LC Paper No. CB(2)2433/01-02(07)

For Discussion on
4 July 2002

Panel on Security of the Legislative Council

HKSAR Identity Card project – Latest developments and the Second Privacy Impact Assessment Report

INTRODUCTION

This paper updates Members on the latest development of the HKSAR ID Card project and reports the findings and recommendations of the second Privacy Impact Assessment (PIA) Report.

BACKGROUND

2. At the meeting on 9 April 2002, Members were informed that the conversion of historical microfilmed ID card and some old paper index cards into electronic image was progressing smoothly, that the System Analysis and Design of the new Smart Identity Card System (SMARTICS) had commenced, and that two consultancy studies (i.e. the second PIA and the SMARTICS Security Review) were on stream. We also consulted Members on the financial requirements of Phase 2 implementation of the project. The Finance Committee approved the funds for Phase 2 on 10 May 2002.

LATEST DEVELOPMENT

Record Conversion Exercise

3. The record conversion exercise is proceeding smoothly as planned. As at 22 June 2002, about 53% of the post-June 1987 ID card records have been successfully converted from microfilms to digital

images. We are confident that the record conversion exercise can be completed on schedule, i.e. records of ID cards issued on or after 1 July 1987 will be digitised before the roll-out of the new ID card in May 2003.

System Analysis, Design and Development

4. The System Analysis and Design was completed in late April 2002 as scheduled. The contractor has forthwith commenced the detailed program development activities, including prototyping and unit tests. We expect that the system development work will be completed in October/November 2002 and will be followed by user acceptance test of the system. Meanwhile, we are finalising the tenders for procurement of the Appointment System and Tag System. With the assistance of the Government Property Agency, we are also actively searching for suitable office space for setting up the nine New Identity Card Issuing Offices.

5. Following many rounds of discussion with the security consultant and data privacy consultant, the contractor of SMARTICS has revised the system design to take account of the recommendations made by the two consultants. We are satisfied that the latest system design has fully met the security and data privacy requirements in the tender.

Security Review

6. The security consultant has conducted a comprehensive study on the security regime of SMARTICS. It covers all aspects of the system including the network and communication, data, application, system access control, chip and card operating system, card acceptance devices, loading and deletion of on-card applications after issuance of cards, logical security, physical security, adopted design principles, and security and risk management. The contractor has taken on board the recommendations and the security consultant has certified that the latest SMARTICS blueprint developed by the contractor is a secure system by contemporary technology standard.

SECOND PRIVACY IMPACT ASSESSMENT

7. The second PIA report includes an overview of SMARTICS and an assessment on how the technical design has addressed the key data privacy recommendations in the first PIA report. The report recognizes that a number of key controls have been built into SMARTICS that address potential risks identified in the first PIA. Details are at Annex I. In respect of key design differences arising from technology limitation or business reasons (e.g. owing to memory and processing speed limitations, fingerprint comparison cannot be ideally performed by the processor on the card as recommended by the first PIA report), appropriate compensating controls are recommended to mitigate data privacy risks. The report further highlights certain areas in the system design that may give rise to privacy concerns and advises how these concerns should be addressed. Lastly, the report proposes the inclusion of a few data protection measures in the manual procedures. Overall speaking, the data privacy consultant considers that the contractor of SMARTICS has acquired a good understanding of the privacy issues and has adopted suitable data protection measures to safeguard the privacy of personal data.

8. A chart summarizing the recommendations of the second PIA report is at Annex II. An update on the status of the recommendations in the first PIA report is at Annex III. We have distributed the second PIA report and the two annexes to the Privacy Commissioner for Personal Data and discussed the summary of recommendations with him. His views, as well as the Government’s response, have been incorporated into Annex II.

Security Bureau
27 June 2002

Annex I

How SMARTICS addresses key data privacy risks raised in the first PIA

Privacy Risk	Controls to mitigate privacy risk
The card might be used to store data that is unknown to the person	• Cardholders are informed of the personal data stored by the ImmD application on their Smart ID card. A cardholder can view their personal data stored in the ImmD application using self-service kiosks as well as other non-ImmD data (presently the e-Cert.) • Installation and use of non-ImmD applications are at the discretion of ID cardholders. Users must authorise the installation of additional non-ImmD applications on the card. • 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 legislative amendment.
The card might be used to disclose data in a manner that is unknown to the person	• The manner in which data stored on the card is disclosed is well defined and carefully controlled. Steps will be taken to ensure that users are educated about the information stored within the ImmD application on the ID card. Important controls include: (a) The card authenticates the terminal upon insertion into the card reader; (b) The card authorises the terminal prior to disclosing stored and protected personal information; (c) The card will authenticate the terminal device using Secure Access Module (SAM) installed in the smart card terminal prior to releasing stored personal information; and (d) The cardholder is authenticated by verifying a cardholder's fingerprint against the template stored in the card.
The card might be used to perform functions that are unknown to the person	• Installation and use of non-ImmD applications is at the discretion of cardholders. User authorisation for non-ImmD applications on the card is required. • For ImmD kiosks, Limits of stay (LOS)/Conditions of Stay (COS) fields on the Smart ID cards are updated for cardholders if necessary. The updated LOS/COS will be displayed to cardholders via the kiosk. • Card users will be informed about the functions that the smart card provides.
A private key might be compromised	• Encryption keys for ImmD applications are generated in a carefully controlled environment and securely injected onto the card. • Once on the card, the sensitive encryption keys do not leave the card so there is little risk of key compromise. • ID card keys are unique per card. The encryption keys of only one card would be affected if the card key were to be compromised. A compromised encryption key would not allow an attacker to capture the keys of all other IDs within the SMARTICS system.
A private key could be invoked by a person	• Once the private keys are injected and stored securely in the protected memory of the smart card, these keys are not accessible directly by any application. Instead, the application can request the built-in crypto-engine inside the smart card to perform cryptographic functions by using pointers to these keys.
Interception of traffic of data	• During transmission between the smart card and the backend systems, all data messages are encrypted and the integrity is protected by a unique sequence number and message authentication code (MAC) within that session of transmission.

How SMARTICS addresses key data privacy risks raised in the first PIA

Privacy Risk	Controls to mitigate privacy risk
	• Network encryption is used to protect the confidentiality of data as it is sent over the network.
The recorded biometrics may be captured by others	• Cards and card reading devices must be mutually authenticated before data (including biometric data) can be read. • Biometric data stored in the Registration of Persons (ROP) servers are subject to access controls and firewalls at the network and application levels. • Fingerprint images will be encrypted before they are stored in the Image Management System (IMS). Fingerprint templates on the Smart ID cards are protected by the mutual authentication between the card and card-receiving device. • The network is protected at the IPsec level using a Public Key Infrastructure ("PKI") based mechanism. • The cards themselves store mathematically generated fingerprint templates, not the actual fingerprint images. It would not be possible to re-generate the fingerprint image itself based only on the information in the card.
The recorded biometrics being obtained illicitly and used by impostors to masquerade as an individual	• At the kiosk level, verification of "live" fingerprints against the fingerprint templates stored on the ID card is required before sensitive functions can be performed on the cards. Kiosks will check the liveliness of the finger. • Kiosks are designed to be tamper resistant. The kiosk memory will be erased (1) when the cover is open, or (2) when the vibration sensors detect a vibration (pre-defined) thereby minimising the possibility that an unauthorised fingerprint reader can be installed. • The entire set of recorded biometrics is stored within the ROP database. The biometric information is protected using access controls as well as encryption. Unique encryption keys will be used for encrypting each biometric image.
Masquerade use of unsupervised devices by impostors who acquire the card and necessary knowledge	• Terminal devices (both self-service kiosks and off-line handheld) are not active until authorised personnel at the SMARTICS central site enables them using mutual authentication. The devices must receive the necessary activation commands through secured channels. • The card authenticates the terminal prior to sending sensitive data stored on the card. An unauthorised terminal would not be successfully authenticated and therefore sensitive data would not be disclosed.
The card data being amended by unauthorised devices	• The smart card does not allow an external terminal device to change its content without proper mutual authentication between the terminal device and the smart card and mutual authentication between the smart card and the backend systems. Therefore, end-to-end authorisation is required to update card data. • The 'smart chip' in each smart card is a tamper-proof device. There are layers of active shielding whereby sensitive data (e.g. key materials) is erased when it is tampered with mechanically, optically, electrically or electronically.

