LC Paper No. CB(1) 382/99-00(04)

Electronic Transactions Bill
Bills Committee Meeting

12-Nov-1999

Presented by
Dr. C.K. Leung, committee member,
Information Technology Division, Hong Kong Institution of Engineers

On behalf of Information Technology Division, Hong Kong Institution of Engineers, I wish to thank the Chairman of this committee for promptly giving us feedback on our previous comments.

We welcome the Government's move towards enacting the Electronic Transactions Bill in order to support and cultivate electronic commerce, and hence to strengthen Hong Kong's position in international trading and commerce.

In our earlier comments, we have sought clarifications on issues related to: -

- Standards of Certification Authorities
- Interoperability of Different Certification Authorities
- Termination of CA Services
- Time of Transactions
- Use of Encryption
- Public and private Key Generation
- Exemption
- Government involvement, and
- Recognition of IT Professionals.

In the following, I would like to follow up some of them briefly.

On Standards for Certification Authority (CA) and Code of Practice

Recently, the Code of Practice has been published for public consultation. This is a detailed set of requirements for a CA who has already been recognized and is carrying out its functions as a recognized CA. Apparently there is not yet any standard against which a CA who applies for recognition can be measured or judged. We think that it is time that we had, in addition to the Code of Practice, a set of well defined**,** objective, and measurable criteria for the accreditation of CA who applies for recognition from DITS.

On Termination of CA Services

The Code of Practice requires the CA who terminates its business to archive its records for at least seven years. But the major problem is not whether the records have been archived or not, it is whether the terminated CA's public key, which has been used to sign its subscribers' certificates, is still verifiable or not. According to ETB clause 40, "the

Director must publish in the Gazette a list of the recognized repositories". According to Code of Practice 3.7.1, "a recognized CA shall publish in the recognized repositories maintained by it its certificate …..". From these we can see that a recognized CA will maintain its own recognized repository where its certificate is kept. If the CA terminates service, its recognized repository will not be maintained anymore. That will mean the recognized CA's certificate will not be available anymore. Even if some users have already download the CA's certificate for future use, since it is not mentioned who will sign the recognized CA's certificate, the downloaded certificate of the CA will be useless since it is not directly available from a recognized repository. All those certificates that have been signed by the CA cannot be verified. Records archival alone cannot solve this problem. The Government should provide more information on how this problem can be solved; otherwise subscriber's interest will not be protected.

On Encryption

We are happy to learn that Government takes a positive view towards encryption usage. But we are concerned that the Government "does not consider it appropriate to deal with encryption by law", as they tell us in their reply to our previous comments. In our opinion, confidentiality is at least as important as digital signature in electronic transactions. If the Government can spend so much effort in enacting a law to recognize digital signature, why not give the same level of consideration to encryption and confidentiality? Market force cannot play any role here since it is the legal status that matters, not cost effectiveness or any other business consideration.

On Public/Private Key Generation

Sections 3.3.2b and 3.3.4 of the Code of Practice clearly imply that a recognized CA will generate both the public key and the private key for a subscriber, and will keep records of them. It is unlikely that, under these codes of practice, a CA would accept a subscriber's submission of his/her own public key for registration. Probably the CA itself will generate the subscriber's key pairs. If the Government thinks it acceptable that a subscriber generates his/her own key pair and submits only the public key for recognition while keeping the private key as a truly private secret, this should be clearly indicated in the Code of Practice for the avoidance of doubt and possible dispute between recognized CAs and the subscribers.

- End of Brief Comments -