Response to the Paper submitted by the Office of the Privacy Commissioner for Personal Data

Public key directory

- It is a matter between the certification authority and its subscribers as to what information about the subscribers should be contained in the digital certificates to be issued and to be listed in the public directory of the certification authority. If a subscriber considers that the digital certificate of a certification authority will disclose his/her personal information which should remain private, the subscriber may choose not to use the service of that certification authority.

- As far as Hongkong Post is concerned, in its plan to provide the certification authority services, it will encrypt the identity card information of the subscribers on the digital certificate so that the identity card information will only be displayed in a "hash value" format in which a conversion back to the original form is not possible.

- It is the intention of the Director of Information Technology Services to stipulate in the code of practice for recognised certification authorities that the recognised certification authorities shall draw the clients' attention to the certification practice statement (CPS) associated with the certificates issued. The CPS shall highlight the personal information that would be displayed in the digital certificate for public inspection. The clients will, therefore, have a clear knowledge about the personal information to be displayed in the digital certificate before they accept the certificate.

Key recovery

- The Electronic Transactions Bill does not contain any provision which introduces a new third party lawful access to encrypted information or records by law enforcement agencies. Nor does the Bill create any new obligation under the Bill to provide access to information for law

enforcement purposes where such obligation does not already exist under other prevailing law.

Identity tracking

- While a digital certificate can be linked uniquely to the person to whom it has been issued, it can also be used to encrypt the information exchanged in electronic communication so that if the digital certificate is transmitted in electronic communication, it cannot be tracked. Other technological measures are also available to address the tracking of digital certificate in electronic transactions.