Annex II

Second Privacy Impact Assessment
Summary of Recommendations

A. Concerns arising from the Design of SMARTICS

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
1.	Design of access controls and user profiles in relation to the SMARTICS applications and functions. (System Design & Controls)	Access rights to the SMARTICS system should be granted based on a "need-to-know" basis and in accordance with the user's job roles and responsibilities. User access level mapping should ensure that an appropriate segregation of duties is maintained when user profiles are assigned to the users. Access to the SMARTICS system should be documented. Segregation should have a wide coverage to include, but not be limited to, the Registration of Persons (ROP) and Card Personalisation and Management System (CPMS) functions.	--	Will comply.
2.	The new kiosks should ensure that the display panel limits the possibility of viewing personal identifiable information by unauthorised individuals. (System Design & Controls)	It would be privacy positive if the display of personal identifiable information in the kiosks is limited to the ID cardholder and if the physical display of personal information could be limited, as much as practicable, to only the cardholder. This could include various alternatives such as installing a polymer mask to limit the viewing angle of the LCD screen (similar to an ATM) or consider a physical design similar to a "voting booth" to limit the public display of personal information. Video surveillance cameras installed to monitor vandalism should not be set in a position where personal data or the keying of passwords/PINs could be viewed.	--	Will comply.

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
3.	Configuration controls of workstations (PC's) and users. (System Design & Controls)	A key requirement of the SMARTICS system design is to ensure key ROP information is kept confidential and not inappropriately disclosed to third parties. To help prevent the unauthorised disclosure of information, ImmD should: ▪ disable the "print screen" function for users who do not need that function; and ▪ disable the cut & paste functions to prevent copying of personal information on workstations not directly used for ROP purposes.	--	Will comply.
4.	Enquiries of personal information by other government departments. (System Design & Controls)	ROP information is disclosed to some government departments either through legislation, or with written permission from the Chief Secretary for Administration. It is important that the procedures and processes comply with relevant legislation, except where valid exemptions apply, including the six principles of the PD(P)O subsequent to the SMARTICS implementation.	--	Will comply.
5.	Changes to personal data stored/shown on the new Smart ID card since the first PIA. (System Design & Controls)	According to the Smart ID Card Feasibility Study Report dated 12 June 2000 and the SMARTICS tender (Tender Ref. PT/0316/2001), the following personal data fields were proposed to be removed from the Smart ID Card (both physical and logical card data): i. Date of Birth Verified Indicator ii. Issuing Office Code iii. Loss Count iv. Right of Abode Indicator	--	From the public's perspective, people find the three asterisks (***) symbol printed on the ID card important and useful. For example, ImmD uses the three asterisks on the ID card to indicate the cardholder's eligibility for HK Re-entry Permit which is a travel document valid for entering the Macau SAR. The public also attach great importance to the Right of Abode indicator which they regard as concrete proof of their immigration status in Hong Kong.

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		vi. Eligibility for HK Re-Entry Permit The HKSAR Government has discussed the inclusion of the Right of Abode Indicator field and the Eligibility for HK Re-Entry Permit field at length and has concluded that it is in the best interest of Hong Kong ID cardholders to retain this information on the card. It appears that the business needs of the HKSAR Government outweigh the small level privacy concerns while the information is already contained in the current ID card.		Deletion of these two data fields will cause confusion and uncertainty to the public.
6.	Audit logs on the kiosk and handheld devices. (System Design & Controls)	Kiosk and handheld devices will have audit logging capabilities. The current design of the audit logs will contain each cardholder's ID number, the card's own serial number, date and time of the event and the operations performed. These audit logs will be passed to the backend system for storage. It appears that storing the cardholder's ID number is unnecessary and privacy invasive since the HK ID number and the card's own serial number are separately stored in the ROP database. To protect the privacy of the cardholder's ID number, ImmD should consider removing it from the logs. ImmD should also enforce strong access controls on audit logs kept within the kiosks and handheld devices. These controls should ensure that the audit logs are only accessible by authorised personnel on need basis. The third PIA should include a detailed review of the access controls enforced.	Consultant's recommendations are supported. Excessive storage of identity card number may induce operational problems in entertaining requests for access of personal records maintained by a government department.	Agree in principle. Will examine the feasibility and implications before system implementation.
7.	The ImmD should obtain undertakings from the SMARTICS Contractor to ensure that hidden "backdoor" program code or "hard-	ImmD should have the code thoroughly reviewed to obtain comfort that adequate processes are in place to ensure that quality and secure code is produced. These	--	Will comply.

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
	coded user IDs" have not been implemented into the system. (System Design & Controls)	processes may include: ▪ level I code review by developers ▪ formal code review by project teams ▪ informal walk-through/peer-to-peer code review by developers ▪ system functionality/usability/end-to-end reviews by Quality Assurance ▪ usability testing by end-users ImmD may also wish to gain comfort over the security of the code by checking, on a sample basis, that common security vulnerabilities do not appear in the code, and that the code is well documented. The SMARTICS contractor should implement detailed acceptance procedures at the system development stage. It may be appropriate to consider the legal implications of subverted code, and possibly, to ensure that appropriate wording or procedures have been included in the Code of Practice for the various contractors.		
8.	Use of the guardian ID in the ROP database. (System Design & Controls)	When a minor applies for an ID card, the ID card of their Parent/Guardian is temporarily stored in the 'Guardian Identity Card Prefix and number' field within the 'HKID Card' entity of the ROP system and will be purged after the application process has been completed. Long-term storage of this data field in a form that is electronically readable and searchable increases the risk of automated and widespread linkage of many parents to children. Inappropriate use of this information could result in establishing complex links between people. Using the parent's ID number in connection to a minor's ID card application for purposes other than originally intended (i.e. to allow a parent to pick up a minor's ID card) could be privacy invasive and against good privacy principles.	--	The 'Guardian Identity Card Prefix and Number' field will only be temporarily stored in the ROP database to facilitate confirmation of guardianship for registration and issue of minor's ID cards. The data will be deleted after issue of the minors' ID cards.

