香港律師會的信頭
Letterhead of THE LAW SOCIETY OF HONG KONG

Practitioners Affairs

Our Ref : PA0005/99/33739
Your Ref :
Direct Line :

10 November, 1999

Miss Salumi Chan
Legislative Council
Legislative Council Building
8 Jackson Road
Central, Hong Kong

Dear Miss Chan,

Re: Bills Committee on Electronic Transactions Bill

I refer to your letter dated 4 November 1999 and attach for your further action copy of the Law Society's submissions on the Bill.

Please note the Law Society's representatives will be :-

Mr. Marcus Bourget, and
Mr. Charles Man（文國權）

Yours sincerely,

Joyce Wong
Director of Practitioners Affairs
e-mail: dpa@hklawsoc.org.hk

Encl.

cc Mr. Marcus Bourget w/o encl.
Mr. Charles Man w/o encl.

THE LAW SOCIETY OF HONG KONG'S SUBMISSIONS ON THE ELECTRONIC TRANSACTIONS BILL

1. Citations

Electronic Transactions Bill ("the Bill")

"Canadian Model" - Uniform Electronic Commerce Act (Draft August 1999) by Uniform Law Conference of Canada.

"EU Model" - Proposal for a Directive of the European Parliament and of the Council on a common framework for electronic signatures (March 25, 1999).

"Singaporean Model" - Electronic Transactions Act 1998.

"UNCITRAL Model" - United Nations Model Law on Electronic Commerce, approved by the UN General Assembly November, 1996.

"US Federal Model" - draft Uniform Electronic Transactions Act presented for final approval to the National Conference of Commissioners on Uniform State Laws convened in Denver, Colorado for its 108th Annual Meeting (July 23-30, 1999).

"LCB" - HKSAR Legislative Council Brief on the Bill (ITBB/IT 107/4/4 (99) VIII).

2. Digital Signatures

One of the important aims of the Bill is to *"give electronic records and digital signatures used in electronic transactions the same legal status as that of their paper-based counterparts"*, the main reason being *"to promote the development of e-commence in Hong Kong"* (LCB, para 2).

Section 6 of the Bill provides:

> *"if a rule of law requires the signature of a person or provides for certain consequences if a document is not signed by a person, a digital signature of the person satisfies that rule of law but only if the digital signature is supported by a recognized certificate and is generated within the validity of that certificate."*

This means that a certificate issued by a recognized Certification Authority ('CA') must cover a digital signature before legal recognition will be accorded to that signature.

A signature can have many functions: to identify a person; evidence of an intention to authenticate a document; to associate a person with the contents of a particular document; to provide certainty of the involvement of a person with a document. The legislation should therefore embrace all electronic signatures and should not be limited solely to the recognition of digital signatures.

As the Bill appears to take a functional equivalent approach to the application of electronic means in place of traditional paper based commercial activities, S.6 of the Bill is overly restrictive in its approach. The intention of the clause was to encourage CAs to register their services with the Director which does not complement (para 10 of the LCB), the Government's overall objective to adopt a technologically neutral approach to the drafting of the Bill.

The UNCITRAL Model Law on Digital Signatures provides:

> *"(1) Where the law requires a signature of a person, that requirement is met in relation to a data message [the rough equivalent of electronic record as used in the Bill] if:*
>
> *(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message*
>
> *(b) that method is reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."*

This comprehensive approach has been followed in sections 7 & 8 of the Bill, and it is difficult to see why a distinction should be drawn on the use of digital signatures. The UNCITRAL clause focuses on two functional elements of a signature:

> *(a) to certify the author of a document; and*
> *(b) to signify his approval of the contents of the document.*

Section (b) establishes a flexible approach to the question of security and, while not debarring the use of recognized certificates, would seem a more appropriate method of allowing the market (with the assistance of legal precedent) to establish appropriate security measures to be taken depending on the purpose of the electronic record. It would also allow the contracting parties, by private agreement, to establish the level of security required, as well as providing the courts with the ability to look at the surrounding circumstances of any particular transaction.

In the Bureau's response to the Law Society's comments, it puts forward this reason for not adopting a more technologically neutral approach, namely:

> *"To date, electronic signature technology other than that based on digital signatures is still immature and there is a lack of a common standard in the market"*.

However, this explanation contradicts the spirit of a technologically neutral approach, and is at odds with the aim of not encouraging the development of technology in a particular direction. Our potential trading partners or competitors in North America, the European Union and Singapore have not adopted such a restrictive approach, and there is no indication of future plans to do so.

