LC Paper No. CB(2)858/04-05(01)

For information

Panel on Security of the Legislative Council

Hong Kong Special Administrative Region (HKSAR) Identity (ID) Card Project: Progress Report

Purpose

This paper updates Members on the progress of the HKSAR ID Card Project.

Progress of the ID Card Replacement Exercise

2. The replacement exercise has been making good progress since its implementation in August 2003. Persons born in 1952 to 1957 are currently invited to apply for their ID cards during the third cycle of the replacement exercise which falls between 27 September 2004 and 12 March 2005. Up to the end of 2004, the Immigration Department (ImmD) has received 1.9 million applications for ID cards under the replacement exercise.

Smart ID Card Awards

3 The smart ID card is rated highly in terms of its comprehensive functions, security and creativity. The Smart ID Card Project received two more awards in 2004[1], including the Gold Award of the Application Category of the Sixth IT Excellence Awards by the Hong Kong Computer Society and the top prize in the category of e-Government & Service of the Asia Pacific Information and Communications Technology Awards.

[1] Hong Kong Smart ID Card Project was awarded the Card Technology Breakthrough Award in the implementation category by the Card Technology Magazine in April 2004.

The Fourth Privacy Impact Assessment

4. The Consultant has recently completed the fourth privacy impact assessment (PIA) which is the last of the four PIAs scheduled across the SMARTICS project lifecycle. The fourth PIA is an overall post-implementation review of data privacy protection relating to system controls, functionalities and manual procedures to ascertain that all privacy protection measures have been suitably implemented and are operating effectively in practice. The Consultant finds that ImmD is privacy conscious and has a strong commitment to addressing privacy issues and concerns arising from the SMARTICS project. ImmD has also been responsive in implementing the recommendations arising from the various PIAs. The Consultant also proposes a few final data protection measures which will assist ImmD to further enhance privacy protection in areas including manual procedures, system control, access security and handling of personal data.

5. A summary of the Consultant's findings and recommendations, as well as the Government's responses, is set out at **Annex**. We have discussed the findings of the fourth PIA report with the Privacy Commissioner for Personal Data ("the Privacy Commissioner") whose views, where applicable, are also set out at Annex. ImmD has already taken measures to comply with the Consultant's recommendations

Code of Practice and Privacy Compliance Audit

6. In consultation with the Privacy Commissioner, ImmD is preparing a Code of Practice which will set out the ground rules on the collection, use of and access to smart ID card data. It will form the basis of the privacy compliance audit of the Smart Identity Card System. The audit will be carried out after the Code of Practice has been endorsed by the Privacy Commissioner.

Security Bureau
14 February 2005

Annex

Fourth Privacy Impact Assessment
Summary of Recommendations

Item	Issues	4th PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
1.	The Hong Kong Government should continue to carefully manage the communication with the general public with respect to the Global PIN utility (which is not a user application of the ImmD) in the smart ID Card, if in future, the need to activate the Global PIN becomes necessary. (Disclosure and Policies)	We understand that there are in total, three "approved" user applications (i.e. applications which are relevant to the ID card holder) that can potentially be downloaded into the smart ID card during the card personalisation process. Specifically, these are the core ImmD application (mandatory), the card face data application (pre-loaded for voluntary non-ImmD use), and the optional e-Cert application from Hongkong Post. As discussed in the paper dated 4 July 2002 which was submitted to the Legislative Council Panel on Security, a Global PIN utility (which is also not an ImmD application) has been included in all smart ID cards. And as previously disclosed, this Global PIN function is a reserved capability in the chip. We understand that the HKSAR Government views the Global PIN as a utility to improve the future functionality of the card and not a standalone application. No personal information is kept within this utility. It has not yet been determined when the Global PIN will be activated, and should there be public demand or if useful applications or opportunities emerge in the future, the OGCIO of CITB has indicated that they would discuss with LegCo on this matter. Activation and use of the Global PIN function will be the voluntary choice of the card holders. If in the future, the activation of this utility is considered necessary, careful communication will be required to ensure that its use and purpose is clearly explained to the public so that no misconceptions will arise leading to privacy related concerns.	• There should be adequate legislative and system control over the activation and use of the function. • Adequate promotion and publicity should be maintained to enable the public to understand how the Global PIN works before activation and use of the function.	The Global PIN is only a reserved capability on the smart ID card. Although a Global PIN utility has been included into the smart ID cards, the PIN can only be activated when an actual application is identified and implemented in future. There is no plan to implement the PIN at this stage. If useful applications or opportunities emerge in the future requiring the implementation of this capability, OGCIO will consider all legislative, administrative and technical implications and consult the Office of the Privacy Commissioner for Personal Data and LegCo before implementation. There would also be adequate promotion and education to the public.