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		The ImmD should ensure that : - this Guardian ID field should not be stored longer than necessary or in a form that would allow easy and automated linkage of large number of minors to parents; and - there is a process in place to reliably remove the Guardian ID field from the ROP database. Alternatively, it could be stored in a transaction type record that is not searchable and is temporary in nature.		
9.	SMARTICS has been designed to support multiple government applications for other non-ImmD on-card applications via ImmD kiosks. (System Design & Controls)	Privacy concerns would be minimised if : - the IT infrastructure (e.g. network, kiosks) is only used for ImmD Smart ID card purposes; and - separate non-ImmD kiosks are used to access other future government department's applications. However, it would be logical for the ImmD to be responsible for managing the day-to-day IT operations and infrastructure related activities upon implementation of the SMARTICS when there are limited non-ImmD applications, namely the Hongkong Post digital certificate (e-Cert) and a library card application. When the number of non-ImmD applications increases and if the ImmD's is given the role as both "Card Issuer" and "Application Provider", there could potentially be operational and perceived privacy implications. The HKSAR Government may wish to consider setting up a facility, separate from the ImmD, to manage the day-to-day IT operations and infrastructure related activities for	Public perception is a difficult issue which needs to be carefully addressed. Publicity should be made to explain clearly the segregation of data/ applications and to reassure the public that only authorized departments will have access to their own set of data. It is appropriate to set up an independent facility to manage and control the non-ImmD applications when their number increases.	Under the proposed system design, immigration data and non-immigration data will be logically separated and compartmentalized. It will prevent ImmD from having access to the non-immigration data, and vice-versa. We agree with the consultant that the privacy concerns arising from the use of ImmD's IT infrastructure are more a matter of perception but would still need to be addressed. From the customer service point of view, cardholders will find it very inconvenient if they cannot read all the data at the ImmD kiosk and have to go elsewhere to read the non-immigration data. From the cost-effectiveness angle, it is not value-for-money for the Government to set up separate non-ImmD kiosks in various parts of the territory solely for reading the limited non-immigration data (viz 'e-Cert').

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		the non-ImmD applications. If this were considered a desirable option, appropriate data privacy and security controls and measures would also need to be implemented.		We note and agree with the report that there is no imminent need for the Administration to set up additional facility to manage the day-to-day IT operations and infrastructure related activities for the non-ImmD applications. The Government will nevertheless consider the recommendations when the number of non-ImmD applications increases in future.
10.	To facilitate data input, certain personal data on the face of the Smart ID card may be electronically read by various government departments. (System Design & Controls)	If the HKSAR Government wishes to facilitate the reading and capturing of data already displayed on the face of the Smart ID card to various authorised entities, the amount of personal data stored within the card face application should be limited to minimum. One possibility is to limit the data to the ID card number and English/Chinese name. If additional information, e.g. the Date of Birth and the Date of Registration, is needed, appropriate communications should be made to explain why this information is necessary to ease any privacy concerns citizens may have. The cardholder should also have full discretion as to whether card face data is to be provided to a particular authorised entity and to electronically copy his/her personal data from the card face application. This would include obtaining consent (e.g. via key strokes/mouse click/electronic signature, etc.) prior to copying information from the card face data application.	While the promotion of e-Government services is understood, the reading or capturing of card face data will leave an electronic trace (e.g. audit trail log) at the common ESD kiosk. To avoid the risk of profile tracing by a centralised controlling body, it is important that the audit trail log should be properly managed so that it will only be accessed and kept by the appropriate entity.	The Government considers that there is a genuine need to have the Card Face Data application to facilitate the provision of e-Government services-currently only the Library card function. It is important to note this is a voluntary application and citizens' consent will be obtained before any data is read. Citizens will be fully informed of the need to include these data items and their usage. On the Privacy Commissioner's comment about electronic trace, the card face data will only be read by smart card readers in public libraries (not ESD kiosks). However, the comment will be considered in implementing the library card function.
11.	The Limit of Stay date ("LOS") could expire between the date of ID	When ImmD prepares the operating procedure manual, steps should be included to ensure that the LOS has not	--	Will comply.

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
	card application and the date of issuance of the Smart ID card. (Procedures)	expired during the card issuance process.		
12.	The option of loading the Hongkong Post digital certificate into the Smart ID card. (Procedures)	Although the digital certificate from Hongkong Post is a non-ImmD application, there may be a public perception that the issuance of the digital certificates is part of the new HKSAR ID card re-registration and issuance process. Cardholders may confuse the nature of the applications / data stored in the Smart ID card and the roles of the various parties involved. ImmD and other departments/bureaux concerned should make a concerted effort to publicise the nature of the applications contained in the Smart ID card and the roles of the various parties. This will also help applicants understand why their personal data is separately provided to and validated by the Hongkong Post as well as ImmD. As part of the marketing and communication efforts surrounding the Smart ID Card, Hong Kong citizens should be made aware of the following: ▪ it is their choice to decide whether to include the Hongkong Post digital certificate in their Smart ID card; ▪ the associated benefits, purpose and use of the Hongkong Post digital certificate; and ▪ the requirement that their personal information will be provided to Hongkong Post upon their acceptance or "opt-in".	--	Publicity will be made to publicise the nature of applications available in the Smart ID card and the roles of the various parties prior to system implementation. Citizens will be informed of their choice, associated benefits, purpose and use of the Hongkong Post digital certificate through various means.
13.	Statement of purpose and collection of personal identifiable information.	Currently, several items in the purpose of collection section of the existing 'statement of purpose' printed on the ROP registration forms appear to be unclear and may		Agree in principle. Will consult the Department of Justice on the appropriate wordings of the 'statement of purpose' to

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
	(Disclosure/Policies)	need to be revised. They include :		be printed on the ROP registration forms.
		■ *Item 1(c)* 'to provide necessary information to the Registration and Electoral Office (REO) to update the electoral roll' is not clear. - As part of the process of reviewing all the application forms, the new form should reflect what personal information is provided to the REO.	The statement of purpose should merely explain why the data is collected and how it will be used.	
		■ *Item 1(e)* '…to assist in the enforcement of any other Ordinances and Regulations by other government departments through carrying out immigration control duties;' is not clear as a data user may collect personal data only for a purpose that is necessary for or directly related to a function or activity or the data user. - This item should be more specific and consider providing examples of the government departments that would use the personal data provided by the citizen in the ROP application form and for what purpose.	--	
		■ *Item 1(h)* 'any other legitimate purposes' in the purpose of collection section is arguably too open-ended to satisfy the requirement to inform the data subject of the purpose for which the data will be used. - It should consider to specify what 'legitimate purposes' means for purposes that are authorised under the ROP Ordinance or Hong Kong law.	Subject to the views of the Department of Justice, it would appear that the words "any other purposes authorised by law" can be used.	
		■ *Item 1(g)* 'for statistics and research purposes' is not clear.	--	

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		The PD(P)O s.62 provides an exemption from DPP3 (the use of personal data restriction principle) for statistics and research, but on condition that the results are not made available in a form, which identifies any data subjects. - The statistics and research use is at an aggregate level usually for the annual reporting purposes and does not include research uses which involve identification of individuals. As such, this item should be elaborated to include this fact.		
14.	Conduct a pre-implementation privacy review of the system controls and functionality prior to "go-live". (Going Forward)	Apart from the planned scope which focuses on the privacy aspects of the procedures that have been developed, the third PIA should be expanded to include reviewing the privacy aspects of: ▪ system controls and operations ▪ data retention periods of personal data (including temporary data files) ▪ any changes that have been made to the system design (including change control mechanism) ▪ any major deficiencies in system control and functionality that should be immediately addressed prior to go-live The third PIA should provide a comprehensive assessment of all major privacy enhancing system controls and functionalities that have actually been built-in to SMARTICS. The review should also help identify major areas in which privacy enhancements should be made before the system is released into production. A summary of the key results from the third PIA focusing on the review of manual procedures, system controls and	It is advisable to expand the scope of the 3rd PIA to include matters relating to data access requests made by the public.	The third PIA will likely be conducted in March 2003 before finalizing the operation procedures of identity card application. We will consider incorporating the recommended scope of study in the third PIA.

