Information Paper
on 11 October 2002

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

Comments by Hong Kong Institution of Engineers	**Administration's Response**
1. For smart ID card with multi purposes, the cardholders should have a discretionary choice on the optional applications on offer. (paragraph 3)	➢ Apart from immigration applications, cardholders will have the choice of whether or which additional applications they wish to include in their smart ID cards.
2. There is a possibility, no matter how remote, that some service providers may restrict services only through the smart ID card, thus restricting the user option. The implication of this should be studied. (paragraph 4)	➢ Apart from the immigration core application, there will be alternative measures for card holders to obtain the services of the other non-immigration applications (i.e. the driving licence, the library card, e-Cert and e-government services) without using their smart ID cards. We have no plan to launch any mandatory non-immigration applications.
3. Data protection measures (both technical and management) are essential to the success of the smart ID card, especially in a mixed environment of 'immigration' and 'non-immigration' applications. (paragraph 5)	➢ Under the SMARTICS, data protection measures (both technical and management) have been incorporated to enforce segregation of 'immigration' and 'non-immigration' applications. These measures include: ▪ Segregation of on-card data, functions, and applications are securely enforced by the MULTOS chip operating system

Comments by Hong Kong Institution of Engineers	Administration's Response
	▪ Mutual authentication of card and card receiving devices to guard against unauthorized access, storage, use or disclosure of data, using the Secure Access Module ▪ Access to ROP data requires authentication of the cardholder by fingerprint matching ▪ Access of e-Cert data requires the use of e-Cert PIN ▪ Inclusion of various privacy enhancing measures in the design of the SMARTICS e.g. - card holder can view the data in the chip - card holder has a voluntary choice of application download / deletion - card holder has a voluntary choice of submitting the data in chip electronically for government services - true compartmentalisation of application specific data
4. The success of a multi-application smart ID card depends on public support, which in turn depends largely on the comfort level of the public have on the proposed data	➢ We have been consulting the Privacy Commissioner for Personal Data and the Legislative Council since the announcement of the project in October 2000 and public

Comments by Hong Kong Institution of Engineers	Administration's Response
protection measures. It is essential that the Government is fully in tune with the public; this would mean collecting public opinions and establishing evidence of public consent and support. Some target performance levels, if explicitly stated, would provide further assurance to the public. (paragraphs 6 & 7)	opinions are collected during various stages of the SMARTICS project. They include:- ▪ Briefings to 18 District Councils from 26.10.2002 to 5.12.2002 to explain the smart ID card project ▪ 7 roving exhibitions at shopping malls and the Immigration Tower to explain to the public the new initiative and to collect their views on the issue in the month of November 2000 ▪ At a special meeting of the Panel of Security held on 11.11.2000, all the professionals and academics attending the meeting expressed clear support for the smart ID card project ▪ Open forums to the general public and focus group were arranged on 6.12.2000 and 6.1.2001. ▪ Promotion campaign in eight local universities and educational institution in February 2001 ▪ A 3-day exhibition at the 'Information Infrastructure Expo 2001' at the end of February 2001 ▪ A web site on the HKSAR Smart ID card with a dedicated e-mail address to collect comments /

Comments by Hong Kong Institution of Engineers	Administration's Response
	views from the public since November 2000. ➢ A special unit in the Smart Identity Card project team has been established to plan for the major publicity and education campaign together with the Information Services Department. Target performance levels are being developed and will be announced at a suitable time.
5. As some applications have already been identified (driving licence, digital certificate and library services), it may be appropriate to clearly spell out some of the key principles related to data protection, e.g. (a) the non-immigration and immigration application should not be linked in anyway, particular in accessing and modifying data stored in the card; and (b) a card holder should have the right and means to review data stored in card, and the provision to request records of change history. Thus, a cardholder can ascertain what data is stored in the card as well as when and who has modified the data. (paragraph 8)	➢ The Government fully recognizes that data privacy is a key issue that must be addressed most carefully. ➢ The content of an ID card is stipulated by Hong Kong law. No additional data can be included on the ID card (on the chip and on the card face) without undergoing examination by the LegCo. ➢ The suggestions made by HKIE have been catered for in the system design of the Smart Identity Card System to ensure that there will be no central database or linkage of database. ➢ Data security in chip will be enforced with the design of a highly secured public key

Comments by Hong Kong Institution of Engineers	Administration's Response
	infrastructure using the MULTOS Key Management Authority (KMA). Only authorized and valid data can be loaded into the chip of smart ID card through controls imposed by the secret keys generated from and managed by the KMA. ➢ For immigration applications, the data stored in chip (i.e. the card holder's personal information shown on card face, the template of his two thumbprints and for temporary resident, his condition of stay including limit of stay) can only be changed upon application submitted by the card holder. For viewing and updating data in chip, access will be permitted only if the card holder's live thumbprint matches the template stored in the chip. ➢ For non-immigration applications, currently only the e-Cert will have additional data (the e-Cert) in the chip. The embedding and subsequent renewal or removal of e-Cert is up to the voluntary choice of the cardholders. The use of the e-Cert embedded in the smart ID card and the viewing of the e-Cert data will be protected by an e-Cert PIN which will only be

Comments by Hong Kong Institution of Engineers	Administration's Response
	known to the card holders themselves. ➢ The card holders will be able to read the data in the chip at designated Immigration Department (ImmD) kiosks.
6. It is essential to establish a security management framework, e.g. to define the data owner, safeguards for employing contract staff in handling personal data, security certification requirements of the computer systems, management and work procedure. (paragraph 9)	➢ Agreed. These considerations have been taken into account in drawing up the tender requirements, designing the technical system, compiling the operating procedures and drafting the ROP (Amendment) Bill. Furthermore, in accordance with the standard practice, ImmD will consult the ICAC on the operating procedures to guard against any loophole. ➢ ImmD places strong emphasis on the security of data and the security of the computer system. For this purpose, a security expert has reviewed the system design and confirmed that the SMARTICS system is highly secure system by contemporary technology standard.
7. It may be necessary to provide a code of practice on the use and collection of fingerprint in order to avoid undue use and spreading of fingerprint information. It may be	➢ At present, the collection of thumbprint is governed by the ROP Ordinance. To cater for changes brought about by the smart element of the new ID card

Comments by Hong Kong Institution of Engineers	Administration's Response
necessary to consider making it an offence for anyone to retain fingerprint information (in image or encoded form) without the explicit consent of the fingerprint owner. (paragraph 10)	and revised work processes under the new ROP system, the Registration of Persons (Amendment) Bill 2001 was introduced to LegCo on 9-1-2002 with related clause 7 (New s. 11) (prohibition of unauthorised handling of particulars) added. Unauthorized access, use, storage and disclosure of ROP data, including the fingerprint information will be an offence subject to a fine at level 5 ($50,000) and imprisonment of 2 years.

Security Bureau
10 October 2002