LC Paper No. CB(1)465/99-00(03)

Response to Further Comments made by the Hong Kong Institute of Engineers (IT Division)

On Standards for Certification Authority and Code of Practice

- The Director of Information Technology Services (the Director) will issue the code of practice for recognised certification authorities together with the associated guidelines after the enactment of the Electronic Transactions Bill. To follow up the comments received during the public consultation exercise on the draft code of practice, the Director is making arrangements to further consult relevant parties in the industry on the drawing up of additional guidelines to clarify the Director's requirements in relation to "trustworthy system", "generally accepted security principles", etc.

- It is our intention to consult the industry when the code of practice and the guidelines are amended in future. We shall make clear this intention when the second reading debate of the Electronic Transactions Bill resumes.

On Termination of Certification Authority Services

- We shall provide in the Electronic Transactions Bill that the Director must maintain for each recognised certification authority an on-line and publicly accessible certification authority disclosure record. The Director must publish in the record information regarding that certification authority relevant for the purposes of the Bill. We do not consider it necessary to explicitly list out in the Bill all the matters to be included in the record. However, we shall set out in the code of practice that a recognised certification authority has to deposit a copy of its public key in the certification authority disclosure record maintained for it by the Director. We consider this arrangement sufficient to ensure that there is a reliable means for verification of the recognised certificates issued previously by a recognised certification authority and of the digital signatures supported by these certificates.

On Encryption

- The definition of "electronic record" in the Electronic Transactions Bill does not draw a distinction between electronic records which are encrypted and those which are not. In other words, both kinds of electronic records will be given legal status so long as they satisfy the relevant requirements under the Bill.

- Clause 8(1)(b) of the Bill on the retention of information in electronic records refers to "the relevant electronic record is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received." If an electronic record is encrypted for retention purpose, it will still meet the requirement of the concerned rule of law if it is retained in a manner that can be demonstrated to represent accurately the information originally generated.

- If an electronic record is encrypted, the information contained in it is accessible so as to be usable for subsequent reference if it can be decrypted.

- The signing and encrypting of an electronic document are two different issues. "Digital signature" is clearly defined in the Electronic Transactions Bill. In relation to an electronic record, it means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine -

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

  (b) whether the initial electronic record has been altered since the transformation was generated.

  In layman's terms, this means that a person has to sign a document digitally with his private key in order to generate a digital signature and the verification of the digital signature shall be carried out using the signer's public key.

- We do not see the need to give separate legal recognition for encryption. Whether an electronic record is encrypted or not, it is an electronic record and its legal status is not affected by it being encrypted.

On Public/Private Key Generation

- The making and keeping of records of documents relating to the generation of a recognised certification authority's own and the subscribers' key pairs is distinctive from the making and keeping of the subscribers' key pairs including the private keys. Whether a recognised certification authority will keep records of both the public key and private key of subscribers is a matter of customer service between the certification authority and the subscribers.

- A recognised certification authority may use its system to generate both the public key and the private key for the subscribers on the latter's request. This is a matter of customer service between the certification authority and the subscribers. In such cases, the recognised certification authority must use a trustworthy system to generate the key pairs.

- We do not consider it appropriate to stipulate, whether in the Bill or in the code of practice, that a recognised certification authority must accept a public key submitted by a subscriber and issue a recognised certificate to the subscriber accordingly. The issue of a recognised certificate needs to be handled with care and we expect that a recognised certification authority would wish to satisfy itself that only if certain criteria (such as security measures) are met would they accept a public key submitted by a subscriber and issue a recognised certificate thereafter. The detailed requirements should be left to the certification authority. Indeed, the certification authority should be given the flexibility as to whether they should provide such service at all. The same applies to Hongkong Post as a recognised certification authority as well as to other recognised certification authorities.