The Bill limits the security mechanism to that provided by a public key infrastructure (PKI) in Hong Kong to be operated by licensed/recognized Certification Authority.

To make PKI operative, a Certification Authority (whether or not recognized) must first verify the identity of the sender of the electronic message by asking him/her to submit proof of identity, usually and inevitably in paper form and to attend in person. This first stage of verification is not fool proof. e.g. Banks have opened accounts for fictitious customers who attended in person but used forged identification documents. The process becomes more complicated if the sender resides outside Hong Kong. A problem arises when the Certification Authority recognized by the Hong Kong Government operates on a world-wide basis to try and accommodate the first stage of the verification process. To rely on overseas agents would compromise the integrity of the whole system, as some countries simply may not have a licensed/recognized Certification Authority.

There has been discussion in the cryptography industry that the digital signature legislation based on the model proposed by Hong Kong imposes a business model that could not survive under the discipline of the market place (Legislating Market Winners by C. Bradford Biddle, biddlecb@cooley.com).

Given the nature of the industry and the unknown direction from which innovation may come and industry standards to be achieved, it would make more sense to adopt the approach of either the UNCITRAL model or Singaporean model, rather than the more restrictive wording in the Bill which may put Hong Kong "out of synch" with international developments and standards. The Bureau comments that further amendments to the Ordinance will be made when necessary, is not an efficient method of dealing with this issue.

To excel in international trade, Hong Kong must adopt proactive policies in relation to e-commence with its overseas trading partners. To opt for a "secure" path which has not been chosen by the majority of international players will probably result in failure and will not achieve the desired effect of igniting "the engine of future economic growth".

See Appendix 1 which contains an analysis of the policies adopted by: US, European Union, Canada and Singapore.

3. **Liability of a Certification Authority ('CA')**

Section 36

One of the major blocks to the promotion of e-commerce is the question of security. While the use of CAs as trusted third parties is an important step in securing business transactions over the net, the CAs themselves must maintain the highest possible security practices in order to preserve their own integrity. The Bill speaks of trustworthy systems as a technologically neutral expression to ensure that a particular CA uses appropriate mechanisms to secure its activities and this can be complemented by provisions in the Code of Practice to be issued by the Director.

However, of special importance is the preservation of the integrity of the private key of the CA. This issue is, to a large extent, separate from the use of trustworthy systems to be employed by the CA on a day to day basis. While day to day error-free operation may be an ideal, *if ultimately unrealistic goal*, the potential losses that could be incurred as a result of the loss of the CA's private key are considerable. e.g. A party who discovers the private key of a CA could produce an unlimited number of ostensibly valid but forged certificates.

Moreover, if a CA's private key was compromised and the corresponding public key revoked, all certificates issued by that CA would be invalid. All of the consumers who utilized that CA would be forced to obtain new certificates. While much would depend on the exact terms of the contractual relationship between the CA and the consumer it is likely that the CA will seek to exclude as much of its liability as possible. Additionally, the loss to the consumer may be insignificant when compared to the costs of seeking recourse against the CA, which may inhibit any action being taken against a CA in such circumstances.

However, if the idea is to promote e-commerce within the consumer (as well as business) sector such risk of loss should not be borne by the consumer, especially in circumstances where consumer expectation of a recognized CA may be far higher than that of an unrecognized CA. While strict liability for losses incurred by a recognized CA's loss of its private key may be too high, the standard of care should be stipulated in the Ordinance, and not the Code of Practice, which merely provides that such information should be kept in a trustworthy manner. Section 36 would not appear to deal with this issue at all.

4. Public Policy Concerns

Another area of concern is the issue of the distribution of financial responsibility should a recognized CA become insolvent or bankrupt. Should it be a requirement of recognition that suitable insurance be obtained to cover the anticipated liabilities of a recognized CA? If so, should the requirement be included in the Ordinance expressly, or simply be left to the discretion of the Director?

Also in circumstances where public officers are granted immunity from prosecution in the performance of their duties under the Ordinance, is it desirable that the Director should be given such a free hand in deciding the method and cost (if any) of any application on a case by case basis? It would be desirable to have strict uniformity in the application of procedures which do not rely, on the wide discretion of the Director.

