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

On Standards for Certification Authority and Code of Practice

- We note the comments on the code of practice for recognised certification authorities. It is the intention of the Director of Information Technology Services to provide more detailed guidelines on the criteria for the recognition of certification authorities as well as the operation of recognised certification authorities.

On Termination of Certification Authority Services

- We note the comments on the termination of certification authority services. The Director of Information Technology Services will continue to maintain the certification authority disclosure record of the recognised certification authority after it has terminated its services. The disclosure record will contain the public key of the recognised certification authority which can be used to verify certificates previously issued by the recognised certification authority before its termination of services. It is also the intention of the Director of Information Technology Services to stipulate in the code of practice for recognised certification authorities that the termination plan of recognised certification authorities should cover not only the archiving of records but also the archiving of the public key of the recognised certification authority after its termination of service.

On Encryption

- We do not see a need to specifically provide encrypted documents with legal status. Whether certain data messages need to be encrypted, and if so the particular encryption technology to be used, is to be decided by the sender and the recipient. We do not consider it appropriate to deal with this matter by law.

On Public/Private Key Generation

- Section 3.3.2b of the draft code of practice for recognised certification authorities stipulates that a recognised certification authority shall make and keep in a trustworthy manner the records of documents relating to the generation of its own and the subscribers' key pairs, not the actual key pairs of the subscribers. Section 3.3.4 stipulates that a recognised certification authority shall provide a trustworthy system for the generation of its own and the subscribers' key pairs, e.g. the recognised certification authority may provide a trustworthy software for the subscriber to generate his own public/private keys. There is no mandatory requirement that the recognised certification authority must generate the private key for the subscribers.

- Whether a recognised certification authority should accept a subscriber's submission of his own public key for registration is a matter of commercial decision to be taken by the certification authority concerned, not by the Government. It is a matter for the clients to decide how their key pairs should be generated. There is no stipulation in the code of practice. We do not consider that there would be doubt or dispute over this matter between the reocgnised certification authority and the subscribers.