of the main elements through which they promote reliance in the trustworthiness of the certificates they issue and, more generally, as the standard of quality and liability that should govern the relationship between certification authorities and their clients.

59. A certification practice statement is a statement by the certification authority of the policies it follows or the details of the practices, procedures, and systems that it employs in its operations and in support of the issuance, management, and revocation of a certificate. Topics covered in a certification practice statement might include: (1) procedures used to authenticate the identity of the applicant for a certificate (prior to issuing the certificate); (2) the physical, procedural, and personnel controls used by the certification authority to perform securely the functions of key generation, certificate issuance, certificate revocation, audit, and archiving; (3) the security measures taken by the certification authority to protect its cryptographic keys; and (4) any related information. These issues are of importance both to the holder who is obtaining the certificate and to the relying parties who will use the certificate issued by the certification authority as the basis for entering into transactions with the holder.

60. The certification practice statement can take various forms, such as a contract involving all interested parties, or public notice to all interested parties. The main element, however, is notice to relying parties. The certification practice statement should constitute notice from the certification authority to all relying parties (including holders) of the practices employed by the certification authority in issuing, managing, and revoking certificates.

Article 10. Representations upon issuance of certificate

Variant A

(1) By issuing a certificate, a certification authority represents to any person who reasonably relies on the certificate, or on a digital signature verifiable by the public key listed in the certificate, that:

(a) the certification authority has complied with all applicable requirements of these Rules in issuing the certificate and, if the certification authority has published the

certificate or otherwise made it available to such a relying person, that the holder listed in the certificate [and rightfully holding the corresponding private key] has accepted it;

(b) the holder identified in the certificate [rightfully] holds the private key corresponding to the public key listed in the certificate;

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

(d) all information in the certificate is accurate as of the date it was issued, 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) to the certification authority's knowledge, there are no known, material facts omitted from the certificate which would, if known, adversely affect the reliability of the foregoing representations.

(2) Subject to paragraph (1), the certification authority which issues a certificate represents to any person who reasonably relies on the certificate, or on 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.

Variant B

(1) By issuing a certificate, a certification authority represents to the holder, and to any person who relies on information contained in the certificate[, in good faith and] during its operational period, that:

(a) the certification authority has [processed] [approved] [issued], and will manage and revoke if necessary, the certificate in accordance with:

(i) these Rules;

(ii) any other applicable law governing the issuance of the certificate; and

(iii) any applicable certification practice statement stated or incorporated by reference in the certificate, or of which such person has notice, if any;

(b) the certification authority has verified the identity of the holder to the extent stated in the certificate or any applicable certification practice statement, or in the absence of such a certification practice statement, the certification authority has verified the identity of the holder in a [reliable] [trustworthy] manner;

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

(d) except as set forth in the certificate or any applicable certification practice statement, to the certification authority's knowledge, all other information in the certificate is accurate as of the date the certificate was issued;

(e) if the certification authority has published the certificate, the holder identified in the certificate has accepted it.

[(2) 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.]

References:

A/CN.9/437, paras. 51-73 (draft article H);
A/CN.9/WG.IV/WP.71, paras. 70-72.

Remarks

61. Draft article 10 is intended to reflect the decision made by the Working Group that, in principle, the draft Uniform Rules should contain provisions regarding the liability incurred by certification authorities in the context of their participation in digital signature schemes (A/CN.9/437, para. 55). The minimum standard of liability set forth in draft article 10 is intended to apply only to the issuance of certificates for the purposes of digital signatures, as defined in draft article 4. The draft Uniform Rules do not attempt to deal with other activities or services that might be performed by certification authorities. Such activities and services may be subject to contractual arrangement between certification authorities and their customers, and to any other applicable law (ibid., para. 71).