Item	Issues (Nature)	2nd PIA Consultant's Views/Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		functionalities should be made available to the public in order to enhance their confidence in the technology of the new Smart ID card system in terms of privacy.		
15.	Future user change requests to the SMARTICS System. (Going Forward)	An effective user change request process should be established as an integral part of enhancing, upgrading, and maintaining the SMARTICS system after its implementation. As users become increasingly familiar with the new system, they will likely request enhancements to be made. Accommodating multiple change requests concurrently may introduce new functionalities beyond the initial design of SMARTICS that may lead to new privacy issues. It is important that privacy considerations are taken into account prior to approval of any enhancements to the system. In particular, data protection principles of the PD(P)O as well as potential privacy concerns of Hong Kong Smart ID cardholders should be taken into account.	--	Will comply.

B. Concerns arising from the Recommendations of the First PIA

Item	Issues (Nature)	Comments of the 2nd PIA Consultant	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
1.	Both the first PIA and the PCO recommended that it would be highly desirable if the processor on the card were to perform the comparison of the fingerprint template so that the personal biometric information does not need to leave the Smart ID card. (Design Change from the 1st PIA)	It is understood that there are technical limitations with current smart card technology (memory and processing speed limitations) that fingerprint comparison cannot be ideally performed on the card. As such, inclusion of the following compensating controls in the SMARTICS design will minimise the risk of unauthorised capture of biometric information once it leaves the card : ▪ The card should authenticate the card-reading device prior to sending biometric information for further analysis. ▪ The card should ensure that the card-reading device is authorised to receive the biometric information stored on the card. ▪ The biometric information read from the card should not be exposed beyond the card reading device. ▪ Once the card reading device authenticates the user using the stored fingerprint template, all copies of the template should be immediately erased from the card reading device. ▪ Devices used for biometric authentication should be tamper proof to prevent the unauthorised capture of biometric information while inside the device.	--	The SMARTICS design has already included all the recommended compensating controls. We will revisit the issue when the technology on on-card comparison of fingerprints is viable.
2.	If the cards are to be capable of supporting cryptographic functions, then the card must perform secure key-generation, and provide secure key-storage and secure key usage for both	In general, if private keys are to be generated off the card and then loaded onto the card, adequate controls should be in place to ensure the secure generation of keys and to prevent the disclosure of keys as they are injected on the card. Sample key controls include : ▪ The keys generated should be random and not	--	The SMARTICS relies on MULTOS security. MULTOS has a Key Management Authority (KMA), which securely places applications and data onto the card using asymmetric cryptographic keys.

Item	Issues (Nature)	Comments of the 2nd PIA Consultant	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
	digital signature and message - encryption key-pairs. (Design Change from the 1st PIA)	predictable. ▪ Unauthorised physical and logical access to the systems used for key generation should be prohibited. ▪ Once key pairs are generated and the private key has been loaded onto the card, all copies of the private key (other than on the card itself) should be destroyed in such a way that there is no way to recover it. ▪ The communication channel between where the key is generated and the card upon which it is loaded must be secure. ▪ The key generation facility should be carefully managed. Application server configuration and maintenance should follow approved procedures. These include controls for host object integrity, system auditing, system queues, and file and directory access permission settings to prevent unauthorised access Cryptograph keys used by ImmD applications are securely generated when the card is initialised and that there is little need for ImmD to implement on-card key generation.		Symmetric cryptographic keys supporting the ImmD's applications are securely generated in the Key Management System (KMS) and injected onto the card during the card personalisation process. Cryptographic keys for Hongkong Post e-Cert application are securely generated by the Hongkong Post and transferred to SMARTICS for embedding onto the ID card during the card personalisation process.
3.	The first PIA recommended that the image for the fingerprint should be omitted from the ROP database to reduce privacy-invasiveness. (Design Change from the 1st PIA)	ImmD has a genuine business and operational need to capture fingerprint images and store them together with other personal information in a central ROP database. From a privacy perspective, the following key control should be in place to prevent inappropriate access to and/or use of this information : ▪ All users who access the ROP System must be	--	The recommended technical controls have already been included in the design of the SMARTICS.

Item	Issues (Nature)	Comments of the 2nd PIA Consultant	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
		authenticated. ▪ The ROP System should enforce multiple levels of access control to enable the ImmD staff at different levels of authority and with different job functions to access only the information that is necessary for them to do their jobs. Access to privacy sensitive fields such as the fingerprint image should be limited to individuals on a need-to-know basis. ▪ Detailed audit logs should be kept to indicate who has accessed what information, when and for what purpose. These logs should be reviewed periodically to check for appropriateness of the information accessed by users. ▪ All communication of sensitive information over the networks that could be subject to eavesdropping should be encrypted. ▪ Controls should be put in place to prevent the capture of ROP data for unauthorised purpose. The SMARTICS has included these controls within the design.		

Annex III

Status of the first PIA recommendations

We have included below a status update of the issues identified in the first PIA and the response from the HKSAR Government.

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
1	63 (Legislation)	The statutory framework for the Registration of Persons (ROP)/ID Card system should be reviewed to ensure that it provides a comprehensive basis for the HKSAR ID Card system as a whole.	Will review.	The ROP (Amendment) Bill 2001 was introduced to LegCo on 9-1-2002. The Bill provides for the introduction of the Smart ID card, the inclusion of non-ImmD application data on the card, the launching of the region-wide ID card replacement exercise, and additional safeguards for the better protection of data privacy.
2	64 (Principle)	If any additional applications or uses are considered for the HKSAR ID Card, they should ideally be voluntary at the entire discretion of the cardholder instead of making the choice of application merely on practical necessity.	Possibly with the only exception of the driving licence, cardholders will be free to choose whether to include additional applications in the Smart ID card. There is community acceptance to this approach, based on the outcome of the public consultation so far. Will discuss further with PCO and consult the views of the relevant LegCo Panels when the feasibility studies of other applications are completed.	All the non-immigration applications to be included in the Smart ID card (including the driving licence) are voluntary.
3	65 (Principle)	Privacy concerns would be lessened if ImmD retained in-house all aspects of the card scheme management and the possibility of the function being performed by any other government agency, or being outsourced, was expressly ruled out.	ImmD will definitely undertake the card registration and card issue functions. The Administration will ensure that all aspects of the card scheme management, including the management of other value-added applications, are secure and will protect the privacy of individuals.	The Commissioner of Registration will be responsible for the registration and issue of the smart ID card and the management of the ImmD applications. The e-Cert (presently the only non-ImmD application requiring storage of data on the ID card) will be managed by Hong Kong Post. The present design of SMARTICS will ensure secure segregation of data and data access by authorised entities only.

