Response to Comments
made by The Law Society of Hong Kong

Legal recognition of digital signature

- The primary aim of the Electronic Transactions Bill is to provide a certain and secure environment for the conduct of electronic transactions over open networks. Without certainty and security, electronic commerce will not be able to develop. Digital signature using public key infrastructure technology is currently the only form of electronic signature with a level of technical maturity that adequately meets the need for user authentication, integrity of data and non-repudiation of transactions. It is by far the most common form of electronic signature being used in the market which can address the issues of certainty and security.

- In considering whether we should give recognition to all forms of electronic signatures, we should look at the practical implications. If the Government and others in the community have no commonly available means to accept and deal with electronic signatures other than digital signatures, any move to recognise other forms of electronic signature would be premature.

- Recognition of other forms of electronic signature which have not yet reached a level of technical maturity to satisfactorily address identified security issues relating to electronic transactions would lead to uncertainty. Security breaches of any kind due to immaturity of the technology would substantially undermine the confidence of the public in participating in electronic commerce. This would impede the development of electronic commerce in Hong Kong.

- However, users of electronic commerce are free to accept various forms of electronic signature which suit their intended purposes. Recognition of electronic signatures other than digital signatures would be governed by common law.

- The adoption of digital signature is technologically neutral in the sense that digital signature is not based on particular types of algorithm products in the market. Moreover, it is up to the user to decide what level of security in respect of the digital certificate should be adopted to suit the intended purpose.

- Technological advances in electronic signature would be accommodated through suitable amendments to the Electronic Transactions Ordinance after its enactment. The concept of electronic signature is already written into the Electronic Transactions Bill as currently drafted. Legal recognition of new forms of electronic signature other than digital signature could be achieved, as and when appropriate, through an amendment to the Electronic Transactions Ordinance. The amendment involved is not envisaged to be complicated. We shall monitor closely developments in the area of electronic signature with a view to keeping our legal framework in step with technological advances in this area.

- It does not seem to be the case that jurisdictions presently considering electronic commerce legislation have moved away from giving legal recognition to digital signature only. The Electronic Transaction Law of Korea enacted earlier this year was based on digital signature. The Act on Digital Signature of Denmark currently in draft form also gives recognition only to digital signature.

- We note that the signature provision in the United Nations Commission on International Trade Law - Model Law on Electronic Commerce refers to a method to identify the signer and to indicate his approval of the information contained in the data message and that the method is reliable for the purpose for which the data message is generated or communicated in the light of all circumstances. It, therefore, means that only those electronic signatures, rather than all forms of electronic signature, which satisfy the requirement should be given legal recognition. We consider that for the time being only digital signature can fulfill the reliability requirement in order to address the needs of user authentication, data integrity and non-repudiation of transactions.

- We do not consider the two-tier approach adopted in the legislation of Singapore, which gives legal recognition to all forms of electronic signature at the first tier, would fulfill our requirement to provide for certainty and security in electronic transactions.

Liability of a certification authority

- Clause 31 of the Electronic Transactions Bill provides that recognised certification authorities shall use a trustworthy system in performing their services. The code of practice for recognised certification authorities will further stipulate that recognised certification authorities shall use a trustworthy system for generation of their own private keys and that they have to keep their own private keys and activation data in a trustworthy manner. There are thus adequate provisions to ensure that recognised certification authorities would keep their private keys in a safe and secure manner. Failure to comply with Clause 31 of the Bill or the code of practice may result in revocation of the recognition of the certification authorities.

Public policy concerns

- Clause 20(3)(b) of the Electronic Transactions Bill specifically provides that one of the main factors which the Director of Information Technology Services (DITS) shall take account of in granting recognition to certification authorities is whether arrangements are put in place by the applicant to cover any liability that may arise from its certification activities. The Director does not have the discretion not to consider this factor.

Other concerns

- To properly discharge the function as the recognition authority, the DITS has to be given some flexibility so that he can deal with applications for recognition as recognised certification authorities having regard to the specific circumstances and facts of each application. However, the DITS has to exercise such authority in a reasonable manner.