For discussion **FCR(2015-16)7**
on 17 April 2015

ITEM FOR FINANCE COMMITTEE

CAPITAL WORKS RESERVE FUND
HEAD 710 – COMPUTERISATION
Immigration Department
New Subhead "Next Generation Smart Identity Card System"

Members are invited to approve a new commitment of $1,448,786,000 for the Next Generation Smart Identity Card System.

PROBLEM

The Immigration Department (ImmD) needs to develop a new computer system, namely the Next Generation Smart Identity Card System (SMARTICS-2), to replace the existing ageing computer system and to enhance operational efficiency and effectiveness in supporting the issue of smart Hong Kong Identity Cards (HKICs).

PROPOSAL

2. The Director of Immigration, with the support of the Secretary for Security and the Government Chief Information Officer, proposes to create a new commitment of $1,448,786,000 for SMARTICS-2.

JUSTIFICATION

Need for a new system

3. The current Smart Identity Card System (SMARTICS) was introduced in 2003. As with other computer systems, SMARTICS was designed for optimal use for about ten years. Having been developed in the early 2000s, its hardware and software are becoming obsolete. It has become increasingly difficult

/to …..

to secure system maintenance and technical support due to limited and dwindling market supply of the outdated technologies. The core software packages supporting SMARTICS have become obsolete and ultimate support from the manufacturers has ceased. The expiry date of the system maintenance agreements was recently extended from December 2013 originally to end 2018. Further extension is considered not desirable as it can no longer ensure system reliability due to prolonged use of outdated technologies.

4. Without suitable and on-going maintenance and technical support, there is increasing risk of system failure which will lead to serious and large-scale disruption of public services, including registration and production of smart HKICs, identity verification for HKSAR passport applicants, etc. There is an imminent need to replace the existing system to ensure timely provision of critical public services and adequate capacity for coping with new public service demands (e.g. enhancing the registration of persons (ROP) process) in future.

Need for new smart HKICs

5. There is no expiry date for the existing smart HKICs[1], but the serviceable lifespan of the card material is ten years under normal usage, as guaranteed by the contractor and subsequently confirmed through independent laboratory tests commissioned by ImmD. In 2012, ImmD commissioned two independent laboratories in Europe to ascertain the durability of the existing smart HKIC[2]. Neither laboratory was able to conclude that the durability of the smart HKICs could go beyond ten years within the framework of the international standards[3] in testing cycles representing usage after ten years. This indicates that the designed serviceable lifespan of smart HKICs issued between 2003 and 2007 is due to expire between 2013 and 2017. While the existing smart HKICs may not necessarily break or malfunction by default once the ten-year mark is reached, the need for replacement would continue to increase over time. To introduce new smart HKICs to replace all the existing ones will avoid the scenario of having to cope with a large number of smart HKICs failing together in a short period of time, which may go beyond ImmD's handling capacity within the normal pledged timeframe and risk causing grave public inconvenience.

/6. …..

---

[1] Similar smart identity cards issued by other jurisdictions, including Germany, Belgium, Malaysia and the Macao SAR, are all set for replacement within five to ten years of issuance for various reasons, including ensuring card durability.

[2] The laboratories conducted a series of ageing tests, such as thermal, chemical, humidity, ultra violet light and dynamic bending stress tests, which aimed to simulate the extension of normal usage.

[3] Such as ISO/IEC 24789 Identification cards – Cards service life which provides guidance on methods and their use to simulate a card's service life, and ISO/IEC 10373 Identification cards – Test methods which define test methods for characteristics of identification cards.

6. Despite the small number of forged smart HKICs detected in recent years, there have been cases of seizure of forged smart identity cards in Europe with card materials and security features similar to the existing smart HKICs. With continued technology advancement, forgery cases of our smart HKICs are expected to become more prevalent if there is no timely introduction of new security features and chip architecture technology.

Major Features of SMARTICS-2

Enhanced ROP process

7. As in the existing system, SMARTICS-2 will continue to support the registration and production of smart HKICs (including receiving applications, conducting record check and case assessment, personalization and card issuance). It will also support the provision of other immigration-related services by ImmD (e.g. identity verification for HKSAR passport applicants) and verification of personal data requested by other government bureaux/departments or public organisations for specific purposes in accordance with the law. Subject to detailed system design, SMARTICS-2 will enhance the ROP process to provide greater convenience to the public. Riding on the new system, improvement initiatives such as on-line form filling, automatic record check for application assessment and self-service collection kiosks with e-cabinet, etc.[4] will be introduced.