Annex III

Status of the first PIA recommendations

	Page No. (Nature)	**Consultant's Views / Recommendations**	**Government's Response/ Way Forward (1st PIA)**	**Status Update as of 30 April 2002 from the HKSAR Government**
4	78 (Principle)	If the card is to hold other applications, there raises privacy concerns about:- ▪ the Smart card scheme operator being a separate government agency; ▪ 'outsourcing' of card management; ▪ the Smart card scheme operator was a commercial operator, either through 'outsourcing' or as a joint venture; and ▪ limited range of administrative aspects being handled by another agency and the ImmD would keep control over all aspects of registration and card-issue.	For the card management:- ▪ the use of a commercial operator has been ruled out; ▪ for ID card matters, ImmD will remain responsible for the registration and issue of ID cards and the maintenance of the application records; ▪ for non-ID card matters, a high level inter-departmental Steering Committee chaired by SITB has been formed to take care of the multiple application aspect of the Smart card scheme. The Steering Committee will make recommendations on the types of applications to be included in the new Smart ID card. ImmD is a member of the Steering Committee. The "scheme operator" is a team of technical people to provide technical advice and support service on the multiple application aspect of the Smart ID card scheme, e.g. provide help desk service, certifying equipment, etc. They will have no access to the data that are kept by individual departments. We are conducting various feasibility studies with regards to the implementation of multi-applications. Based on the findings of these studies, we will firm up the design on all aspects of the card management scheme giving due regard to privacy concerns. In any case, we have no intention to outsource the card management.	Under the proposed ROP (Amendment) Bill 2001, the Chief Executive-in-Council is the authority to approve the add-on applications while the Commissioner of Registration is the authority to administer the inclusion or storage of these add-on application data in the Smart ID card.

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
5	67 (Technical advice)	If the cards are to be capable of supporting cryptographic functions, the private keys, for both digital signature and message-encryption purposes, should be generated on the chip alone to ensure maximum privacy protection.	Will be considered in the feasibility study on digital certificate.	ImmD's applications rely on MULTOS security. MULTOS has a Key Management Authority (KMA), which securely places applications and data onto the card using asymmetric cryptographic keys. ImmD's SMARTICS relies on the Secure Access Module (SAM) to securely communicate with the terminals and the ROP back-end system using symmetric cryptographic keys. Cryptographic keys supporting the ImmD's applications are securely generated and injected onto the card during initialisation and personalisation processes. Since the environment in which the symmetric and asymmetric cryptographic keys are to be generated is secure, the advantages of generating the keys on the card itself are reduced. Cryptographic keys (secure session keys) are on-card generated.
6	71/72 (Procedure)	It appears that the omission of the thumbprint from the ROP database would have a limited negative impact (some relatively minor inconvenience for those who have lost or damaged cards), in return for a very considerable reduction in the system's privacy-invasiveness.	Have serious reservation to omit the thumbprint from the ROP database. Without the thumbprint that is the record of last resort and the unique key for verification of identity, ImmD shall not be able to quickly and positively authenticate if a person is the rightful holder of a lost or damaged card. More importantly, the proposal would adversely affect the speed in re-establishing the identity of distressed Hong Kong residents who have lost their	The current design of SMARTICS will include an image of the thumbprints in the ROP database. As the template algorithms available in the market are proprietary items, it is not advisable to store only the thumbprint template in the ROP database to avoid ImmD from being locked on to a particular vendor. In the event that the

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
	87/88 (Technical advice)	An alternative approach would be for the ROP database to carry only the thumbprint template. ImmD should: ▪ design alternative processes and procedures to handle a situation in which thumbprints are not held on the ROP database, or are held only in template form; ▪ in the Request For Tender, require tenderers to provide proposals relating to alternative implementations in which the ROP database contains the thumbprint, contains only a template of the thumbprint, and contains neither; ▪ conduct trials to confirm that these procedures do not significantly reduce the integrity of the scheme, nor unduly increase the efforts and costs of individuals or the ROP Registration Office; ▪ subject to satisfactory outcomes of these trials, implement the system without storing the thumbprint in the ROP database.	identification documents and are stranded in overseas countries. In normal circumstances, most foreign governments will only provide the thumbprint impressions to ImmD for verification. While the quality of the thumbprint impressions are normally adequate for visual checks against the thumbprint records kept by ImmD, they may not be good enough for the generation of templates for matching purposes. Delays will occur if we need to ask the government concerned to take another set of thumbprint impressions. The storage of raw and encrypted fingerprint images in the ROP database is preferred to the storage of templates because the latter will make one-to-many matching much easier. The use of proprietary biometrics template techniques will also lead to vendor lock-in. We should avoid this risk because it is impractical to ask the whole population to provide the thumbprints again if the vendor runs out of business. In view of PCO's advice, we will explore in forthcoming tender whether vendors could provide creative suggestions which would address the concerns of both sides. We also agree that if a decision is taken to maintain the thumbprint images in the ROP databases, we will work out the appropriate legislation/regulatory and technical measures (e.g., encryption of thumbprints) to restrict access to such data and to re-assure the public that there will not be one-to-many matching searches, as we have committed publicly before.	algorithm needs upgrading or amendment, the vendor may charge exorbitant fees. It would be even more disastrous if the vendor runs out of business. Additional privacy safeguards have been adopted both at the technical design level and changes to the current legislation have been considered. Amendments to the current ROP Ordinance will assist to address concerns about data privacy. There will be provisions to penalise unauthorised access, use, storage, and disclosure of ROP information. The provision to prohibit a registration officer from disclosing ROP data, except with the written permission of the Chief Secretary for Administration, will be moved from the ROP Regulations to the ROP Ordinance in order to raise its status.

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
7	82 (Procedure)	ImmD will need to ensure that the statement of purpose and of the parties to whom the personal data may be transferred [Data Protection Principle [DPP1(3)(b)(I)(B)] keeps pace with the actual uses and disclosures of personal data, both now and particularly under the new system.	Will comply.	The SMARTICS Identity Card (General) Division of the ImmD SMARTICS project team has been established to review the 'statement of purpose' and use of the ROP data.
8	82 (Procedure)	ImmD should review the adequacy and accuracy of its 'statement of purpose' included on forms to satisfy the underlying objective of DPP 1(3).	Will comply.	The SMARTICS Identity Card (General) Division of the ImmD SMARTICS project team has been established to review the 'statement of purpose' printed on the ROP forms.
9	83 (Procedure)	During the card replacement exercise, ImmD may wish to consider whether arrangements can be made for a range of individuals who have special circumstances or needs. These include, potentially: ▪ persons-at-risk (various categories described under Special Arrangements on p.79) ▪ public figures, whose participation in normal registration processes might cause difficulties either for them or for ROP staff; and	Some of the suggested special arrangements e.g., non-capture of thumbprint, additional ID cards, etc, will adversely affect the integrity of the ROP database. For the sake of fairness, we will have to treat all residents alike. But if there are good reasons, we will consider providing special assistance on a case-by-case basis.	No further updates.