62. At its thirty-first session, the Working Group generally agreed that wording along the lines of paragraph (1) of Variant A was, for the most part, acceptable in substance as the basis for future discussions. Although it does not expressly establish a rule on liability, paragraph (1) sets a minimum standard from which the parties should not be allowed to derogate by private agreement. In particular, no clause limiting the liability of a certification authority should be considered within the scope of any protection or benefit provided by the Uniform Rules if it conflicts with the above-mentioned requirements. Where the liability of a certification authority is alleged, the certification authority is presumed to be liable for the consequences of issuing a certificate, unless it can prove that it meets the requirements listed in paragraph (1). However, should a certification authority wish to undertake obligations stricter than the representations listed in paragraph (1), it should be allowed to do so, by way of clauses included in a certification practice statement or otherwise (A/CN.9/437, para. 70). Paragraph (2) is intended to address situations where certification practice statements would contain such stricter standards.

63. Variant B, while inspired by Variant A, places stronger emphasis on self-regulation by certification authorities. In particular in subparagraph (b), the certification authority does not

warrant that the holder rightfully holds the private key. Instead, the certification authority warrants that, for the purpose of establishing the link between the holder and the private key, it followed at least the procedures set forth in its certification practice statement or used "reliable" or "trustworthy" methods for identifying the holder. Paragraph (2) of Variant B makes it clear that paragraph (1)(a)(ii) also applies where the certificate is issued under the laws of another jurisdiction. The Working Group may wish to decide whether such clarification should be expressed in the Uniform Rules or in a guide or commentary.

Article 11. Contractual liability

(1) As between a certification authority issuing a certificate and the holder of that certificate [or any other party having a contractual relationship with the certification authority], the rights and obligations of the parties are determined by their agreement.

(2) Subject to article 10, a certification authority may, by agreement, exempt itself from liability for any loss due to defects in the information listed in the certificate, technical breakdowns or similar circumstances. However, the clause which limits or excludes the liability of the certification authority may not be invoked if exclusion or limitation of contractual liability would be grossly unfair, having regard to the purpose of the contract.

(3) The certification authority is not entitled to limit its liability if it is proved that the loss resulted from the act or omission of the certification authority done with intent to cause damage or recklessly and with knowledge that damage would probably result.

References:

A/CN.9/437, paras. 51-73 (draft article H);
A/CN.9/WG.IV/WP.71, paras. 70-72.

Remarks

64. Paragraph (1) restates the principle of party autonomy in connection with the liability regime applicable to the certification authority. Paragraph (2) deals with the issue of exemption clauses, which are generally declared admissible, with two exceptions. The first exception comes from a reference to draft article 10, which is intended to set a minimum standard from which certification authorities should not be allowed to derogate (see above, para. 58). The second exception is inspired by the UNIDROIT Principles on International Commercial Contracts (Article 7.1.6), as an attempt to provide a uniform standard for assessing the general acceptability of exemption clauses. It may be noted that the reference to the limitation or exemption of liability being "grossly unfair" suggests a flexible approach to exemption clauses. That approach may lead to broader recognition of limitation and exemption clauses than would otherwise be the case if the Uniform Rules were to refer merely to the law applicable outside the Uniform Rules.

65. Paragraph (3) deals with the situation where loss or other damage would result from intentional misconduct by the certification authority or its agents. The substance of the suggested rule is inspired by similar wording used in many international transport conventions, and recently used in article 18 of the UNCITRAL Model Law on International Credit Transfers.

Article 12. Liability of the certification authority to parties relying on certificates

(1) In the absence of a contrary agreement, a certification authority which issues a certificate is liable to any person who reasonably relies on the certificate for:

(a) [breach of warranty under article 10] [negligence in misrepresenting the correctness of the information stated in the certificate];

(b) registering revocation of a certificate promptly upon receipt of notice of revocation of a certificate; and

(c) [the consequences of not] [negligence in] following:

(i) any procedure set forth in the certification practice statement published by the certification authority; or

(ii) any procedure set forth in applicable law.

(2) Notwithstanding paragraph (1), a certification authority is not liable if it can demonstrate that the certification authority or its agents have taken all necessary measures to avoid errors in the certificate or that it was impossible for the certification authority or its agents to take such measures.