Enhanced card security features

8. The new smart HKICs will make use of latest polycarbonate materials to ensure better visual appearance, improved text printing quality and increased durability under normal usage. The opportunity will also be taken to enhance card face security features to ensure a continued low forgery rate with advancement in technology[5].

/9. …..

---

[4] On-line form filling allows applicants to complete smart HKICs application forms from any location through the internet instead of having to complete the form in person at the ROP office or card replacement centre. This would shorten the processing time when the applicant attends the ROP office or card replacement centre. Automatic record check assists the Registration Officer to conduct record check automatically instead of manually, thereby reducing the time needed in the registration process. Self-service collection kiosks with e-cabinet allow applicants to collect their new smart HKICs at a collection kiosks installed with automatic card dispenser. Applicants may therefore collect their new cards at their convenience without having to make prior appointments with the Registration Office.

[5] For reference, some of the latest security features being used in identity cards alike in other jurisdictions include see-through window, hologram effect, lenticular effect, full-colour UV print, etc.

9. The existing smart HKICs support a contact interface only. To access data from the chip, the user needs to insert the smart HKIC into a card reader, where the chip will physically connect with the reader directly to allow communication. Tapping on proven chip technology for faster data retrieval and lower chip damage, the Government proposes to introduce an additional "contactless" chip interface (no need for any physical connection between the chip and the reader) making use of close-range wireless transmission, safeguarded by multi-dimensional security features.

10. The proposed new "contactless" chip interface will be designed strictly in accordance with ISO 14443 (type A or B), a proven and internationally-adopted standard for smart card chips for secured documents. With a view to ensuring trusted and secured wireless communication and data transmission between the chip and the reader, as well as preventing "passive" or "remote" reading of chip data, access to the chip must be initiated by the cardholder. Before communication, the identity of the chip and the reader must be defined, and mutual authentication must be confirmed. In addition, all communication and data transmission must be encrypted throughout the process.

11. Same as the existing smart HKIC chip, the chip in the proposed new smart HKICs will not be powered by any standalone battery and will not be able to send out any signal by itself. Access to chip data through the "contactless" chip interface must be initiated by the cardholder through taking out the smart HKIC and placing it onto an authorised optical card reader, which will optically capture a "key text string" from the card face (like taking a photograph, commonly known as Basic Access Control). After successfully capturing the "key text string", the specific algorithm implanted in the reader will generate a real-time, one-off encrypted key. The encrypted key will then need to be authenticated by the chip to enable a one-on-one, exclusive communication channel. In order to access data stored in the chip, the reader will need to further submit a different, second key to the chip for another authentication process.

12. As successful capturing of the "key text string" printed on the card face by optical means by the authorised reader is a "pre-requisite" to activating the close-range wireless transmission function of the chip, the cardholder takes control over the data transmission process by physically placing the card directly onto the reader. If the cardholder does not take out the smart HKIC himself, or if there is no encrypted key in the specific card reader authorised with certificate, it is not possible to access the chip through the "contactless" chip interface.

13. Detailed information on the multi-dimensional safeguards for the proposed new "contactless" chip interface is at Enclosure 1.

Encl. 1

Personal data privacy protection

14. Apart from the above designed multi-dimensional security features, the existing ROP Ordinance (Cap. 177) (ROPO) and the ROP Regulations (Cap. 177A) (ROPR) provide stringent safeguards against unlawful access to the chip data and mount tight control over the collection or use of ROP data.

15. Regulation 12(1B)(a) of the ROPR provides that a person to whom an identity card relates has lawful authority to gain access to data specified in Schedule 1 to the ROPR which are stored in the chip embodied in the identity card if he gains such access by using facilities provided by or with the approval of the Government, including, at present –

Immigration-related facilities exclusively controlled by ImmD

(a) e-Channels;

(b) Self-service e-Passport application kiosk;

(c) Enrolment kiosk for Macao e-Channels;

(d) SMARTICS kiosks;

Non-immigration-related facilities under Multi-application Smart ID Card (MASC) scheme, subject to cardholder's consent [6]

(e) Public library service;

(f) Leisure Link Self-service Kiosks;

(g) e-Health System; and

(h) Public-Private Interface-Electronic Patient Record Sharing Pilot Project.

16. Regulation 12(1B)(b) of the ROPR provides that a person to whom an identity card relates has lawful authority to gain access to data specified in Schedule 5 to the ROPR which are stored in the chip embodied in the identity card if he gains such access only for the purpose for which the data are stored. At present, such data includes only the e-Certificate. There are no other legal provisions in the ROPO, ROPR or any other laws in Hong Kong giving anyone the same lawful authority to gain access to data which are stored in the chip embodied in the identity card.

