Information Paper
on 11 October 2002

LC Paper No. CB(2)21/02-03(01)

Bills Committee of the Legislative Council

Registration of Persons (Amendment) Bill 2001

Comments by Professor Graham Greenleaf	Administration's Response
1. Proposed non-immigration uses not truly voluntary	
1.1 Driving Licence Function – - compulsory change to online licence	- The driving licence application, as with the other initial non-immigration applications, is voluntary for citizens to choose. Citizens will be free to apply and use the existing plastic licence. - In fact, for licence records stored in Transport Department (TD)'s backend computer system, there will be no change – such records are already in TD's backend system. The smart ID card allows citizens to use their e-Cert in a secure way to access their own driving licence records online in TD's backend system.
- comprehensive Police online checking is likely (ROP Reg.11 does not exempt holders of plastic licence)	- As for Police checking, it is already the current practice for Police to contact their call centre to check with TD's backend system where necessary. With the enhancement of TD's backend system by 2004 and Police's communications system by early 2006, Police will be able to check with TD's backend system direct when circumstances warranted. The information obtained by Police for traffic enforcement in future and circumstances for checking should be no different from (not more comprehensive than) the current practice.

Comments by Professor Graham Greenleaf	Administration's Response
1.2 HK Post e-cert - The "deep infrastructure" ITBB and HK Post are aiming for is a monopoly government provider of digital signature. Privacy dangers will be less if there are multiple providers.	- The smart ID card platform is for government applications initially as we recognize that there may be public unease towards commercially owned applications stored on the smart ID card at the initial stage. We will consider allowing digital certificates issued by recognised certification authorities (CAs) under the Electronic Transactions Ordinance (Cap. 553) other than HKPost to be embedded onto the smart ID card when there is strong public support. We have kept LegCo informed of this. - In fact, more issues on privacy protection would need to be studied if multiple providers of digital certificates could embed their certificates onto the smart ID card.
- If use of a digital signature is compulsory in other contexts (e.g. online change of address), this makes the obtaining of an e-cert only "pseudo voluntary".	- On the use of digital certificate, this is only required for some online government services requiring strong authentication or signature – and this requirement is to safeguard the citizen. It is untrue to say that getting an e-Cert on the smart card is only pseudo voluntary. e-Certs issued by HK Post and other CAs are available on other media. Citizens are also free to choose to obtain government services through conventional means (e.g. counter service). Thus the e-Cert application on smart ID card is voluntary as well as non-discriminatory.
1.3 Online Change of Address - Clearly no real choice here - only possible with HKPost e-cert as yet	- The online change of address applications on the Electronic Services Delivery (ESD) Scheme portal currently supports digital certificates issued by HK Post and enhancement work is at the final phase to support digital certificates

Comments by Professor Graham Greenleaf	Administration's Response
- If ROP Reg18, requiring updating of particulars, was enforced then this use would also become pseudo-voluntary, as convenience dictates use.	issued by another recognized CA - DigiSign. However, smart ID card is only one of the many media for storing e-Cert and doing e-transactions. Of course, there are other channels for change of address, e.g. postal, telephone. So, there does not exist the question of no choice. - Regulation 18 only requires an ID card holder to report corrections of particulars (e.g. change of address) to a Registration of Persons (ROP) office where such particulars have become incorrect or differ from those previously submitted to a registration officer. It does not, however, dictate the manner in which the report is to be made. Under the existing arrangement, an ID card holder can report his new address to a registration officer in person or by post. Upon the introduction of the smart ID card, we will provide an additional channel to the public who can use their e-Cert to report change of address electronically. These choices are voluntary and non-discriminatory. As long as these choices remain open, whether a person finds the online means more convenient will very much depend on his habit and level of computer literacy.
1.4 Library Card Function - There is no need for the ID number to be used. Library card number should be stored on a separate component on the card, providing the convenience of dispensing with a separate library card, without expanding the use of ID number into another information system.	- The library card application has been designed to use the ID card number as a matching key to the library card number, instead of storing the library card number in the chip of the smart ID card. This was to avoid the need to load a second application onto the ID card in order to reduce the cost of implementation and to reduce inconvenience to citizens if they lost their ID card. It would be very costly to maintain computer links between ImmD and LCSD for

