Information Paper
on 11 October 2002

LC Paper No. CB(1)48/02-03(02)

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

Comments by Professor Matthew Lee	Administration's Response
1. Citizens should be offered the option of loading digital certificates from other providers even though the first digital certificate is to be provided free by the Hongkong Post and automatically loaded onto the smart ID card. (paragraph 7)	➢ Given the consideration that there may be public unease towards commercially-owned applications stored on the smart ID card at the initial stage, we will allow only on-card applications provided by the Government initially. ➢ But this does not mean that we will exclude digital certificates issued by other Certification Authorities as a matter of policy. We will consider allowing digital certificates issued by recognised Certification Authorities other than HKPost to be embedded on smart ID cards should there be strong public support at a later stage.
2. Data (for the library card application) should be encrypted. Mutual authentication techniques should be employed. Indeed access security measure for data held in this compartment (the card face data compartment) of the smart ID card should not be any less than other data on the card. (paragraph 8)	➢ Only authorised parties (only LCSD at present) in possession of the relevant unlocking Secure Access Module (SAM) keys can read (and not write/update) the data in the card face data compartment. And the data will be encrypted during transmission. Hence there will be secure protection for the card face data and certainly not to a lesser extent than that for other data on the card. ➢ Agree that mutual authentication has to be successfully carried out

Comments by Professor Matthew Lee	**Administration's Response**
	between a smart ID card and the card-reading device before access to data is allowed. This is through the matching of SAM keys between the card and the device.
3. Citizens opting-out of the non-immigration uses should not be put in a more disadvantageous position. Those opting-in should enjoy more convenience. (paragraph 10)	➢ We confirm that the non-immigration applications are voluntary for citizens to choose. Citizens will be free to adopt these non-immigration uses or choose the existing means of service provision. But if they choose to adopt them, they can certainly enjoy more convenience, e.g. carry one less card.
4. The proposed amended Regulation 12 makes the unauthorized storage or tampering of data in the chip of a smart ID card an offence. To strengthen the intended deterrence effect, the unauthorized access to and use of such data should be made an offence too to deter a main a source of potential encroachment on privacy. The penalty proposed should be increased as far as possible to strengthen the intended deterrent effect. (paragraph 11)	➢ We have already included a new Section 11 to the ROP Ordinance so that any person who, without lawful authority or reasonable excuse, gains access to, stores, uses or discloses any particulars furnished to a registration officer shall be guilty of an offence under the ROP Ordinance. These particulars include data on the card face and the chip. ➢ The proposed penalty for any person who commits an offence under the new Section 11 shall be a fine at level 5 and imprisonment for 2 years. The penalty for this offence has already been set to the maximum level as stipulated in the proposed amended Section 7(3) of the ROP Ordinance.

Comments by Professor Matthew Lee	Administration's Response
5. Internal government databases should not be allowed to cross-linked. Once that prohibition is guaranteed, an application merely enabling more effective way of collecting and processing existing data for an existing purpose should have insignificant privacy impact and to demand PIA on such uses introduce unnecessary delay and waste public funds. The current proposed non-immigration uses fall into this category. (paragraph 12)	➢ Data on card for different applications will be segregated and only authorized parties can have access and there will be no sharing of database by Government departments. The latest (2nd) PIA study commissioned by ImmD has already addressed the loading of e-Cert on the smart ID card, the implementation of card face data compartment etc. The implementation of the non-immigration applications, which mostly represents an e-interface for existing services, observes the data protection principles and addresses the perceived privacy risks. Given these circumstances, we agree with Prof Lee that separate PIA on multi-applications is not necessary.

Security Bureau
10 October 2002