/17. …..

[6] For the use of all such facilities, cardholders have to insert the smart HKIC into a card reader to gain access to the chip to read the required information from the chip, authorised under Regulation 12(1B)(a) of the ROPR, and present such information to the corresponding facilities set out above for access to different public services.

17. Pursuant to Regulation 12(1A)(b) of the ROPR, any person who, without lawful authority or reasonable excuse gains access to any data stored in a chip (of a smart HKIC) shall be guilty of an offence and liable to a fine at level 4 ($25,000) and to imprisonment for two years. The proposed new chip interface of the new smart HKICs will be governed by the same legal provisions.

18. ImmD will engage independent experts and consultants to ensure necessary safeguards are in place to comply with legal requirements on protection of personal data as well as system security at each and every stage of project development and future application.

19. Drawing reference to the implementation of the first-generation SMARTICS, ImmD will commission qualified independent consultants to conduct Privacy Impact Assessments (PIAs) during each critical stage of the implementation of SMARTICS-2, including feasibility study, system analysis and design, pre-implementation and post-implementation. Each PIA report will be submitted to the Privacy Commissioner for Personal Data (PCPD) for comments to ensure compliance with relevant data protection principles and other requirements under the Personal Data (Privacy) Ordinance (Cap. 486). The recommendations of the consultants and the PCPD, if any, will be adopted for the subsequent stage to enhance implementation of SMARTICS-2.

20. The external consultant who completed the first PIA in October 2014 has confirmed that proposed access protection measures and mutual authentication are effective means of preventing unauthorized access to personal data stored in the smart HKICs through contactless interface. A summary of the consultant's technical assessment and recommendations made in the first PIA in relation to card interface, card materials and security features on card body is at Enclosure 2. ImmD has submitted the first PIA report to PCPD and its comments will be incorporated into the next implementation stage.

Encl. 2

21. In addition to PIAs, ImmD will engage an independent auditor to conduct information technology security risk assessment and security audit (ITSRAA) at different stages of implementation to ensure the effectiveness of those security measures in protecting information in SMARTICS-2 and smart HKICs.

22. During project implementation, ImmD will perform regular self-compliance checks. Upon completion of the territory-wide identity card replacement exercise, planned to be in 2022, ImmD plans to engage an independent consultant to conduct a further privacy compliance audit.

/**Benefits** …..

Benefits

23. SMARTICS-2 with a new smart HKIC will bring about the following benefits –

(a) **sustain ImmD's existing effective operations into the next decade by avoiding possible large-scale system failure** that could cause severe disruption to the ROP process and massive failure of smart HKICs;

(b) **tap on latest technology for faster data retrieval and lower chip damage, hence enhancing efficiency in immigration clearance**. The time required for clearance at e-Channels for Hong Kong residents will be significantly reduced by 33% from 12 to eight seconds which translates into an increase of 50% throughput of e-Channels for Hong Kong residents[7]. This is a significant benefit to the entire community given the huge and growing volume of passenger traffic, i.e. up to 114 400 000 movements recorded from Hong Kong residents entering or leaving Hong Kong using e-Channels in 2014;

(c) **support more secure and accurate identity verification** through the new chip with higher storage capacity that will allow storage of higher resolution photo image (supporting facial recognition technology and providing a platform for alternative biometric authentication on top of fingerprint verification[8]) and updated fingerprint templates for more secure and accurate identity verification;

(d) **enhance security features of smart HKICs for better deterring forgeries** in the race against advancing technologies in the next decade, to achieve better visual appearance and improved text printing quality on the card face, and to enhance durability of card under normal usage; and

/(e) …..

[7] At present, an e-Channel can handle 5 HKIC holders (60s/12s) per minute on average. With the introduction of new smart HKICs with new chip interface, the same e-Channel can handle 7.5 passengers (60s/8s) per minute on average. The throughput has thus increased by 50%.

[8] While fingerprint verification remains a very effective biometric authentication technology, some HKIC holders cannot use it because their fingerprints are too thin or blurred. Meanwhile, the digital photo stored in the chip of the existing smart HKIC does not support facial recognition technology due to size limitation.

(e) **expand the capacity for meeting potential new public service needs** through upgrading the ageing hardware and software, including enhancement of the ROP process through various improvement initiatives such as online form filling, self-service collection kiosks with e-cabinet, and automatic record check, etc. The Office of the Government Chief Information Officer (OGCIO) is conducting a separate Technical Study[9] to review other possible uses of the smart HKICs under the MASC scheme.