(3) Notwithstanding paragraph (1), a certification authority may, in the certificate [or otherwise], limit the purpose for which the certificate may be used. The certification authority shall not be held liable for damages arising from use of the certificate for any other purpose.

(4) Notwithstanding paragraph (1), a certification authority may, in the certificate [or otherwise], limit the value of transactions for which the certificate is valid. The certification authority shall not be held liable for damages in excess of that value limit.

References:

A/CN.9/437, paras. 51-73 (draft article H);
A/CN.9/WG.IV/WP.71, paras. 70-72.

Remarks

66. Draft article 12 is intended to reflect the view expressed at the previous session that the Uniform Rules should contain a rule establishing a rebuttable presumption of liability. Under such a rule, for example, in the event of erroneous identification of a person or erroneous attribution of a public key to a person, the certification authority would be held liable for the loss sustained by any injured party, unless the certification authority could demonstrate that it had done its best efforts to avoid the error. Such a liability scheme is intended to provide additional protection to any person using the service of a certification authority, without however imposing strict liability on the certification authority (see A/CN.9/437, para. 58).

67. In the context of the discussion regarding draft articles 10 to 12, the Working Group may wish to consider the question whether the liability of certification authorities should be subject to limits and how such limits could be established (see A/CN.9/437, paras. 63-67). At its previous session, various suggestions were discussed by the Working Group with regard to the possible methods for limiting the amount of the liability incurred by certification authorities. One possible approach would be to determine a fixed amount. Other suggested approaches would rely on a limitation of the liability by reference to a multiplier of the fee paid by the subscriber, a percentage of the transaction value or a percentage of the actual loss sustained by the injured party. It was pointed out, however, that the damage that might result from the acts of a certification authority was not easily quantifiable, so as to serve as an objective criterion for arriving at a fixed amount of liability. Also, the service rendered by a certification authority, and the fees it charged, often bore no relationship to the value of the transactions to which they related or to the damage that might be sustained by the parties (ibid., para. 66). As to the suggested comparison between the situation of a certification authority and that of a carrier under international conventions applicable to the transport of goods and the transport of passengers (ibid., para. 67), a preliminary review of those texts suggests that limits of liability are generally established by reference to a fixed amount (e.g., in the case of the transport of passengers), possibly in combination with a reference to the value of the goods being transported. That issue may need to be considered by the Working Group at a future session on the basis of further study by the Secretariat.

Article 13. Revocation of a certificate

(1) 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 the applicable certification practice statement or, in the absence of such policies and procedures, promptly upon:

(a) receiving a request for revocation by the holder identified in the certificate, and confirmation that the person requesting revocation is the [rightful] holder, or is an agent of the holder with authority to request the revocation;

(b) receiving reliable evidence of the holder's death if the holder is a natural person; or

(c) receiving reliable evidence that the holder has been dissolved or has ceased to exist, if the holder is a corporate entity.

(2) The holder of a certified key pair is under an obligation to revoke the corresponding certificate where the holder learns that the private key has been lost, compromised or is in danger of being misused in other respects. If the holder fails to revoke the certificate in such a situation, the holder is liable for any loss sustained by third parties having relied on the content of messages as a result of the holder's failure to undertake such revocation.

(3) Regardless of whether the holder listed in the certificate consents to the revocation, the certification authority that issued a certificate must revoke the certificate promptly upon acquiring knowledge that:

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

(b) the certification authority's private key or information system was compromised in a manner affecting the reliability of the certificate; or

(c) the holder's private key or information system was compromised.

(3) Upon effecting the revocation of a certificate under paragraph (3), the certification authority must notify the holder and relying parties in accordance with the policies and procedures governing notice of revocation specified in the applicable certification practice statement, or in the absence of such policies and procedures, promptly notify the holder and promptly publish notice of the revocation if the certificate was published, and otherwise disclose the fact of revocation upon inquiry by a relying party.

(4) [As between the holder and the certification authority,] the revocation is effective from the time when it is [received] [registered] by the certification authority.