Comments by Professor Graham Greenleaf	Administration's Response
	the loading of the library card number onto the chip and subsequent updating. Thus, if we had loaded the library card number onto the chip and the card was lost, the citizen would have to make a special trip to LCSD to get a new library card number loaded onto his card. Our implementation approach obviates the need both to maintain the computer link and for the citizen to visit LCSD if he/she loses his/her ID card. - If we were to store the library card number in the smart ID card, it would not be printed on the card face. It would then cause inconvenience to citizens as they have to either memorize the library card number or record it on a piece of paper so that they could make reference to it when using remote library services by telephone or through the Internet. - Citizens are free to continue applying for and using the existing plastic library cards. It is only an additional option that they can use their smart ID card as library card. .
2. Lack of Privacy Impact Assessments for non-immigration uses - ITBB should be required to provide a PIA for each proposed additional use of the ID card or number, and that the ROP Ordinance should be amended accordingly. - The terms of reference for the PIAs should require approval by LegCo.	- A separate PIA is not necessary as the 2nd PIA conducted by the ImmD on SMARTICS has already addressed the privacy aspects of the non-immigration applications, e.g. the PIA on SMARTICS has already looked into the reading and capturing of card face data stored in the chip of the ID card for library card application and the loading of e-Cert

Comments by Professor Graham Greenleaf	Administration's Response
	onto the ID card. - Moreover, the smart ID card only provides an additional option for the citizens – they can continue to obtain the services in the existing way, e.g. plastic library cards and driving licences will still be issued and HK Post will continue to issue e-Certs on floppy disks (or other media) and citizens can continue to notify the relevant government departments of their change of address via postal or other means. The smart ID card merely provides a platform and a medium for the non-immigration applications to ride on and the PIA on SMARTICS has already examined this aspect. - The implementation of the non-immigration applications has observed the data protection principles and addressed the perceived privacy risks. For example, citizens would be informed of what is stored in the card and how it would be used. Most importantly, the non-immigration applications will be voluntary at the choice of the citizens.
3. Dangers of Increased Use of ID Number by Private Sector - The smart ID card may dramatically increase the collection and retention of ID numbers and their use to link internal organizational data.	- The collection, retention and use of personal data, including the ID card number, is governed by the ROP Ordinance (Cap 177) and its Regulations, the Personal Data (Privacy) Ordinance [PD(P)O] (Cap. 486) and the guidelines stipulated in the Code of Practice on the Identity Card Number and Other Personal Identifiers (the Code) issued by the Privacy Commissioner for Personal Data. Regarding the use of ID card number by

Comments by Professor Graham Greenleaf	Administration's Response
- The card face data segment on the chip will be able to be accessed electronically by libraries and on a case by case basis for other functions that may be approved in future. The chip therefore has differential levels of security for different segments, making it very likely that electronic capture of "card face data" will proliferate, and therefore uses of the ID number.	private sector, the Code stipulates that unless authorized by law, no data user may compel an individual to provide his ID card number. The introduction of smart ID card will not allow the private sector to bypass these requirements. Furthermore, the smart ID card is at this stage open to government applications only and the private sector will not have access to data in the chip. Whilst we do not rule out the possibility of allowing commercial applications at some stage, this will be considered only if there is general public support and card holders will continue to have the free choice to decide whether or not they wish to reveal their ID card number to a private organisation. - Whether or not a Government department needs to read or capture the card face data electronically will be determined by the type of service requested by the card holder. The card holder's consent will also be required before the department is able to do so. - Technically, a smart ID card will not allow a card reading device to read the personal data in the chip unless it is satisfied that the card reading device is authorized to do so. Similarly, the card receiving device will not proceed to read the data in the chip unless it is satisfied that the ID card is valid. Through the use of cryptographic keys, this two-way authentication will ensure that only authorized government departments can gain access to the card face data. Therefore the "card face data" compartment will not lead to unnecessary increase in the collection and retention of ID card number through the "card face data" compartment. At the initial stage, only LCSD

Comments by Professor Graham Greenleaf	Administration's Response
	will be able to access this compartment for the library card application.
4. LegCo not being given Adequate Control over Expansion of this ID System 4.1 New uses can be added to the card/chip merely by amendment to Schedule 5 which does not require positive LegCo approval.	- There is no question of LegCo not being given adequate control over inclusion of new-applications that require storage of additional data to the smart ID card. Before any new non-immigration use is proposed for inclusion, the relevant LegCo Panels will be consulted, certainly before commencing the negative vetting procedures for amendments to Schedule 5. Besides, where the underlying legislation for the non-immigration applications has to be amended, separate legislative exercise is required. Subjecting amendments to Schedule 5 to negative vetting of LegCo will not deprive LegCo's scrutiny.
4.2 ROP database - The ROP data can be used as authorized by any Ordinance (new s9) – no positive LegCo approval (under s35 of the Interpretation and General Clauses Ordinance (IGCO)) needed but only disallowable by LegCo under IGCO s34.	- The purpose of the new section 9 is to impose restrictions on the use or disclosure of particulars collected under the ROP Ordinance to a few pre-defined circumstances and to make it an offence for unauthorized handling of particulars. One of the circumstances is that the use of ROP particulars must first and foremost be permitted or authorized by law. There is no such clear and unambiguous provision at present. Hence the inclusion of the new section 9 is privacy positive.