SAVINGS AND COST AVOIDANCE

24. SMARTICS-2 will enable ImmD to cope with service demands in the coming ten years and improve the quality of service to the public. It will also bring about the following savings and cost avoidance –

(a) Non-recurrent cost avoidance of $3,163.91 million accumulated from 2017-18 to 2022-23, being the cost and staff resources required to upgrade the existing system in order to sustain the current business operations;

(b) Recurrent cost avoidance of $12.79 million in 2018-19 and $28.23 million from 2019-20 onwards, being an additional recurrent cost required for the maintenance of the upgraded system mentioned in item (a) above;

(c) Recurrent staff cost avoidance of $82,000 in 2017-18 and increasing to $1.76 million in 2026-27 and onwards, being the staff cost required to cope with the projected additional workload arising from handling additional workflow of the upgraded system;

(d) Recurrent realisable savings of $8.14 million in 2017-18, $39.10 million in 2018-19 and $45.64 million from 2019-20 onwards, being the annual cost required for procurement of existing smart HKICs and for maintenance of the existing system; and

/(e) …..

[9] OGCIO's separate Technical Study would review and recommend the architecture and framework for the new multi-application smart HKIC, including identifying new data to be stored into the new smart HKIC, exploring provision of new value-added services, and proposing transitional arrangement and migration strategy for existing smart HKIC applications. For any new application to be introduced, the Government will ensure the lawfulness to access Card Face Data (CFD) by the proposed application, consult relevant Legislative Council Panels on the intended use of CFD, amend the underlying legislation of the business if required, and plan for and implement data security and privacy measures.

(e) Recurrent notional savings of $409,000 in 2017-18 and $1.63 million from 2018-19 onwards, being the annual notional staff savings arising from the introduction of self-service collection kiosks with e-cabinet upon the implementation of SMARTICS-2.

Encl. 3 25. A cost and benefit analysis for SMARTICS-2 is at Enclosure 3.

FINANCIAL IMPLICATIONS

Capital Expenditure

26. It is estimated that SMARTICS-2 project will incur a capital expenditure of $1,448,786,000 over eight financial years from 2015-16 to 2022-23. The breakdown is as follows –

($'000)

	Items	**2015-2016**	**2016-2017**	**2017-2018**	**2018-2019**	**2019-2020**	**2020-2021**	**2021-2022**	**2022-2023**	**Total**
(a)	Hardware	-	11,844	22,761	192,999	18,760	20,465	20,465	3,411	290,705
(b)	Software	-	5,103	8,779	73,905	7,839	8,552	8,552	1,426	114,156
(c)	Communication Network	-	-	547	2,982	3,058	3,058	3,058	255	12,958
(d)	Implementation, Contract Staff and Consultancy Services	483	12,493	40,555	108,002	-	-	-	-	161,533
(e)	Smart Cards	-	-	33,405	112,200	112,200	112,200	112,200	-	482,205
(f)	Site Preparation and Accommodation	-	-	63,103	66,384	26,000	26,000	26,000	12,760	220,247
(g)	Publicity	-	-	1,816	3,661	4,004	4,204	2,649	2,040	18,374
(h)	Consumables and Miscellaneous	-	-	-	3,872	4,224	4,224	4,224	353	16,897
(i)	Contingency	49	2,944	17,097	56,401	17,609	17,871	17,715	2,025	131,711
	Total	**532**	**32,384**	**188,063**	**620,406**	**193,694**	**196,574**	**194,863**	**22,270**	**1,448,786**

27. On paragraph 26 (a) above, the estimated expenditure of $290.71 million is for purchasing computer hardware, such as system servers, workstations, storage devices, network equipment, card personalization machines, self-service kiosks, etc.

/28. …..

28. On paragraph 26(b) above, the estimated expenditure of $114.16 million is for purchasing system software, application software and packages.

29. On paragraph 26(c) above, the estimated expenditure of $12.96 million is the setup cost and communication network rental charges for the card replacement exercise.

30. On paragraph 26(d) above, the estimated expenditure of $161.53 million is for acquiring implementation services from external service providers and contract staff, including system analysis and design, development, testing, installation and training, etc. It also includes the acquisition of consultancy services to conduct consultancy studies, namely the PIAs and the ITSRAA at different implementation stages of SMARTICS-2.

31. On paragraph 26(e) above, the estimated expenditure of $482.21 million is for procuring about 9 455 000 customized blank smart cards, which include 8.8 million cards for the card replacement exercise, 55 000 for system testing, and 600 000 for meeting the demand of ROP offices in the first year after SMARTICS-2 is launched.

