Center for Information Security and Cryptography
Department of Computer Science and Information Systems
The University of Hong Kong
Pokfulam Road, Hong Kong. Tel: (852) 2857-8451 Fax: (852) 2559-8447
Email: cisc@csis.hku.hk Web site: http://www.csis.hku.hk/cisc

Clerk to Bills Committee on
Registration of Persons (Amendment) Bill 2001
Legislative Council Secretariat
3/F Citibank Tower
3 Garden Road
Central
Hong Kong

Re: Registration of Persons (Amendment) Bill 2001

Dear Sir or Madam,

As a response to your consultation document, “Public views sought on Registration of Persons (Amendment) Bill 2001”, I would like to submit, on behalf of the Center for Information Security and Cryptography (CISC) at The University of Hong Kong, our views on the proposed Hong Kong Smart ID card. As our Center is a research center on security technologies, our views are focused on the technical aspects of implementing the Smart ID card with multiple-applications capability, and not on the legal aspects thereof. Nonetheless we hope that by offering a technical perspective on the issues, we may facilitate a better understanding among the general public of the impact of the new ID card.

- A common concern about the new Smart ID card is the protection of confidentiality and privacy of the data stored in the IC chip of the card. It is a basic principle in security design that the data stored in such a chip should be kept minimal. 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 with state-of-the-art encryption technology. As for the information stored in the IC chip which is also printed on the face of the card, it is still advisable to protect it by either access control or encryption to prevent electronic copying of such data.
- There are two major security concerns as regards any smart card-based system. One is the physical security of the card. 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 and which the vendors should be able to comply with, such as the ISO 7816 series.
- Another concern is the protection of confidentiality and privacy of the data stored in the back-end computer servers, in relation to which the smart card will be used as an authentication device. Compared to the issue of physical security of the card as discussed above, this concern is even more important as it can be expected that such back-end computer servers will contain far more data about a citizen than the smart card. It is therefore important that all relevant

government departments should implement clear and sufficient security policies to ensure that the confidentiality and privacy of data stored on these back-end computer servers are protected.

- One advantage of using the Smart ID card is that the card is in fact a miniature computer, and so enables mutual authentication between the card and the card reading device. If this mutual authentication mechanism is correctly implemented, attacks such as faking a card reader to steal information from the card will be prevented. This feature should be implemented in the new Smart ID card.
- We understand that the Smart ID card will provide a function of fingerprint authentication. From the security point of view, it is important to store only some selected fingerprint information in the Smart ID card from which it is technically impossible to re-construct the fingerprint, and not to store the entire fingerprint. If the system is properly designed, effective and efficient fingerprint authentication can still be carried out using only selected fingerprint information.

These are the main concerns of us as a group of information security researchers. Please feel free to contact us if there are further questions.

Dated this 19th day of September, 2002.

Lucas Hui
Honorary Director
Center for Information Security and Cryptography
The University of Hong Kong