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

Standards for Certification Authorities

- Standards in respect of the operation of certification authorities are still evolving. We will closely monitor the development of industry standards in this regard and will incorporate them in the overall framework for granting recognition to certification authorities as appropriate. Given that such industry standards will refer to matters of technical details and will change over time in step with technological developments, we do not consider it appropriate to stipulate them in the Electronic Transactions Bill.

- The Director of Information Technology Services (DITS) will publish a code of practice for recognised certification authorities under Clause 39 of the Bill to set out the detailed requirements as regards standards and procedures for carrying out the functions of recognised certification authorities. We intend to specify in the code of practice the minimum qualification and experience required of the person who may seek the DITS's approval to audit the operation of recognised certification authorities. The DITS has published the draft code of practice for consultation. A copy of the draft has been sent to the Hong Kong Institute of Engineers for comment. We welcome specific comment in this area.

Interoperability of Different Certification Authorities

- It is up to the transacting parties to decide which certification authority provides the most suitable form of certification services (in terms of, for instance, the level of security of the key pairs issued, the reliance limits of the digital certificates, etc.) for the transaction in question having regard to the intended purpose of the transaction. As far as Government is concerned, we will not specify that our suppliers must use the service offered by a designated certification authority. But we would encourage our suppliers to use the service of recognised certification authorities, the trustworthiness of which have been verified by the Government in the recognition process.

- In the draft code of practice which the DITS has published for public consultation, we have set out the requirement that a recognised certification authority shall, where applicable, adopt an open and common interface to

facilitate the verification by others of digital signatures supported by the recognised certificates which it issues. The development of an open and common interface amongst recognised certification authorities will help to ensure their inter-operability.

- We shall also actively develop and establish cross recognition between HKSAR and other economies in respect of the operation of certification authorities so as to facilitate cross-border electronic transactions.

Termination of CA Services

- Under the draft code of practice for recognised certification authorities which the DITS has published for consultation, a recognised CA, in terminating its services, shall make arrangements for its records (including the certificates which it has issued) to be archived in a trustworthy manner for not less than seven years. Parties to an electronic transaction will have the means to verify past digital signatures supported by recognised certificates issued by the recognised certification authority concerned, even after the certification authority has terminated its services.

- A recognised certification authority intending to terminate its services is also required under the code of practice to advertise such intention in one English language daily newspaper and one Chinese language daily newspaper in Hong Kong for at least three consecutive days no later than 60 days before the termination of its services. This will enable the consumers to make necessary alternative arrangements ahead of the intended termination. The DITS will also announce the termination in the on-line and publicly accessible certification authority disclosure record maintained for that certification authority.

Time of Transactions

- We note the comment on the time of transactions. Clause 18 of the Electronic Transactions Bill contains provisions on the time of sending and receipt of electronic records. This will enhance certainty. As regards the time for electronic transactions to be made, there are various common law principles which should apply equally to conventional and electronic transactions.

- The parties to an electronic transaction may also agree their own arrangements as regards the time of transaction.

- Certification authorities, or other trusted third parties, are free to offer time stamping services.

Encryption

- It is our policy to establish a secure environment for the conduct of electronic transactions. The use of encryption technology will help to ensure the integrity and confidentiality of electronic communications. We welcome the development of encryption technology, but its use should be determined by the market. We do not consider it appropriate to deal with this by law.

- We welcome the opportunity for Hong Kong people to use various types of strong encryption techniques in electronic transactions. This will help to promote the development of electronic commerce in Hong Kong and enhance the confidence of the public in secure electronic transactions.

Public / Private Key Generation

- The generation of public/private key for a subscriber and the management of the key pair are commercial arrangements to be agreed between the certification authority and the subscriber. We do not consider that these arrangements should be stipulated by legislation.

Exemption

- Under Clause 11 of the Electronic Transactions Bill, the Secretary for Information Technology and Broadcasting may by order exclude application of Clauses 5 to 8 of the Bill to a rule of law. The order is subsidiary legislation by nature and is subject to the negative vetting procedure of the Legislative Council.

- It is our intention to review the exclusion list from time to time, taking into account developments in electronic commerce. We have adopted the subsidiary legislation format precisely to facilitate the review of the exclusion list in an efficient manner.

Government Involvement

- The Postmaster General is a recognised certification authority under the Electronic Transactions Bill. It is exempt from Part VII of the Bill on "Recognition of certification authorities and certificates by Director" which deals with procedures for seeking recognition and for the DITS to suspend and revoke recognition. Apart from this, the Postmaster General has to comply with other parts of the Bill in the same way as other recognised certification authorities.

- The Postmaster General, as a public authority, has a duty to abide by the laws of Hong Kong and the DITS has full confidence in discharging his obligations under the Bill.

Recognition of IT Professionals

- We note the views about the role that the members of the Hong Kong Institute of Engineers can play in enhancing security in electronic transactions.