32. On paragraph 26(f) above, the estimated expenditure of $220.25 million is for site preparation of nine new identity card replacement centres[10], five existing ROP offices, a card personalization centre[11] and computer room facilities as well as for the payment of rent for the card replacement centres.

33. On paragraph 26(g) above, the estimated expenditure of $18.37 million is the publicity cost arising from the community publicity campaigns on details of the new smart HKICs and the card replacement exercise.

/34. …..

[10] Taking into account the maximum capacity and workload of the existing five ROP offices of ImmD in handling day-to-day registration work, ImmD estimates that nine additional replacement centres will be required across the territory to cope with the one-off card replacement exercise.

[11] The card personalization centre is the venue to produce cards customized to specific HKIC card holders. Steps of personalization include loading data onto the chip, printing and engraving the personal portrait and other information on the card, etc.

34. On paragraph 26(h) above, the estimated expenditure of $16.90 million is for acquiring consumables and miscellaneous items for the card replacement centres and the start-up consumables in ROP offices, including printer toner, and subscription of government common services, etc.

35. On paragraph 26(i) above, the estimated expenditure of $131.71 million represents a 10% contingency on the cost items set out in paragraphs 26(a) to 26(h).

Recurrent Expenditure

36. We estimate that the annual recurrent expenditure arising from the project will be $1.75 million in 2017-18, increasing to $59.06 million in 2018-19 and further to $84.44 million from 2019-20 and onwards. This covers the costs for hardware and software maintenance, smart cards, on-going support services, communication network, consumables and service subscription fee. Such requirement will be reflected in the estimates of the relevant years, with the breakdown as follows –

		($'000)		
	Items	**2017-18**	**2018-19**	**2019-20 & onwards**
(a)	Hardware Maintenance	-	5,037	20,147
(b)	Software Maintenance	-	2,675	10,698
(c)	Smart Card	-	30,600	30,600
(d)	On-going Support Services	-	13,735	15,985
(e)	Communication Network	1,253	5,009	5,009
(f)	Consumables	365	1,457	1,457
(g)	Service Subscription Fee	136	543	543
	Total	**1,754**	**59,056**	**84,439**

37. On paragraph 36(a) above, the estimated annual expenditure of $20.15 million is for hardware maintenance to sustain the system.

38. On paragraph 36(b) above, the estimated annual expenditure of $10.70 million is for software maintenance and licence fees to sustain the system.

/39. …..

39. On paragraph 36(c) above, the estimated annual expenditure of $30.60 million is for purchasing 600 000 blank new smart cards for the existing annual card consumption of the ROP offices.

40. On paragraph 36(d) above, the estimated annual expenditure of $15.99 million is for the on-going support service of the system.

41. On paragraph 36(e) above, the estimated annual expenditure of $5.01 million is for communication network rental charges.

42. On paragraph 36(f) above, the estimated annual expenditure of $1.46 million is for acquiring consumables, such as printer toner, etc.

43. On paragraph 36(g) above, the estimated annual expenditure of $543,000 is for subscription of government common services.

ONE-OFF TERRITORY-WIDE IDENTITY CARD REPLACEMENT EXERCISE

44. Drawing reference from the previous identity card replacement exercise, the Government will launch a one-off territory-wide identity card replacement exercise to replace the existing smart HKICs for all HKIC holders by phase from 2018 to 2022 in an orderly manner[12]. This seeks to minimise the risk of potential damage caused by disruption to public services and the impact on frontline law enforcement arising from any sudden upsurge of defective cards. If the proposed exercise commences in 2018, ImmD estimates that 8.8 million smart HKICs will be replaced in the four-year exercise.

45. A dedicated team of in-house and contract staff will be required to prepare for and to conduct the card replacement exercise. Our latest assessment is that the above would entail an estimated staff cost of some $1,500 million from 2016-17 to 2022-23. In line with the arrangement for the previous card replacement exercise, ImmD will review the staff requirement and include it in the annual Estimates of the respective year.

/IMPLEMENTATION …..

[12] As in previous replacement exercises, specified groups of HKIC holders, e.g. by year of birth, will be invited by batches to replace their smart HKICs.

IMPLEMENTATION PLAN

46. We plan to implement the proposed project according to the following schedule –

Activity	Target Completion Date
Procurement of Hardware, Software and Services	First quarter 2016
System Development and Implementation:	
System Analysis & Design	Third quarter 2016
System Development	Second quarter 2017
User Acceptance Test	Fourth quarter 2017
Site Preparation	Second quarter 2018
Training	Second quarter 2018
Production Rollout	First quarter 2018

47. Upon the rollout of SMARTICS-2, a card replacement exercise is planned to be launched in the second quarter of 2018 for four years.

