Information Paper
on 11 October 2002

Bills Committee of the Legislative Council
Registration of Persons (Amendment) Bill 2001

Comments by Mr. Lucas Hui, Centre for Information Security and Cryptography, HKU	**Administration's Response**
1. It is a basic principle in security design that the data stored in the IC chip should be kept minimal.	➢ Data stored in the chip will be kept to the minimum. Apart from the basic personal information shown on the card face, the only additional data to be held is the template of the card holder's two thumbprints. If the card holder is a non-permanent resident, the captured data will include relevant conditions of stays applicable to holder.
2. Any information that is stored in the IC chip, but that is not printed on the face of the card, must be protected by adequate access control (e.g. by a password) or by adequate encryption.	➢ The manner regarding the storage of data in the chip of the smart ID card is well defined and carefully controlled.
3. It is still advisable to protect the information stored in the IC chip which is also printed on the face of the card by either access control or encryption to prevent electronic copying of such data.	➢ Strict access control will be exercised to ensure that data in the chip can only be read by the card holder and authorized personnel. This is enforced by authenticating the card-receiving device using Security Access Modules (SAM) installed therein and authenticating a cardholder by verifying the cardholder's fingerprint against the template stored in the card. ➢ Sophisticated cryptographic technique will be used to protect the more sensitive data such as the thumbprint template and condition of stay.

Comments by Mr. Lucas Hui, Centre for Information Security and Cryptography, HKU	Administration's Response
4. To ensure that the card adopts currently acceptable security practice, the government should stipulate that the card is designed according to international smart card standards, such as the ISO 7816.	➢ The smart ID card complies with international smart card standards including ISO 7810, ISO 7816, ISO 10373 and ANSI 322. The combination of the Infineon chip and the MULTOS smart card operating system is certified to have attained the highest level of security – ITSEC E6.
5. It is important that all relevant government departments should implement clear and sufficient security policies to ensure that the confidentiality and privacy of data stored on the back-end computer servers are protected.	➢ Relevant regulations and guidelines, for example, the Security Regulations on Information Systems issued by the Security Bureau, are in place to ensure the confidentiality and privacy of data. All government departments must follow the regulations. Confidential data should be encrypted during storage in the back-end host computer and servers during storage and transmission through communication network. ➢ Controls are built in the application design so that only those officers who are authorised to handle such applications are allowed to access the corresponding data stored in the system. ➢ In addition, transaction logs and audit trails will be maintained to provide a trace on transactions performed and the officers involved.
6. To prevent attacks such as faking a card reader to steal information from the card, mutual authentication mechanism should be implemented in the new Smart ID card.	➢ Mutual authentication of card and card receiving device using the Secure Access Module will be implemented for the new smart ID

Comments by Mr. Lucas Hui, Centre for Information Security and Cryptography, HKU	Administration's Response
	card system. ➢ Authenticity of the cardholder is ensured by fingerprint matching upon access of personal data.
7. It is important to store only some selected fingerprint information in the Smart ID card from which it is technically impossible to reconstruct the fingerprint, and not to store the entire fingerprint.	➢ Only the two thumbprints (or if not possible, any other two fingerprints) of the card holder will be stored in the chip in the form of template which are mathematically generated digits and cannot be used to reconstruct the fingerprint image themselves.

Security Bureau
10 October 2002