Comments by Professor Graham Greenleaf	Administration's Response
	- In future, if new legislation is to be enacted to extend the use of particulars to other departments which are not presently permitted to do so, LegCo approval will have to be sought.
- New forms of disclosure from the ROP database only require approval in writing from the CS (new s10), with no LegCo scrutiny at all.	- The new section 10 is not a new form of disclosure - this provision already appears in Regulation 24 of the existing ROP Regulations. We decide to move Regulation 24 from the subordinate legislation to the primary legislation because our Privacy Impact Assessment consultant recommends that we should raise its status. This can be seen as the second layer of protection on the privacy of ROP data, in addition to the PD(P)O.
4.3 Some new uses will not require any legislation - If no additional data on card, no Schedule 5 change needed - Driving licence and library applications only require amendments to other Regs by coincidence - Does online change of address use require legislation?	- Amendment to Schedule 5 will only be introduced when there is additional data to be stored. Where appropriate, the underlying legislation for the non-immigration applications will be amended. Applications have to be looked at individually as their nature may be different and they may be under a very different legislative framework e.g. the driving licence application requires amendment to the Road Traffic Ordinance (Cap. 374) to remove the requirement to carry a physical licence while driving for ID card holders. The library card application requires amendment to the Libraries Regulation (Cap. 132AL) to recognise the use of smart ID card as a library card. As for online change of address, this application does not require specific amendment to any legislation because the Electronic Transactions Ordinance (Cap. 553) already provides that, if a rule of law requires the signature of a

Comments by Professor Graham Greenleaf	Administration's Response
	person, a digital signature supported by a recognised certificate under the ETO of that person satisfies the requirement. - For the above reasons, we consider legislation is only required when there is additional data on chip or when changes to the underlying legislation are necessary.
- If only needs disclosure of ROP data, CS can authorize	- In authorizing any disclosure of ROP data, CS has given due regard to PD(P)O. This will continue to be the case in future.
- Should all uses require LegCo approval under IGCO s35?	- Non-immigration applications that involve amendment to the underlying legislation will require LegCo approval, and in the case where additional data are required to be stored in the chip, amendment to Schedule 5 will also be required. In both situation, the relevant LegCo Panels will be consulted and the proposed amendment has to be laid on the table of LegCo for scrutiny. The involvement of LegCo in all non-immigration applications will not be neglected.
4.4 Official card access - The use of card readers to do ID checks is open to any "authorized persons' approved by CE (new Reg11A), and there is explicitly no LegCo scrutiny of this (new Reg11A(4)).	- At present, only immigration and police officers have the power to check ID cards in the street. However, it is necessary to allow the Chief Executive the flexibility to order other "authorized persons" (law-enforcement officers) to perform the same task so that he can deal with emergency situations (such as massive influx of illegal immigrants from elsewhere) speedily and effectively. Similar provision can be found in section 17C(2)(c) of the

Comments by Professor Graham Greenleaf	Administration's Response
	Immigration Ordinance (Cap. 115).
5. Other queries	
5.1 Will non-officials be able to use readers? - No legal prohibition on others scanning the digital ID number from the card – technically possible?	- It is technically not possible for an unauthorized person to use his own reader to scan the ID card number in the chip because the reader cannot authenticate itself to the smart ID card. Under the new section 11 of the ROP Ordinance, unauthorized handling of particulars (including unlawful access, storage or disclosure of particulars) is an offence, which is liable to a fine at level 5 and to imprisonment for 2 years.
- Reg 11A allows private sector "authorized users"	- The intention of the new Regulation 11A is to make it clear that verification of fingerprints can be performed by immigration and police officers only if there are reasons to doubt the identity of an ID card holder. To cater for emergency situations (such as sudden influx of illegal immigrants from elsewhere), it is proposed to give CE the flexibility to order other "authorized persons" to do the job if the need arises. The term "authorized persons" is intended to mean law-enforcement officers. Private sector will not be given any such power.
- Scannable ID numbers could massively increase retention and internal use of ID numbers	- As mentioned in item 3 above, only authorized card reading devices with the appropriate cryptographic keys can read the personal data in the chip of the smart ID card. Any party intending to access the information must first obtain approval from the Government as well as the consent of the card holder. Again, the law, in particular the ROP Ordinance and its Regulations, PD(P)O and the