PUBLIC CONSULTATION

48. We consulted the Legislative Council Panel on Security on the proposal on 6 January 2015. In response to members' questions, we provided additional information on the security and privacy protection of the future smart HKICs. The Panel further discussed the matter at its meeting of 3 February 2015 and 3 March 2015. The Panel supported in principle the Government's submission of the proposal to the Finance Committee.

/BACKGROUND …..

BACKGROUND

49. Every person in Hong Kong is required to apply for an HKIC unless exempted or excluded in accordance with the ROPO and ROPR[13]. The current SMARTICS was introduced in 2003 and the computerised paper form HKICs were replaced with (the current) polycarbonate smart HKICs through a territory-wide identity card replacement exercise from 2003 to 2007 for all HKIC holders. There are currently around nine million smart HKICs in circulation.

50. SMARTICS is an online computer system supporting registration and production[14] of smart HKICs and other immigration-related services by ImmD (e.g. identity verification for HKSAR passport applicants) as well as handling requests of verification of personal data by other government bureaux or departments for specific purposes (e.g. verification of identity and card validity by the Police, automatic validation of registration and personal information of applicants for the Elderly Health Care Voucher Scheme by the Department of Health) as allowed under the law.

51. The current smart HKIC is a polycarbonate card with embedded contact chip in which the cardholder's particulars are laser-engraved on the card surface while the templates of cardholder's fingerprints and facial image are stored in the embedded chip which is protected by cryptographic techniques. The fingerprint verification technology allows ImmD to authenticate cardholder's identity, enabling self-service immigration clearance at control points via e-Channels. Besides, as provided under the MASC scheme coordinated by the OGCIO, a personal e-Cert can be stored on the smart HKIC for performing electronic transactions for commercial and other purposes under the Electronic Transactions Ordinance (Cap. 553). The MASC also enables the provision of other government services, such as library card service, booking of leisure facilities, eHealth system service and electronic patient record sharing.

/52. …..

[13] The ROPO and ROPR provide, inter alia, that every person in Hong Kong is required to apply for an identity card, unless exempted or excluded as specified in the law, e.g. short-term visitors, children under the age of 11, the aged and the infirm. For reference, out of the 34 countries in the Organization for Economic Co-operation and Development, identity cards are issued in 28 of them (82%), where there are specified statutory requirements under which the card must be produced upon demand by the authorised personnel in 16 of these countries (57% of those countries who have issued identity cards). Amongst countries where identity cards are issued, wireless technology is adopted in Germany, the Netherlands, Chile, Finland and Sweden.

[14] Including receipt of application, record check, case assessment, personalisation and card issuance.

52. In March 2010, ImmD engaged an external consultant to conduct its third Information Systems Strategy (ISS-3) Review. On completion of the review, the ISS-3 consultant recommended that ImmD, amongst other things, implement SMARTICS-2 to address the obsolescence of hardware and software of the existing SMARTICS and cater for new business needs. SMARTICS-2 is part of the eight strategic information technology projects formulated under the ISS-3 Review to be implemented in a structured programme. The eight ISS-3 projects are –

(a) New Information Technology Infrastructure[15];

(b) Immigration Control System[16];

(c) SMARTICS-2;

(d) Next Generation Electronic Passport System;

(e) Visa Automation System;

(f) Assistance to Hong Kong Residents, Births, Deaths & Marriage, Right of Abode Decision Support System;

(g) Enforcement Case Processing System; and

(h) Human Resources Management System.

53. The eight ISS-3 projects are inter-related and essential to ImmD's mission-critical operations. It is of paramount importance that they are implemented in full so as to achieve synergy and ensure the sustainability of ImmD's services. Implementation of ISS-3 would also generate department-wide service improvement opportunities.

Security Bureau
April 2015

[15] A funding of $862.20 million was approved on 9 December 2011 for the development of the project vide FCR(2011-12)56.

[16] A funding of $912.22 million was approved on 8 February 2013 for the development of the project vide FCR(2012-13)67.

Additional Information on the Multi-dimensional Safeguards for the Proposed New Chip Interface

Introduction

To strengthen the data protection for the new smart HKIC, multi-dimensional security measures elaborated below will be in place for the proposed new chip interface.

