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

Comments by the Privacy Commissioner for Personal Data	Administration's Response
1. General – the implementation approach for the driving licence and library card applications has the advantage of minimising security risk from data concentration. (paragraph 6(a), first sub-paragraph)	- Agreed with PCO's comment. Indeed minimising the storage of application-specific data in the chip of the smart ID card will avoid the need for citizens to update such data stored in the chip and thus be more convenient for them to use the applications.
2. General - different entities (currently Police and LCSD) having access to and/or control of the identification data in the common compartment will create difficulty in protecting the privacy of such data. (paragraph 6(a), second sub-paragraph)	- The data in the card face data compartment will be loaded by ImmD and other authorised parties can only read (i.e. not write/update) the data. The data will be well protected so that only bodies authorized to be in possession of the relevant unlocking Secure Access Module (SAM) keys can gain access. The data cannot be updated or changed. And currently only LCSD will be authorised to access this compartment for the library card application and only after citizens have given consent for LCSD to do so. Police will only need to view the ID card number printed on the ID card (i.e. not using the chip) for the driving licence application. Police will not have access to data in the common compartment.
3. General - spell out more clearly in the ROP Ordinance the responsibility of ImmD on the security of data stored in the common compartment for shared access by different entities.	- The SMARTICS is designed to be privacy positive and ImmD is doing everything possible to protect the security of data. Data in the chip will be protected by means of cryptographic keys

Comments by the Privacy Commissioner for Personal Data	Administration's Response
(paragraph 6(a), third sub-paragraph)	while mutual authentication has to be successfully carried out between a smart ID card and the card-reading device before access to data is allowed. As described above access to the common compartment will be controlled by the distribution of SAM keys for authorised purposes only (currently only for library card application). Unauthorized persons will not have access to the card face data. Indeed the security consultant commissioned by ImmD has certified that the SMARTICS blueprint is a secure system in contemporary technology standard. - The ROP (Amendment) Bill does provide enhanced privacy protection measures e.g. unauthorised access to/use of data stored in the ID card will be made an offence. - At present, LCSD is the only department which will have access to the data in the common compartment. The proposed arrangement is that, when a person expresses his wish to use the smart ID card as a library card, he will have to complete an application form and give consent to LCSD to read and capture certain data items from the common compartment of the ID card chip, instead of keying in the data items into the library card system manually. This is to enhance efficiency and make full use of the smart element of the new ID card. LCSD is the data user and will be governed by the

Comments by the Privacy Commissioner for Personal Data	Administration's Response
	relevant legislation and code of practice in that respect. We do not think it is necessary to have this written into the ROP legislation.
4. e-Cert – inclusion of e-Cert into the smart ID card, which will be carried by the cardholder wherever he goes, may create unnecessary security risk in case of loss or impersonation unless security is re-inforced by additional safeguards e.g. biometrics. (paragraph 6(b))	- Access to and use of e-Cert on smart ID card will be protected by an e-Cert PIN. To enable cardholder to use the e-Cert stored in the smart ID card, the e-Cert PIN will be distributed, in a sealed PIN mailer, to the genuine cardholder upon presentation of his ID card as an identity proof to HKPost staff at the HKPost service counters at the New Identity Card Issuing Offices or designated Post Offices. Once the cardholder has reported loss of his e-Cert to HKPost, the e-Cert in question will be revoked and will no longer be valid for use. - Under the current system design of the SMARTICS, the only biometric data stored in the smart ID card is the template of the card holder's two thumbprints. The use of this template is currently limited only to immigration/ROP functions. We do not think it is necessary to extend the use of biometric data to the e-Cert because it is already protected by the e-Cert PIN which is known only to the person concerned.
5. Driving licence – no strong objection to using the smart ID card as a means to retrieve driving licence data, especially as it is citizens' choice to use the smart ID card for the driving licence	- The driving licence application is voluntary in the sense that citizens will be free to obtain/retain the paper driving licence.