Annex III

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		▪ persons with genuine objections to the standard processes for capturing photograph or thumbprints, either for religious or conscientious reasons or because of disfigurement.		
10	83 (Legislation)	ImmD needs to review the need for the items of information required under ROP Regulation 4 to be updated.	Will review.	An internal review is being conducted to see if there is a need to collect all the prescribed items of information under Regulation 4.
11	84 (Legislation)	Consideration should also be given to statutory amendments to give legal protection to individuals against 'presumption of guilt' due solely to technology failures (e.g. corrupt or damaged cards, card-receiver failure, loss of communications links).	Hong Kong law is based on 'presumption of innocent'. According to legal advice, legislative amendment will not be required for this purpose.	No further updates.
12	84 (Procedure)	ImmD should review its records retention policy and develop and implement a disposals schedule in respect of all personal data, in all storage media, to comply with the requirements of DPP 2(2) and s.26 in relation to retention and erasure of data when the purpose for holding it has expired.	At present, ROP records are kept for a long period of time even if the person concerned was deceased because the data will still be needed for a variety of purposes, in assessing claims to right of abode or applications for Certificate of Registered Particulars by descendents. We will, however, review the record retention policy to ensure that the requirements of DPP 2(2) and s.26 will be compiled.	The SMARTICS Identity Card (General) Division of the ImmD SMARTICS project team has been established to review the record retention policy.

Annex III

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
13	84 (Legislation)	Statutory amendments will be required to the ROP Ordinance and Regulations, and possibly to other laws, to provide for the new scheme, including specifically for the following elements: reading of 'non-visible' card data by departments other than ImmD; provision of thumbprints in various scenarios for comparison with the prints recorded in digital form on the card.	Will consult PCO on the legislative amendments.	ROP (Amendment) Bill 2001 was introduced to LegCo on 9-1-2002 with related clauses 7(9) (restriction on use of particulars) and 13 (power to verify identity by fingerprint match) added.
14	85 (Legislation)	ROP Regulation 24 should be amended to expressly cover all personal data held by ImmD in connection with the ROP function.	Will comply.	Particulars to be furnished under ROP regulation 4 have covered all personal data required by ImmD in connection with the ROP function. Additional personal data required under SMARTICS has been specified in the ROP (Amendment) Bill 2001.
15	85 (Legislation)	Consideration should be given to moving the prohibition into the ROP Ordinance itself, or any amendments made subject to the express approval of LegCo (i.e. positive disallowance), so that it cannot be overridden by pre-existing provisions in Ordinances giving a power to obtain information.	Will comply.	ROP (Amendment) Bill 2001 was introduced to LegCo on 9-1-2002 with related clause 7(10) (duty not to disclose photographs, fingerprints and particulars) added.
16	85 (Legislation)	Any subsequent legislative provisions to authorize disclosures of ROP information should also be subject to a positive approval process in LegCo.	Will comply.	ROP (Amendment) Bill 2001 was introduced to LegCo on 9-1-2002 with related clause 7(10) (duty not to disclose photographs, fingerprints and particulars) added.

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
17	85 (Legislation)	The ROP Ordinance should make all unauthorised use (including 'mere' browsing), and including unauthorised disclosure of the information concerned, an offence, subject to suitable penalties.	Will need to look at the issue further with Department of Justice as to the establishment of mens rea, in cases of 'mere' browsing.	ROP (Amendment) Bill 2001 was introduced to LegCo on 9-1-2002 with related clauses 7(10) (Duty not to Disclose Photographs, Fingerprints and Particulars) and 7(11) (Prohibition of Unauthorised Handling of Particulars) added.
18	85 (Procedure)	ImmD should ensure that all disclosures from the ROP database and other records (whether provided directly or via an ability to read card data) are authorised by relevant permission under ROP Regulation 24.	This is already the case. Will continue to comply.	No further updates.
19	85 (Procedure)	With regard to matching procedures, ImmD will need to ensure that any requests for further automated matching under the new system meets the definition of matching procedure in the PD(P)O and endorsed by the Privacy Commissioner.	This is already the case. Will continue to comply.	No further updates
20	85 (Principle)	Privacy concerns about the use of personal data held on, or supplied in connection with, the HKSAR ID Card would be significantly reduced if ImmD, or the government as a whole, were able to give commitments: ▪ that the card will not be contactless; ▪ that the details which are	Agree in principle. ImmD will probably use contact smart cards but have reservation to expressly rule out the use of contactless cards. This is because with the change in technology, it is quite possible that contactless cards can be as secure as contact cards.	Contact smart card technology will be employed for SMARTICS. Understand that contactless smart card technology is advancing rapidly, we therefore cannot rule out the possibility that a contactless smart card may in future become as secure as contact smart card. Will comply with the Feasibility Study Report on card face details and chip data

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		permitted to be displayed on the card will be no more than those envisaged in the Feasibility Study Report; ▪ about the specific data items that may be stored in the chip; ▪ about the organizations or classes of organizations permitted to access data directly from the chip, and for what purposes; ▪ about the organizations or classes of organizations permitted to take (or read) thumbprints for the purpose of comparison with the digitised print on the card, and the circumstances in which this will be permitted; and ▪ about the circumstances under which conversion of any of the information which is merely imaged (previously microfilmed) into fully machine-readable form is permitted.		contents. Data items to be loaded into the chip of the smart ID card are clearly specified in the ROP (Amendment) Bill. The Bill also provides for the circumstances in which the taking of fingerprints for the purpose of comparison with the template on the card are permitted. Personal data of cardholder is compartmentalised within application boundaries such that personal data under respective application is accessible only through terminals of corresponding government departments. However, fingerprint capture, access and comparison are limited to Immigration authorised terminals and kiosks only. Converted digital image from microfilm remains in the state of a static image for page viewing only. Fully machine-readable forms such as OCR and other recognition technologies are disallowed.
21	86 (Principle)	Person-to-person linkage is a very privacy-invasive activity. ImmD should ensure that provision of 'associated person' data (e.g. parent-child, guardian-child & spouses etc.) to authorised	Agree in principle.	There are adequate provisions under the PD(P)O and ROP Regulation 24 to govern the disclosure of 'associated person' data.

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		agencies is covered by proper legal authority. That is, permissions issued pursuant to ROP Regulation 24 are worded so as to allow 'associated person' data to be disclosed.		
22	86 (Principle)	The data stored on the card chip for the ROP/ID card application should be subject to all of the limitations embodied in the Feasibility Study (FS) Report, in particular that they are :- ▪ limited to the data-items currently envisaged and set out in that Report; ▪ subject to the specified technical protections; and ▪ accessible only by the specified and very limited number of devices and organizations for the specific purposes stated.	Will comply with PCO's comments.	The following privacy enhancing measures have been included in the design of the SMARTICS such as: ▪ Citizen's choice of viewing electronically stored data ▪ Citizen's choice of application download/deletion ▪ Card specific confidential download ▪ True compartmentalisation of application specific data ▪ Citizen's choice of add-on application enablement
23	86 (Technical advice)	The system specification for the new system should expressly include the segregation of data, functions and applications as well as limited conveyance of information by card number that it currently does.	Agree in principle, but subject to the views of the consultants who are studying the multiple application side of the system.	Segregation of on-card data, functions, and applications are securely enforced by the MULTOS chip operating system.
24	87 (Technical advice)	The Request For Tenders (RFT) should explicitly require proposals to explain precisely how integrity of data and	Will comply.	Done. Protection of data against disclosure to,