[(5) As between the certification authority and any other relying party, the revocation is effective from the time it is [registered] [published] by the certification authority.]

References

A/CN.9/437, paras.125-139 (draft article F);
A/CN.9/WG.IV/WP.71, paras. 66-67.

Remarks

68. Draft article 13 is intended to reflect the various views expressed at the previous session of the Working Group by setting forth a default standard governing revocation of certificates. At all times, however, a certification authority can avoid the default standard by establishing procedures governing revocation in its certification practice statement, and following those procedures. As regards the time of effectiveness of a revocation, the Working Group may

wish to decide whether a distinction should be drawn between the situation of the holder and that of any other relying party (see A/CN.9/437, para. 130).

Article 14. Suspension of a certificate

During the operational period of a certificate, the certification authority that issued the certificate must suspend the certificate in accordance with the policies and procedures governing suspension specified in the applicable certification practice statement or, in the absence of such policies and procedures, promptly upon receiving a request to that effect by a person whom the certification authority reasonably believes to be the holder listed in the certificate or a person authorized to act on behalf of that holder.

References

A/CN.9/437, paras. 133-135 (draft article F).

Remarks

69. At its previous session, the Working Group decided that the Uniform Rules should contain a provision on suspension of certificates (see A/CN.9/437, paras. 133-134). As regards the time of effectiveness of a suspension, the Working Group may wish to decide whether provisions should be added along the lines of paragraphs (4) and (5) of draft article 13.

Article 15. Register of certificates

(1) Certification authorities shall keep a publicly accessible electronic register of certificates issued, indicating the time when any individual certificate expires or when it was suspended or revoked.

(2) The register shall be maintained by the certification authority

Variant A for at least [30] [10] [5] years

Variant B for ... *[the enacting State specifies the period during which the relevant information should be maintained in the register]*

after the date of revocation or expiry of the operational period of any certificate issued by that certification authority.

Variant C in accordance with the policies and procedures specified by the certification authority in the applicable certification practice statement.

References

A/CN.9/437, paras. 140-148 (draft article G);
A/CN.9/WG.IV/WP.71, para. 68-69.

Remarks

70. At the previous session, no objection of principle was raised to including in the Uniform Rules a provision on registration of certificates (see A/CN.9/437, para. 142). The proper maintenance of a widely accessible register (sometimes referred to as a "repository") featuring, in particular, a certificate revocation list (CRL) may be regarded as an important element in establishing the trustworthiness of digital signatures. When dealing with the ways in which such registers and CRLs should be maintained by certification authorities, the Working Group may wish to consider whether relying parties should be under an obligation to verify the status of the certificate by consulting the relevant register or CRL before they could rely on the validity of the certificate.

71. More generally, the Working Group may wish to discuss whether the Uniform Rules, in establishing minimum standards for the operation of certification authorities, should also deal with the rights and obligations of parties relying on certificates.

Article 16. Relations between parties relying on certificates and certification authorities

[(1) A certification authority is only allowed to request such information as is necessary to identify the user.

(2) Upon request, the certification authority shall deliver information about the following:

(a) the conditions under which the certificate may be used;

(b) the conditions associated with the use of digital signatures;

(c) the costs of using the services of the certification authority;

(d) the policy or practices of the certification authority with respect to the use, storage and communication of personal information;

(e) the technical requirements of the certification authority with respect to the communication equipment to be used by parties relying on certificates;

(f) the conditions under which warnings are given to parties relying on certificates by the certification authority in case of irregularities or faults in the functioning of the communication equipment;

(g) any limitation of the liability of the certification authority;

(h) any restrictions imposed by the certification authority on the use of the certificate;

(i) the conditions under which the holder is entitled to place restrictions on the use of the certificate.

(3) The information listed in paragraph (1) shall be delivered to the user before a final agreement of certification is concluded. That information may be delivered by the certification authority by way of a certification practice statement.

(4) Subject to a [one-month] notice, the user may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received by the certification authority.