Item	Issues	4th PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
2.	Consider providing additional guidance and support to key ImmD staff who are responsible for reviewing key privacy related audit logs. (Manual Procedures)	The SMARTICS has been designed with many logging functions to track the usage of the system and to report any exceptional transactions/actions performed by users and that certain audit logs produced by the SMARTICS can be used to enhance privacy if used effectively. We understand that ImmD has been providing user training in the review of audit trail reports before and after the implementation of the SMARTICS. During our review and interview with various ImmD staff assigned with the responsibility to review and respond to log events, we noted from a few of them during our review that provision of additional training and support may strengthen the staff's awareness with respect to how audit logs are effectively reviewed as a privacy enhancing measure to ensure consistency amongst the different sections within the ImmD. One possibility would be to provide further guidance or support to staff involved with the audit trail review process (e.g through internal memorandums or short briefings, etc.).	-	Already complied. To provide further guidance on the review of audit logs, guidelines have been issued to section heads or officers in charge of the user sections/offices in May 2004. Individual section/office will also provide on-the-job training to staff members who are assigned to check the audit logs.

Item	Issues	4th PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
3.	Consider periodically reviewing the assignment of access rights of officers within the ImmD to ensure that assigned access rights are appropriate and not excessive. (Manual Procedures)	Whilst the SMARTICS controllers are responsible for setting up the initial user profiles of all ImmD staff, we understand that the section head or officer in charge of the user section/office has the capability of granting the approved access rights to an officer acting on his/her role (only in the same location office, e.g., Immigration Headquarters) while he/she is not in the section/office (only up to the rights they possess within their respective sections/locations). Whilst we also understand that the user section management is ultimately responsible for ensuring that access rights are appropriately granted to SMARTICS users within their own jurisdictions, there is risk that such 'borrower' rights maybe inappropriate or excessive if not promptly revoked following the authorised period of use as the granting of rights are conducted on operational need basis. We recognise that audit logs have been implemented and that the SMARTICS has an audit log report "Update Summary on User Maintenance Details" which tracks before and after images of all user access rights being changed. Currently, section heads would need to review individually, the access rights of each staff member on screen. However, periodic review (e.g., every quarter or half year) by an appropriate member (e.g., section head) of the staff in the section would further enhance the security and privacy of access of the SMARTICS and ensure that 'borrowed' rights are properly revoked following the authorised period of use. This process could possibly be conducted as part of a periodic privacy compliance review.	• The on-line review conducted by the section head or officer in charge should be well documented for future audit review purpose. • The on-line review should be conducted on a more regular basis given the sensitivity of the ROP data involved.	Already complied. The granting/deletion of an access right will be recorded in a register by the section head or officer in charge. In addition, on-line review of the user privilege will be regularly conducted by section head or officer in charge of the user section/office to ensure that user access rights are properly allotted and not excessive.