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		functions will be protected with details of hardware, system software and application level features. The card should perform challenge to and authentication of devices and processes with which it interacts, and only participate in processes where the results are satisfactory, in order to provide protection of the data against disclosure to, and of processes from performance by, unauthorised parties. The card should participate effectively in the authentication of the person presenting it so as to prevent the exercising of the cardholder's prerogatives by an imposter.		and of processes from the performance by, unauthorised parties is done by mutual authentication of card and card receiving device using the Secure Access Module. Authenticity of the cardholder is ensured by fingerprint matching upon access of personal data.
25	87 (Technical advice)	It is highly desirable that the biometrics stored on the card do not leave the card under any circumstances. The RFT should invite tenderers to address this issue. It should be made a 'highly desirable' feature that would weigh significantly in the assessment of tenders, if it proves to be available.	Agree in principle but subject to technical study, in particular, the transaction response time. Will invite tenderers to look into the issue and propose solutions.	Agree in principle. However, the current technology in Smart card does not permit the SMARTICS to do so because of memory and performance constraints. We will revisit this issue as soon as it is technologically viable.
26	87 (Technical advice)	If the cards are to be capable of supporting cryptographic functions, then the following additional specifications should be included:	The future FS on digital certificate will take into account those recommendations on key generation and storage. Will consider the suggested backup arrangements for	ImmD's applications rely on MULTOS security. MULTOS has a Key Management Authority (KMA), which securely places applications and data onto

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		▪ the card must perform secure key-generation, and provide secure key-storage and secure key usage for both digital signature and message-encryption key-pairs; ▪ cardholders must be given the choice concerning the number and usage of key-pairs and certificates acquired; ▪ any backup arrangements for private keys need to be entirely at the discretion of the cardholder, such that individuals have a genuine choice of organizations offering back up services, including non-government service providers; ▪ no government agency should be able to gain access to any such backup; and ▪ compulsory escrow arrangements for private keys must be precluded.	private keys.	the card using asymmetric cryptographic keys. ImmD's SMARTICS relies on the Secure Access Module (SAM) to securely communicate with the terminals and the ROP back-end system using symmetric cryptographic keys. Cryptographic keys supporting the ImmD's applications are securely generated and injected onto the card during initialisation and personalisation processes. Since the environment in which the symmetric and asymmetric cryptographic keys are to be generated is secure, the advantages of generating the keys on the card itself are reduced. Cryptographic keys (secure session keys) are on-card generated. To date, only e-Cert issued by the Hong Kong post will be available upon implementation of SMARTICS. For optimal security, backup of private keys and escrow services are not possible, as the private key cannot be exported out of the Smart ID card.
27	87 (Principle)	Privacy concerns would be eased if ImmD could confirm that the digital thumbprint will only be used for one-to-	Will comply	Only one-to-one comparison of digital thumbprint is allowed in the design of the SMARTICS system.

Annex III

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		one comparisons for the purpose of authenticating the claim of identity of a person, and for no other purpose, especially for one-to-many comparisons in order to identify a person from their thumbprints.		
28	88/89 (Technical advice)	An appropriately qualified independent technical consultant, should certify, following a technical audit, that the design and implementation of the scheme ensures that the following risks have been comprehensively and effectively addressed:- ▪ the risks of using the card to store and disclose data unknown to the person and to perform functions unknown to the person; ▪ if the key is to support cryptographic functions, the risk that a private key could be discovered and invoked by a person other than the cardholder; ▪ in relation to card-reading devices, the risk of :- ▪ interception of traffic, and hence access to personal data or access to a stream of data; ▪ the recorded biometrics becoming capturable by other	Will look into these areas in the next PIA and the Security Audit.	Citizens will be informed of the personal data stored in their Smart ID cards. A cardholder can view his personal data stored in the card using self-service kiosks. Access to personal information stored in the card is restricted to the cardholder and authorised personnel. This is enforced by : ▪ authenticating the card receiving device using a SAM installed therein ▪ authenticating a cardholder by verifying the cardholder's fingerprint against the template stored in the card All activities are conducted with the complete knowledge and interaction with the cardholder. A private key stays in the protected memory space inside the Smart ID card once the card is personalised at issuance. Technically, the private key is used by the

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		agencies, organizations or individuals; ▪ other organizations seeking to capture the biometrics themselves, as a more efficient means of authentication than visual inspection of the ID Card; ▪ the recorded biometrics being obtained illicitly and used by impostors to masquerade as an individual; ▪ the PIN or PINs being captured; ▪ masquerade use of unsupervised devices by impostors who acquire the card and any necessary knowledge; and ▪ card-data being amended by inappropriate devices.		crypto-engine inside the Smart ID card and will not be directly accessed by the Smart ID card applications nor external interfaces. During transmission, all data messages are encrypted and integrity protected by unique sequence number and message authentication code (MAC). Card and card reading devices must be mutually authenticated before data (including biometrics data) can be read. Fingerprint images will be encrypted before storing into the database. Terminal devices (both self-services kiosk and off-line handheld readers) are not active until authorised personnel at SMARTICS central site enables them using mutual authentication techniques and sends the necessary activation commands through secure channel. The Smart ID card does not allow external terminal device to change its content without proper mutual authentication between the terminal device and the Smart ID card and mutual authentication between the terminal and the backend computer, thus ensuring an end-to-end authorisation for updating data on card.

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
29	89 (Technical advice)	The new scheme should embody all of the privacy-positive security features that are in the existing scheme, including access controls and interface controls relating to other ImmD systems, and external systems such as ECACCS. Controls should apply at all times, including, for example, to mobile registration operations.	Will comply.	In addition to the privacy-positive security features that are in existing scheme, the following privacy enhancing measures will be implemented in the SMARTICS : ▪ Citizen's choice of viewing electronically stored data ▪ Citizen's choice of application download/deletion ▪ Card specific confidential download ▪ True compartmentalisation of application specific data ▪ Citizen's choice of add-on application enablement
30	89 (Technical advice)	ImmD should work towards integrating access controls to its computer systems with its human resource management system(s), in relation to the timely invalidation of user ID/password pairs on departure of staff and during extended periods of absence.	Agree to work towards this direction although the proposal involves the integration of another system that is not yet well developed/computerised.	A comprehensive role-based access control system is available in the SMARTICS such that timely invalidation of user ID/password pairs can be achieved.
31	89 (Technical advice)	The specifications of the scheme relating to the gathering of logs and audit trails should be enhanced to ensure that sufficient detail is gathered.	Will comply.	The SMARTICS is designed in such a way that transaction logs and audit trails will have sufficient details to reveal the transaction types and the officers involved.
32	89 (Technical advice)	The specifications for the scheme should be amended to require much higher standards of reliability and resilience than the "at least that of the current system" suggested in the Feasibility Study Report.	Agree but subject to technical feasibility and cost effectiveness.	Under the SMARTICS, a high level of reliability and resilience will be achieved using a fault tolerance design combining high availability computing, backup computer centre, redundant network links,

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		Disaster recovery planning should be based on much more than the suggested "basic survival" mode.		etc
33	89 (Principle)	ImmD should include understanding of the privacy issues associated with ID cards and their use, and the way in which these issues have been addressed, in training programs for relevant staff.	Will comply.	A 'training sub-section' of the ImmD SMARTICS project team has been established to plan for staff training in this aspect.
34	89 (Legislation)	Making it an offence to solicit (with or without payment) unauthorised disclosure of ROP data.	Will comply.	ROP (Amendment) Bill 2001 was introduced to LegCo on 9-1-2002 with related clause 7(11) (prohibition of unauthorised handling of particulars) added.
35	90 (Legislation)	Placing limits and/or conditions on the use of ROP data by persons or organizations to whom ROP data is disclosed (both directly pursuant to ROP Regulation 24 and indirectly under Regulation 23), and making it an offence to breach those limits/conditions.	Will comply.	ROP (Amendment) Bill 2001 was introduced to LegCo on 9-1-2002 with related clause 7(11) (prohibition of unauthorised handling of particulars) added.
36	90 (Principle)	ImmD should re-affirm its commitment to take disciplinary action against any officers or employees breaching security, and/or using personal data outside relevant legal authorities.	Will comply.	ROP (Amendment) Bill 2001 was introduced to LegCo on 9-1-2002 with related clause 7(11) (prohibition of unauthorised handling of particulars) added.
37	90	Publication of aggregate statistics about	Will consider.	Aggregate statistics about disclosures of