Comments by Professor Graham Greenleaf	Administration's Response
- Altering card content is prohibited, but not reading	Code of Practice on the Identity Card Number and Other Personal Identifiers, must be observed before collection, storage and/or use of personal data are effected. Unless authorized by law, no data user may compel an individual to provide his ID card number. - Government will employ state-of-the-art technology on data protection including measures at hardware, software and application levels to ensure that data in the chip cannot be read by unauthorized parties. In addition to the provision on prohibiting unauthorised alteration of card contents (the new regulation 12(1)A), we propose to include a new section 11 to the ROP Ordinance such that if a person gains access to the ROP data without lawful authority or reasonable excuse, he will commit an offence and be liable to a fine at level 5 and to imprisonment for 2 years.
5.2 Individual access - Can individuals use readers at home?	- It is possible for individuals to use smart card readers at home to read or use his e-Cert, by entering his e-Cert PIN for authentication of identity. Other than that, they will have to go to an immigration kiosk and use their thumbprint to view the data in the chip. Home use card readers cannot perform this function.

Comments by Professor Graham Greenleaf	Administration's Response
5.3 Protections - Protections are mainly aimed at misuse and security	- This is not correct. On top of the data privacy safeguards in the existing ROP Ordinance and PD(P)O, it is the objective of the ROP (Amendment) Bill 2001 to include new provisions to reinforce or supplement the data protection elements where they are needed. Typical examples are the new sections 9, 10 and 11 which are clearly privacy positive.
- There is no comprehensive legal regime for this ID system. It would be preferable if the ROP Ordinance was redrafted as a comprehensive code controlling all aspects of HK's ID system.	- In the course of preparing the ROP (Amendment) Bill, we have studied carefully the legal provisions in the existing ROP Ordinance and its Regulations, PD(P)O and Code of Practice on the Identity Card Number and Other Personal Identifiers. We have also considered the recommendations of the Privacy Impact Analysis consultant and the views of the Privacy Commissioner for Personal Data. Our view is that there is already a comprehensive legal regime for the ID card system. What we need to do is to build in new provisions to provide for the changes arising from the introduction of the smart ID card, the inclusion of non-immigration applications on the card, the launching of the region-wide ID card replacement exercise in 2003 and additional safeguards for better protection of data privacy. Before concluding the ROP amendment, we have submitted a few papers to the LegCo Panel on Security to explain its framework and coverage. Feedbacks from Members have been fully taken into account.

Comments by Professor Graham Greenleaf	Administration's Response
5.4 Multi-purpose cards raise the risks: cancellation of multiple rights possible, risks of identity theft may be higher, aggregation of separate personal data.	- We attach much weight to the security of the smart ID card. We have also committed publicly that different applications in the chip will be segregated and there will be no sharing of database between government departments. To ensure that the new smart ID card system (including the card itself) is able to meet the highest security standard, we have commissioned a security consultant to study the system design. The security consultant has certified that the latest SMARTICS Blueprint developed by the contractor, revised in accordance with his comments, is a secure system in contemporary technology standard.
5.5 ID card + chip + digital signature may become a "cyberspace passport": uses may become compulsory (by law or de facto)	- Not agreed. There is no linkage of database or sharing of data among government departments. On the other hand, the public has a genuine and non-discriminatory choice to decide whether they would like to include the non-immigration applications in their new ID card. These measures, as recommended by the Privacy Impact Assessment consultant, are to ensure that the hypothetical situation will not happen.
5.6 Caution in ID expansion is appropriate in HK - ID systems are an important element in the mechanisms by which States exercise control over populations. Expansions of ID systems carry a lower level of risk in fully democratic political systems, which have more checks and balances. Taking into account the fact that the PRC is not a democracy and nor is HK a full democracy, and that HK is considering enacting a security	- We are already taking a cautious approach in implementing the multi-application smart ID card. In the present case, the smart ID card will be used for limited purposes. While there is scope for more value-added applications to be included in the smart ID card, LegCo will be consulted. Inclusion of new applications in the chip will require legislative amendments and is subject to vetting by LegCo.

Comments by Professor Graham Greenleaf	Administration's Response
law the content of which could have major impact on the true meaning and implications of any ID card system, it seems appropriate for HK to take a very cautious approach to any proposals for the expanded uses of any ID system.	

Security Bureau
7 October 2002

response-Prof Greenleaf.doc