Item	Issues	4th PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
4.	Consider including relevant references within the Code of Practice on ROP Data in order to ensure that the data collected under the "remarks" field of SMARTICS is related to the application and is not excessive personal data. (Disclosure and Policies)	During our review of the SMARTICS, we noted that there is a "remarks" field associated with the ROP data of each ID card holder. The "remarks" field essentially provides ImmD users with the capability of including notes / additional information on each applicant throughout the card application process. We understand that this information is kept as part of the SMARTICS to assist with the card application process up to a maximum of only 80 characters. Currently we understand that the "remarks" field is not specifically used for recording personal data, and that pre-defined "remarks" in the form of a "pull down menu" has been designed by incorporating most of the information required for processing an application. However, users are still free to type in any information if needed. Whilst written manual procedures have been issued to ImmD staff on the input of the remarks field, it is difficult to explicitly define what would be considered appropriate / inappropriate information that can be recorded. The ImmD could consider including relevant reference within the Code of Practice on ROP Data to assist with clarifying to ImmD staff that no excessive personal data should be collected.	-	The "remarks" field is useful in the card application process to facilitate the input of additional information which is relevant to the application. Other than the internal guidelines issued to the staff in the use of "remarks" field, similar guidelines will also be incorporated in the Code of Practice on ROP Data, which is being drawn up, to ensure that only appropriate and relevant information will be collected and recorded in the SMARTICS.

Item	Issues	4th PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
5.	Enhancements to the SMARTICS which support the business processes of the Confidential Records Unit should be implemented as soon as practical. (System Controls and Access Security)	We understand that the SMARTICS will be implemented with a number of enhancements to improve the efficiency of tracking ROP Record requests within the Confidential Records Unit (CRU) of the ImmD. Currently, all requests are tracked in a separate database. The proposed enhancements will improve the logging of the requesting party (name and authorisation), the reason for the request and data provided into a single unified system. During our review, we understand that the SMARTICS enhancements were to be implemented in the first quarter of 2004, however, due to system performance considerations, the implementation will be delayed until later this year. Where possible, these enhancements should be implemented as soon as practical as the enhancements / controls will strengthen the existing privacy controls within CRU by ensuring that:- ▪ each time an enquiry is made in the SMARTICS and when ROP Records are disclosed, there is a corresponding request that has been properly authorised and logged within the same system, ▪ the CRU can efficiently obtain statistics on the disclosure of ROP records. *Note: This recommendation was addressed by the ImmD during the performance of the 4th PIA. The ImmD has implemented the necessary enhancements within SMARTICS in May 2004 and that the CRU is conducting all of their work within SMARTICS.*	-	Already complied. All the requests handled by the CRU are processed and recorded under the SMARTICS.

Item	Issues	4th PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
6.	Consider enhancing the SMARTICS workstations to ensure that ROP data cannot be stored in the local SMARTICS workstation. (System Controls and Access Security)	We understand that the Certificate Unit is responsible for providing to the public official certificates on registered particulars (ROP data), exemption certificates and the issuance of Consular Corps identity cards. The certificate is prepared on a SMARTICS workstation in the Certificate Unit using the SMARTICS to invoke a pre-defined Microsoft Word template. The ROP data are then manually inputted into the template and uploaded into the SMARTICS when completed. During our review, we noted that ImmD staff are able to save the completed templates (with personal data) onto the local hard disk drive using the " Save As" function. The risk is that ROP data can be potentially stored and accumulated on the SMARTICS workstation's hard disk drive. Whilst we understand that these workstations have been "hardened" so that the floppy drive and USB have been disabled to minimise the risk of information transmission, nonetheless, the ImmD should consider whether it was possible to disable this function so that data is not stored in the local hard disk drive of SMARTICS workstation. The risk is that there are no audit trails on ROP data stored on the local Workstation. *Note: This recommendation was addressed by the ImmD during the performance of the 4th PIA. In May 2004, the ImmD has disabled the "Save As" function such that no files can be saved in the local hard disk drive of the SMARTICS workstation.*	-	Already complied. The "Save As" function has been disabled.