Response to Comments made by Mr Damien Wong

Technology Neutrality

- 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. Digital signature using public key infrastructure (PKI) technology is currently the only form of security technology with a level of technical maturity that adequately meets the need for user authentication, integrity and confidentiality of data and non-repudiation of transactions. It is also commonly available in the market and is based on open standards.

- The establishment of the public key infrastructure with the support of certification authorities as the trusted third parties in electronic transactions is also the common model adopted in other places in the world for providing a secure environment for the conduct of electronic commerce.

- The adoption of digital signature using PKI technology is technologically neutral in the sense that it is not based on particular types of algorithm products in the market. Moreover, it is up to individual certification authorities to decide what types of digital certificates should be issued and to individual users to decide what level of security in respect of digital certificates should be adopted to suit the intended purposes.

Crime Relating to Fake Key

- The primary purpose of the Electronic Transactions Bill is to promote the development of electronic commerce in Hong Kong, not to tackle computer crime in general.

- There are general provisions in existing legislation, e.g. the Theft Ordinance (Cap. 210), the Crimes Ordinance (Cap. 200) which deal with crimes concerning faking. The Security Bureau, law enforcement agencies and the Department of Justice are reviewing existing legislation to examine whether they need any updating to take account of technological developments in electronic transactions.

- Clause 31 of the Electronic Transactions Bill stipulates that a recognised certification authority must use a trustworthy system in performing its certification services, which cover the generation of the subscribers' key pairs. This will help to prevent the generation of fake keys by systems used by recognised certification authorities. For the reason stated in the first bullet, we do not consider it appropriate for the Bill to contain detailed rules and guidelines relating to prevention of fake key crime in general.

Classification of Electronic Transactions

- We consider that we should leave it to the transacting parties to decide on the appropriate level of security for their particular transaction having regard to its purpose. The implementation of the voluntary recognition scheme will encourage certification authorities to seek Government recognition and to use trustworthy system in providing their services. This will promote the availability of quality certification services and their popular use in Hong Kong. Over-regulation, which would be the case if Government were to stipulate in the Bill what security level or standard should be adopted for a particular industry or a particular type of transactions, would stifle the further development of electronic commerce in Hong Kong. From a practical point of view, such an approach would also be too inflexible to take account of developments in security technology.

Abuse, Misuse or Stealing of Private Key

- Whether an act is criminal or not is a question of fact, to be determined having regard to the circumstances of individual cases and the relevant provisions in law. For example, if the misuse or the stealing of the private key of another person amounts to dishonest appropriation of property belonging to another person with the intention of permanently depriving that person of the property, then pursuant to section 2 of the Theft Ordinance (Cap. 210), the person who misused or stole the private key has committed the crime of theft.