(5) Subject to a [three-month] notice, the certification authority may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received.]

References

A/CN.9/437, paras. 149-150 (draft article J);
A/CN.9/WG.IV/WP.71, para. 76.

Remarks

72. At its previous session, the Working Group noted that the various elements listed in draft article 15 should be placed in square brackets, to be considered by the Working Group at a later stage (see A/CN.9/437, para. 150).

CHAPTER IV. RECOGNITION OF FOREIGN ELECTRONIC SIGNATURES

Article 17. Foreign certification authorities offering services under these Rules

Variant A

(1) Foreign [persons] [entities] may become locally established as certification authorities or may provide certification services from another country without a local establishment if they meet the same objective standards and follow the same procedures as domestic entities and persons that may become certification authorities.

(2) Variant X The rule stated in paragraph (1) does not apply to the following: [...].

Variant Y Exceptions to the rule stated in paragraph (1) may be made to the extent required by national security.

Variant B The ... *[the enacting State specifies the organ or authority competent to establish rules in connection with the approval of foreign certificates]* is authorized to approve foreign certificates and to lay down specific rules for such approval.

References

A/CN.9/437, paras. 74-89 (draft article I);
A/CN.9/WG.IV/WP.71, paras. 73-75.

Remarks

73. By allowing foreign entities to become established as certification authorities, draft article 17 merely states the principle that foreign entities should not be discriminated against, provided that they meet the standards set forth for domestic certification authorities. While that principle may be generally accepted, it may be of particular relevance to express it with respect to certification authorities, since certification authorities might be expected to operate without necessarily having a physical establishment or other place of business in the country in which they operate.

Article 18. Endorsement of foreign certificates by domestic certification authorities

Certificates issued by foreign certification authorities may be used for digital signatures on the same terms as certificates subject to these Rules if they are recognized by a certification authority operating under ... *[the law of the enacting State]*, and that certification authority guarantees, to the same extent as its own certificates, the correctness of the details of the certificate as well as the certificate being valid and in force.

References

A/CN.9/437, paras. 74-89 (draft article I);
A/CN.9/WG.IV/WP.71, paras. 73-75.

Remarks

74. Draft article 18 enables a domestic certification authority to guarantee, to the same extent as its own certificates, the correctness of the details of the foreign certificate, and to guarantee that the foreign certificate is valid and in force. It refers to the matters referred to as "cross-certification" at the previous session of the Working Group. Draft article 18 essentially contains a provision on the allocation of liability to the domestic certification authority in the event that the foreign certificate is found to be defective (see A/CN.9/437, paras. 77-78).

Article 19. Recognition of foreign certificates

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

(2) Signatures and records complying with the laws of another State relating to digital or other electronic signatures are recognized as legally equivalent to signatures and records complying with these Rules if the laws of the other State require a level of reliability at least equivalent to that required for such records and 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.]

(3) Digital signatures that are verified by reference to a certificate issued by a foreign certification authority shall be given effect [by courts and other finders of fact] if the certificate is as reliable as is appropriate for the purpose for which the certificate was issued, in light of all the circumstances.

(4) Notwithstanding the preceding paragraph, Government agencies may specify [by publication] that a particular certification authority, class of certification authorities or class of certificates must be used in connection with messages or signatures submitted to those agencies.

References

A/CN.9/437, paras. 74-89 (draft article I);
A/CN.9/WG.IV/WP.71, paras. 73-75.

Remarks

75. Draft article 19 refers to the matters referred to as "cross-border recognition" at the previous session of the Working Group (see A/CN.9/437, paras. 77-78). Paragraphs (1) and (2) deal with the ways in which the reliability of foreign certificates and signatures may be established in advance of any transaction being made (and any dispute having arisen as to the level of reliability of a signature). Paragraph (3) establishes the standard against which foreign signatures and certificates may be assessed in the absence of any prior determination of their reliability. Paragraph (4) preserves the right of Government agencies to determine the procedures to be used in communicating with them electronically.

* * *

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.