The Law Society of Hong Kong
9 November 1999

Appendix 1:

Background note on Electronic Signatures, Digital Signatures, and Certification Authority in the US, EU, Singapore and Hong Kong

1. **"Digital Signature"**

The intended signatory of an electronic message/record first applies to a certification authority for a key pair consisting of a private key and a mathematically related public key. The private key is kept by the intended signatory for the creation of a digital signature to be attached to the electronic message/record. The public key is deposited with the certification authority, which is opened for inspection by the public; the recipient of the electronic message/record will use the public key to verify the digital signature and data integrity of the electronic message/record.

The certification authority checks the identification and takes any other steps necessary to assure itself that the intended signatory is indeed who he/she claims to be. The certification authority then issues a certificate attesting to the connection between the intended signatory and his/her public key.

A Digital signature is only one example of an electronic signature. Electronic signatures appear in a wide variety of forms with different security characteristics. As a general term, an electronic signature has no security characteristics. This concept will be used in the submission when referring to "electronic signature".

2. **US Federal Model**

The recently published draft Uniform Electronic Transactions Act (with prefatory and reporter's notes) prepared by the National Conference of Commissioners on Uniform State Laws adopted the minimalist approach, namely, the proposed statutory provisions are only salutary directives to assure that electronic signatures will be treated in the same manner, under existing law, as manual signatures and there will not be any legal protection for "secure" electronic signatures. The Committee considered it important to establish, to the greatest extent possible, the equivalency of electronic signatures and manual signatures. S.106 recognition provision states:

S.106. Legal Recognition of Electronic Records, Electronic signatures, and Electronic Contracts

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies the law.

(d) If a law requires a signature, or provides consequences in the absence of a signature, the law is satisfied with respect to an electronic record if the electronic record includes an electronic signature.

"Electronic signature" is liberally defined as "*an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.*" (Page 9)

As at 24 May 1999, only Missouri, Utah and Washington have enacted restrictive recognition legislations requiring electronic signatures to be digital signatures verified by a valid certificate issued by licensed/recognized Certification Authorities before they are recognised by law as hand signatures. The other U.S. states have not adopted such a restrictive approach.

3. EU Model

The European Commission, in its recently published *"Proposal for a Directive of the European Parliament and of the Council on a common framework for electronic signatures"* (March 25, 1999), endorsed the view that:

Para 7: ".... in order to stimulate the Community-wide provision of certification services over open networks, certification service providers should in general be free to offer their services without prior authorization; whereas prior authorization does not only mean any permission which requires the certification service provider concerned to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect."

Para 10: ".... the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorization of the service provider involved."

Based on the above principles, the European Commission proposed the adoption of the following directives (page 8):

Article 5
Legal effects

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

(a) satisfy the legal requirement of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies that requirement in relation to paper-based data, and

(b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that the signature is in electronic form, or is not based upon a qualified certificate, or is not based upon a qualified certificate issued by accredited certification service provider, or is not created by a secure signature creation device.

"Electronic signature" is liberally defined as *"data in electronic form attached to, or logically associated with, other electronic data and which serves as a method of authentication"*.

An earlier research report *"The Legal Aspects of Digital Signatures"* (October, 1998) prepared by the Interdisciplinary Centre for Law and Information Technology, Katholieke Universiteit Leuven, Faculty of Law, for DG XV-Internal Market and Financial Services of the European Commission, concluded that the German experience of introducing *"[security] standard through legislation doesn't necessarily lead to market acceptance" and that "as long as the market does not accept a standard, it remains useless"*.

4. Singaporean Model

The Singaporean Model basically adopts the UNCITRAL Model which recognizes electronic signatures as hand signatures without any security qualification as to what constitutes an electronic signature. Section 8 of the Electronic Transactions Act 1998 states:

> **Electronic signatures**
>
> *8.(1)Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.*
>
> *(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.*

"Electronic signature" is liberally defined in Section 2 as *"any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record."*

The Singapore Electronic Transactions Act only gives effect to a digital signature generated with a valid certificate as a secure electronic signature, namely, its authenticity and integrity are presumed unless the contrary is proved; an electronic signature per se suffices as a paper signature. The parties themselves enjoy the convenience and are free to rely on unqualified electronic signatures if they so wish with/without verification by licensed/unlicensed (or recognized/non-recognized) Certification Authority.

5. **Canada**

The Uniform Law Conference of Canada observed in the June 1999 draft of the Uniform Electronic Commerce Act that:

> *"questions of attributing a signature to a person are matters of fact to be proved separately, if they arise. Often attribution is not in doubt, only the "fact" of whether a signature is present."*

The proposed Canadian Model is similar to the Singaporean Model on which electronic signatures are recognised as hand signatures without any security qualification as to what constitutes an electronic signature.

33487