Security Features

New chip of distinct ISO standard for secured documents

2. Radio Frequency Identification (RFID)[1] is a collective term referring to a wide range of wireless communication devices adhering to a number of different distinct standards. The proposed new smart HKIC will be designed strictly in accordance with ISO 14443 (type A or B), a proven and internationally adopted standard for smart card chips for secured documents, which supports a close communication range of around 10 cm. It is distinct from other RFID standards and applications, such as those RFID tags for item labeling (ISO 15693) and warehouse management (ISO 18000-6), electronic seals for cargo containers (ISO 18185), etc., which support a much longer communication range of up to hundreds of meters for entirely different purposes, such as tracking of goods, but usually have little or no protection for the information stored.

Access control and two-level authentication

3. The following security and privacy protection considerations are taken into account to ensure trusted and secured wireless communication and data transmission between the chip and the reader –

(a) access to chip must be initiated by the cardholder;

(b) identity of the chip and the reader must be defined and mutual authentication must be required before communication; and

(c) all communication and data transmission must be encrypted throughout the process.

/4. …..

[1] RFID widely covers various type of wireless communication device in compliance with respective standards.

4. Against the aforesaid considerations, the chip in the proposed new smart HKIC will be a passive type, i.e. not powered by any standalone battery. Without power, it is not able to send out any signal by itself. That means the wireless data transmission function will always be off. Reading of chip data through wireless data transmission will only start to function if all of the specific steps outlined below are successfully carried out –

(I) the smart HKIC card is directly placed onto an optical card reader[2] (the reader) authorised with certificate and equipped with the specific algorithm to generate a random encrypted key from a "key text string[3]" captured optically from the card face, with the side of the smart HKIC on which the "key text string" is printed facing towards the optical card reader;

(II) if the "key text string" is successfully captured by the authorised reader (in the manner of a computer scanner), the reader will generate a real-time, one-off encrypted key based on the captured "key text string" and the specific algorithm of the authorised reader;

(III) the encrypted key generated by the reader will be ***authenticated*** by the chip, requesting the chip to enable a one-on-one, exclusive encrypted communication channel;

(IV) only if the encrypted key is authenticated by the chip, the encrypted communication channel between the chip and the reader will be established. It is worth noting that even after the encrypted communication channel is successfully established, the wireless data transmission function of the chip remains turned off up to this point, i.e. no data stored in smart HKIC chip will be transmitted to the reader. The data transmission function will only be activated after further authentication;

(V) after the encrypted communication channel has been established through steps (I) to (IV) above, the reader will need to submit a second, different encrypted key to the chip for ***authentication***. **Only after successful authentication of the second key by the chip will the data transmission function be turned on, and then data be read from the smart HKIC chip by the reader**; otherwise the data transmission function will remain turned off at all times.

Annex See Annex for a flowchart illustration of these steps.

/5. …..

[2] An optical card reader is a device that supports optical scanning of the card face and reading the smart card chip.

[3] The "key text string" is composed of certain information printed on the smart HKIC card face and cannot be used to uniquely identify a particular person, e.g. part of HKIC number plus date of issue of the HKIC.

5. The safeguards embedded into the above two-level authentication process are designed to ensure that there is no "passive" or "remote" reading of chip data. The key features are highlighted below.

(A) Access control for wireless communication

6. Successful capturing of the "key text string" printed on the card face by an authorised reader (at **Step I** above) is a "pre-requisite" to activating the wireless data transmission function of the chip. Otherwise, the chip will not respond to any communication request. Cardholders take control over initiating the authentication process by placing the card directly onto an authorised reader. In other words, if the card is stored inside a wallet or purse, garments or however otherwise concealed, no communication with the chip will be activated as the wireless data transmission will remain turned off. Indeed, even if the card is taken out in the open but not placed correctly (e.g. not with the "key text string" facing the reader) and within 2 cm from an authorised reader, the "key text string" cannot be successfully captured and the encryption process and hence wireless communication will not begin at all (stopped at **Step I** above).

7. The above procedure, generally known as Basic Access Control (BAC), is a proven technology which has been adopted in overseas jurisdictions for many years. More sophisticated technologies, such as Supplemental Access Control (SAC) or Password Authenticated Connection Establishment (PACE), have also emerged over the years[4]. The Immigration Department will ensure that the latest and proven technology is adopted for the new smart HKIC.

(B) Authorised readers

8. As an additional safeguard, under SMARTICS-2, only optical card readers authorised with certificate and equipped with the specific algorithm to generate a random encrypted key from a "key text string" captured optically from an HKIC will be able to activate the wireless data transmission process. Even if a party has knowledge of the "key text string" of an HKIC (e.g. by means of the photocopy of that HKIC), it is not possible for the party to initiate any wireless data transmission without an authorised reader (stopped at **Step II** above).

/(C) …..

