December 1999

Electronic signatures: are international uniform rules any nearer?

Jay Forder
Bond University, jay_forder@bond.edu.au

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Recommended Citation
Jay Forder. (1999) "Electronic signatures: are international uniform rules any nearer?".

Electronic signatures
Are international uniform rules any nearer?

by Jay Forder, Consultant Editor

Introduction
The Electronic Transactions Act 1999 was approved by Federal Parliament in November. The signature provision in the Act is based on article 7 of the UNCITRAL Model Law on Electronic Commerce. As noted in our February 1999 issue, it provides that a signature requirement is taken to have been met if, having regard to all the relevant circumstances at the time, it was reliable as was appropriate for the purposes for which the information was communicated.

One of the major criticisms is that this gives no guidance as to what might constitute a reliable method in the circumstances. In the absence of further legislation, this issue will have to be determined by the courts. The determination is likely to take place long after the signature was used. It seems clear that electronic commerce would be better served if, before entering the transaction, there was more certainty about what the law recognised as a satisfactory electronic signature. Given the global nature of electronic commerce, it would also be helpful if there was some international uniformity.

UNCITRAL recognises these criticisms and its Working Group on Electronic Commerce has been encouraged to develop appropriate rules. This note outlines the progress made by the Working Group at its thirty-fifth session in September this year. I have included the text of some of the draft provisions. This should give a good flavour of what the uniform rules might eventually look like.

Draft Uniform Rules
The Working Group has been considering 13 articles. Article 2 will contain definitions and consideration of it was postponed to a future meeting so that review of the substantive provisions could be completed first.

Article 1. Sphere of application
After minor changes to some terminology, it was agreed the draft to go forward to the next meeting would be:

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

It was also agreed that it should be made clear, as is done by a footnote in the Model Law, that nothing prevents an enacting state from extending the scope beyond commercial activity.

Article 3. Technology neutrality
The Working Group strongly supported the principle of technology neutrality. By the end of discussion on this article, the draft appears to be as follows:

"None of the provisions of these Rules shall be applied so as to exclude, restrict, or deprive of legal effect any method [of signature] that satisfies the requirements of article 6(2) of these Rules or otherwise meets the requirements of applicable law."

The original draft had referred to, "satisfying the requirements of article 7 of the Model Law". To maintain internal integrity in the Uniform Rules (so they can be adopted without also implementing the Model Law), this was changed to refer to draft article 6(2) - which will include the same criteria as article 7 of the Model Law.

Article 4. Interpretation
The draft is likely to contain a relatively non-contentious provision on interpretation along these lines:

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

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

Article 5. Variation by agreement
The Group considered a number of alternatives providing for freedom of contract or party autonomy. They noted the view that, "absence of regulation had greatly facilitated the development of electronic data interchange" and strongly supported the principle of freedom of contract. It was decided, however, to postpone the decision as to whether some of the Rules should be mandatory. The form of the draft to be considered at the next meeting is:

"These Rules may be derogated from or varied by agreement unless:
(a) these Rules provide otherwise;
(b) the law of the enacting State provides otherwise."

Article 6. Compliance with requirements for signature/Presumption of signing
This article represents the heart of the provisions. The aim is to establish some certainty about the legal effect of using electronic signatures. It is clear from the deliberations that there is still a long way to go before finality is reached. There was still debate about whether it would be useful to use the concept of an "enhanced electronic signature" to refer to a signature that satisfies certain criteria and is thus presumed to have legal effect or whether this can be achieved without having to define a new term. This has been left to future meetings.

There was general agreement that certainty should be achieved by a rebuttable presumption as to the legal effectiveness of the signature rather than a substantive rule. It was left to a future meeting to discuss possible rules implementing procedural requirements for rebutting the presumption. As to the criteria that would trigger the presumption, the Working Group had considerable difficulty. Apart from including the general provision in article 7 of the Model Law (which is now in sec 10 of our Federal Act), the Group considered a number of additional formulations of broad criteria.

It seems clear that electronic commerce would be better served if ... there was more certainty about what the law recognised as a satisfactory electronic signature.
For example, it considered requirements that the signature should be unique to the holder and the signer should have sole control of the signature creation device. Ultimately it decided these criteria did little to prove the method was reliable.

The Group recognised that it might be necessary to first decide on the level of reliability required to trigger the presumption and then consider how this level might be expressed. The Secretariat is to prepare revised drafts with variants to reflect a number of views and discussion is to be resumed at a future session.

**Article 7. Presumption of original**
The Working Group considered a draft article assuming a data message to be an original if a method was used which provided a reliable assurance as to the integrity of the information. After debate about whether it was necessary and how it should relate to the provisions in the Model Law, the Group agreed the draft should be kept as a possible article for future discussion.

**Article 8. Determination of enhanced electronic signature.**
Draft article 8 stated:

"(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."

Retention of this article was supported, although a number of alternative ways of expressing it will be considered further. An explanatory note is likely to be inserted, making it clear that an express determination under this article is not the only way for a signature to have legal effect.

**Article 9. Responsibilities of the signature holder**

There was broad support for an article clarifying the obligations of the signature holder. It appears the draft will be reformulated slightly for the next meeting and its main provisions are likely to be:

"(1) A signature holder shall:

(a) notify appropriate persons without undue delay if

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

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

... Exercise due care to avoid unauthorized use of its signature.

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

**Articles 10 & 11. Reliance on enhanced electronic signatures and certificates.**

These draft articles state that a person is not entitled to rely on an enhanced electronic signature of a certificate to the extent that it is not reasonable to do so. They set out factors to be taken into account when determining what is reasonable. For example, one factor is whether the relying party took appropriate steps to determine the reliability of the signature of the candidate.

Views were expressed for and against these articles. In the end, the Group decided they should be re-drafted to take account of some of the concerns expressed and considered further at a later meeting.

**Article 12. Responsibilities of an information certifier**

After clarifying or rejecting some provisions in the draft, the main provisions of article 12 are likely to take the following form:

"(1) An information certifier shall:

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

(b) exercise due diligence to ensure the accuracy and completeness of all material representations made by the information certifier that are relevant to the life-cycle of the certificate, or which are certified in the certificate;

(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 identified in the certificate holds [at the relevant time] the signature device referred to in the certificate;

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

(iv) 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) utilize trustworthy systems, procedures and human resources in performing its services."

Discussion of a suitable article dealing with the consequences of failure to meet these requirements was cut short due to lack of time. Two other points were flagged for future discussion: a rule setting out the minimum contents of a certificate and factors to be taken into account in deciding the trustworthiness of the certifiers' resources under (e).

**Article 13. Recognition of foreign certificates and signatures**

The Group considered a draft that attempted to ensure there was no discrimination between domestic and foreign information certifiers. The exact wording to go forward to the next meeting is still unclear, but it is likely to provide that if the laws or practices of foreign states regarding signatures or certifiers are as reliable as those of the enacting state, then the signatures or certificates are legally equivalent.

**Conclusions**

UNCITRAL's work on electronic commerce is to be welcomed. It is never easy to arrive at uniform rules satisfying the interests of all international players. Unfortunately, the Working Group appears to be struggling to come up with a suitable approach. The crucial provisions are still far from an appropriate final form.