Comments by the Privacy Commissioner for Personal Data	Administration's Response
application or to use the conventional driving licence. (paragraph 6(c))	
6. Library card – the use of smart ID card as library card may give rise to unjustified security risks. To ease public concern and to enable citizens to make an informed choice, it is important to explain clearly the implications involved. (paragraph 6(d))	- The use of smart ID card as library card is just an alternative means to accessing library services. Citizens will be free to use the existing library card to enjoy library services. Only certain card face data will be read from the smart ID card (including English name, Chinese name, date of birth and ID card number for the registration of new patrons; and ID card number and date of issue for the checking-out of library materials). These are data items appearing on the card face anyway. Access to the card face data compartment is controlled by the SAM keys distributed to authorized parties only. - In addition, data will only be read from patrons' smart ID cards after they have given their consent to use the smart ID card as a library card and patrons will be well informed of the implications involved. Adequate notices will be put up in libraries to explain this. Thus, we do not agree that there are unjustified security risks. - Libraries will launch wide publicity by putting up posters, issuing pamphlets, etc, to inform patrons of the free choice they have to use the smart ID card as a library card; and that specific card face data will be read from their smart ID card to enable this service if they have given consent.

Comments by the Privacy Commissioner for Personal Data	Administration's Response
7. Conclusion – citizens should be given a meaningful choice on the use of the smart ID card, accompanied by all the essential information to alleviate any unnecessary concern. (paragraph 9)	- Strongly support PCO's comment. It has always been our intention to roll out a comprehensive publicity and promotion programme nearer the ID card replacement exercise to ensure adequate communication to the public.
8 Clause 13 – spell out in the proposed Regulation 11A the precise circumstances under which a citizen may be compelled to provide his thumb or other fingerprint to a police officer, an officer of ImmD or an authorized person for verification of identity.	- The new Regulation 11A has already specified the one and only circumstances in which the fingerprint verification could be effected - namely, that only when a police officer, officer of the Immigration Department or an authorized person **has reason to doubt the identity of a person,** that the officer can require the person concerned to produce his identity card and scan his fingerprint for identity verification. This provision will make it clear that identity card checks cannot be conducted for other unrelated purposes. - We fully understand PCO's doubts as to whether other "authorized persons" should be given the same power as members of ImmD and the Police to inspect ID cards. Labour inspectors is an example of such authorized persons. Under section 17L of the Immigration Ordinance, a senior labour inspector or labour inspector has the authority to require an employee of the premises or places he entered to produce for inspection an identity card which the employee was required to carry under section 17C of the same

Comments by the Privacy Commissioner for Personal Data	Administration's Response
	Ordinance. The authority is given to labour inspectors for the purpose of law enforcement against the employment of illegal immigrants. - It remains our view that it is necessary to retain "authorized person" in the new Regulation 11A of the ROP Regulations so that in emergency situations (such as sudden massive influx of illegal immigrants from elsewhere), CE will have the flexibility to order other law enforcement agencies to perform ID card checks together with the staff of ImmD and the Police.
9. Clause 15 – To comply with the data protection Principle 1(1) of the PD(P)O, ImmD should review and provide justification for its need to keep such an extensive list and updated personal data of the citizen, particularly items like residence, place of business, employment are susceptible to change from time to time. Otherwise, ImmD should consider revising the reporting requirement under Regulation 18(1) to require citizens to report corrections of particulars to the Commissioner of Registration.	- We believe that for the purpose of Registration of Persons, it is necessary to require an applicant to furnish the particulars stipulated in Regulation 4 of the ROP Regulations and such particulars are not excessive. While items such as residence, place of business and employment are subject to change, the information is directly related to the person concerned and will be useful if there are doubts on the identity of a person who claims to be the rightful holder of the ID card. It can also help to trace the whereabouts of a person should this become necessary. - It is the legislative intent of Regulation 18(1) of the ROP Regulations for ID card holders to report correction of particulars. The onus must rest on the

Comments by the Privacy Commissioner for Personal Data	Administration's Response
	cardholders themselves as they are the ones who know which particulars have become incorrect. This is also in line with Principle 2 of Schedule 1 to the PD(P)O in that all practical steps should be taken to ensure the accuracy of personal data. - Admittedly, the penalty for not reporting correction of particulars has not been strictly enforced in the past. However, this should not be taken to mean that ID card holders do not have a duty to do so. For example, there are similar provisions in other legislation requiring members of the public to report changes of particulars even though the penalty clause has not been strictly enforced. More channels will be made available to the public (instead of attending the ROP office in person, they can also do so by post, fax or through the internet by using their e-cert) to facilitate them to fulfil their obligations of reporting changes.

Security Bureau
8 October 2002

Adm's Response to PCO.doc