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
	(Public Consultation)	disclosures of ROP information to other agencies would be a significant demonstration of commitment to this principle.		ROP information to other government departments will be maintained. The only exception is statistics relating to "the purposes of safeguarding security, defence or international relations in respect of Hong Kong" (Section 57, PD(P)O, Chapter 486).
38	90/91 (Principle)	It is partly in the spirit of the openness and transparency principle that Privacy Impact Assessments should be carried out in public, and with the widest possible input. While there has been no public input into this PIA to date, public release of the PIA report as soon as possible would be consistent with the objective of DPP 5 of the PDPO. Ideally, this PIA should be made public, to assist consideration of the proposal by legislators and other stakeholders. In addition to public release of the PIA, it should be given to key representatives of the public.	An abridged version of the first PIA report has been distributed to LegCo Members. We will also disclose the results of future PIAs.	We have pledged to the members of the LegCo Security Panel on 9-4-2002 that we would report the findings of the 2nd PIA.
39	90 (Public Consultation)	Wider consultation about the HKSAR ID Card scheme would both engender confidence in the scheme, and enable ImmD to take account of any concerns in the design.	The first round of public consultation was completed in December 2000. We will consult the views of the relevant LegCo Panel before other non-immigration applications are to be included in the Smart ID card.	All eighteen District Councils were consulted during the first round public consultation program. The 2nd round publicity consultation campaign in eight local universities and educational institution was completed in February 2001.

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1^{st} PIA)	Status Update as of 30 April 2002 from the HKSAR Government
				A 3-day exhibition was held during 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/ views from the public has been established since November 2000.
40	91 (Public Consultation)	In order to facilitate understanding amongst stakeholders, ImmD should make available technical briefing materials.	An abridged version of the management summary of the Feasibility Study Report on the new identity card system was issued to LegCo Members in early December 2000.	No further updates
41	91 (Public Consultation)	Given the tight timetable, ImmD could consider convening a public interest reference group, comprising key representatives, to provide an efficient channel for information about the proposal, and for feedback. Consultation would not therefore need to be completed in the immediate future and could proceed in parallel with the tendering process.	A special LegCo Security Panel meeting which was opened to the public and focus groups, was held on 11.11.2000. Besides, open forums to the general public and focus group were arranged on 6.12.2000 and 6.1.2001.	A 'Discussion Forum on Smart Card from the Smart Card & IT Industry' have been set-up and met twice on 31-8-2001 and 21-9-2001 prior to the close of the SMARTICS tender. Visits to local university Smart card professionals for advice prior to the close of the SMARTICS tender were conducted.
42	92 (Public Consultation)	There will presumably be a major public information and education campaign prior to the commencement of re-registration; and there will also need to be awareness and training activity associated with the proposed 'kiosks' at which individuals will be able to check	Being arranged.	The SMARTICS Identity Card (General) Division of the ImmD SMARTICS project team has been established in May 2002 to plan for the major publicity and education campaign together with the Information Services Department.

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1^{st} PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		the contents of their cards. Explanation of privacy issues and the ways in which they have been addressed should form part of these campaigns.		
43	92 (Public Consultation)	ImmD should incorporate material on privacy issues into public information campaigns and related activity preceding and accompanying the introduction of the new ID Card.	Done. Promotion leaflets contain concrete measures to be taken to address privacy concerns.	No further updates.
44	92 (Procedure)	ImmD's approach to satisfying requests for access is to use existing statutory processes where they already exist. Most of the template certificates used in reply to such applications are designed to meet the particular needs. ImmD needs to ensure that responses to these requests satisfy DPP6 and s.19(1) of PD(P)O by providing all of the applicable personal data, together with whatever explanation may be required (e.g. of codes).	Already complied with.	No further updates.
45	92 (Procedure)	ImmD should review its processes for responding to subject access requests under DPP 6 to ensure that individuals are given access to all the ROP data to which they are entitled.	Already complied with.	No further updates.
46	93	The RFT should be formally reviewed,	Will incorporate into RFT privacy features and additional	Done. We have consulted the PCO before

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
	(Expert advice)	prior to despatch to vendors, by persons with specialist expertise in the privacy aspects of schemes of this nature, to ensure that any additional privacy-positive measures adopted as a result of this PIA Report have been translated effectively into tender specifications.	privacy-positive measures as recommended in all PIAs and agreed by the Administration. Will consult PCO before finalizing the RFT.	finalizing the SMARTICS Tender for issuance. Section 13 (Data Privacy Requirements) was included in Part VII, Project Specification of the SMARTICS Tender.
47	93 (Expert advice)	The selected tender should be reviewed, prior to finalisation of the contract, by persons with specialist expertise in the privacy aspects of schemes of this nature, for its conformity with the privacy requirements of the RFT.	Will vet tenders carefully to ensure conformity with the privacy requirements of the RFT and consult PCO before finalization of contract.	The tender proposals were evaluated by an inter-departmental assessment panel comprising the senior government officials in accordance with the prescribed procedures and criteria endorsed by the Central Tender Board. Office of the Privacy Commissioner for Personal Data (PCO) was consulted to comment whether the selected proposal was in conformity with the privacy requirement of the tender. On the advice of PCO, the proposal was enhanced to ensure the contractor's full commitment in meeting the tender requirement in the privacy aspect.
48	95 (General)	ImmD needs to recognize the very substantial privacy implications of the proposed scheme, and the resultant need for an integrated strategy in relation to all of the following: ▪ legal authorizations and constraints; ▪ consultation, preferably directly	We have discussed the matter with PCO and agreed that our privacy strategy should encompass the following areas :- Legislative aspect – to ensure that the necessary data privacy safeguards are laid down in law so as to deter abuses and to gain the confidence of the public; Administrative aspect – to ensure that the necessary procedural safeguards and code of practice are drawn up;	The 2nd PIA consultancy is in progress (April 2002).

Status of the first PIA recommendations

	Page No. (Nature)	Consultant's Views / Recommendations	Government's Response/ Way Forward (1st PIA)	Status Update as of 30 April 2002 from the HKSAR Government
		with the public, but at least with key representatives; ▪ technical specifications; ▪ organizational policy commitments; ▪ compliance with the PD(P)O; and ▪ public awareness, education and training campaigns. Implementation of an integrated privacy strategy will involve a combination of legislative amendments, policy commitments, and specifications in the scheme design, tendering, contractual and implementation stages of the project.	Technical aspect – to ensure that the necessary privacy enhancing technologies are built into the system; Publicity aspect – to ensure that the general public fully understands what they can do with their ID cards and their data privacy rights. We will conduct further PIAs at different stages of the project. We will also develop a code of practice jointly with the PCO.	