[4] Some countries have already issued personal identification documents (e.g. identity cards, electronic passports) supporting SAC/PACE technology, e.g. Germany, Switzerland, Republic of Kosovo, Moldova, Bosnia and Herzegovina.

(C) Non-unique Key Text String

9. To ensure no possible tracking of individuals through unauthorised wireless data transmission, the "key text string" on the HKIC will be non-unique, drawing reference to the model adopted in the German identity cards[5]. That means even in the extremely unlikely, hypothetical situation where a party had unlawful access to both the "key text string" and an authorised reader, the successful completion of **Steps I to III** above will not reveal an individual's identity.

(D) Real-time communication session

10. Each one-on-one, exclusive encrypted communication channel (established after successful completion of **Steps I to III** above) between the smart HKIC chip and the reader is only valid for a one-off session, and the communication channel will no longer exist after the smart HKIC chip has been taken away from the reader. That means even if an encrypted communication channel has been established with a card before, the second time when the same card goes near the same reader, the encrypted communication channel will not be established automatically again unless **Steps I to III** are repeated successfully (i.e. unless the cardholder takes out the card again and places it on the reader as required).

(E) Exclusive communication

11. To address concerns about eavesdropping, the encrypted communication channel established through mutual authentication in **Steps I to III** above will be one-on-one and exclusive. That means only the successfully authenticated reader can read from the chip. Other readers, even put close to the chip when a channel is established, will not be able to read from the chip.

/(F) …..

[5] This feature is similar to that adopted in German identity card, in which a non-unique six-digit number printed on card face is used as the "key text string".

(F) Proven encryption technology for personal IDs

12. Access to the data stored in the chip through **Step IV and V** above requires proper (second) authentication with strong encryption technologies (including Public Key Infrastructure, asymmetric and symmetric key encryption algorithms such as the Rivest-Shamir-Adleman cryptosystem, Elliptic Curve Cryptography and Advanced Encryption Standard) for protecting information confidentiality. The technique, which is also known as Extended Access Control or Mutual Authentication, is a proven security feature widely adopted by many overseas jurisdictions, including German identity cards, and electronic passports issued by Germany, Czech Republic, Switzerland and Italy. No skimming and eavesdropping of the personal information will be possible, and only an authorised reader is allowed to read the personal information from the smart HKIC chip. That means even if one is able to detect signals within proximity when wireless data transmission with the chip is ongoing (after successfully going through **Steps I to V** above), one can only detect "scrambled" signals which have no meaning at all.

Annex

Non-unique Key Text String on HKIC

Step (I) –
Place smart HKIC on **authorised optical card reader**

Within 2cm

Chip

Authorised Optical Card Reader

Step (II) –
Reader captures **non-unique key text string**, then generates ***1st encrypted key*** for **access control**

Algorithm

Algorithm

Reader Processor

Step (III) –
Chip ***authenticates*** 1st encrypted key
(The chip supports a close communication range of around 10 cm in accordance with ISO 14443)

Step (IV) –
Real-time and **exclusive encrypted communication channel** established between chip and reader

Step (V) –
Reader submits ***2nd encrypted key*** to turn on data transmission upon ***authentication*** by chip with **proven encryption**

Summary of the First Privacy Impact Assessment Conducted on SMARTICS-2 on Card Interface, Card Materials and Security Features on Card Body

Area	Potential Risk	Assessment/Recommendations
Card interface	There may be skimming, eavesdropping and cloning attacks on the personal data stored in Hong Kong Identity Card (HKIC).	Through inspection of Selected Business System Options and Function Specification, we noted that the following logical access protection measures such as Basic Access Control (BAC) and mutual authentication are proposed to be applied for accessing the data stored in the chip of HKIC. We noted that these logical access protection measures are effective means to prevent unauthorised access to the personal data stored in HKIC through contactless or contact interface. We recommend that Immigration Department (ImmD), during the later stages of SMARTICS-2, should assess the effectiveness of the proposed logical access protection measures. We also recommend that ImmD continue to monitor the evolving technology of the logical access protection measures during the design and implementation of SMARTICS-2. **No exception noted.**
	If the contactless interface of the dual interface HKIC is compromised, sensitive personal data that supposedly can only be accessed through the contact interface may be leaked through the contactless interface.	Since dual interface uses only one chip set, without proper control, personal data that supposedly can only be accessed through the contact interface may be leaked through the contactless interface if the latter is compromised. Through inspection of Selected Business System Options and Function Specification, we noted that dual interface card is proposed to be applied to the chip of HKIC, and logical access protection measures such as BAC and mutual authorization will be implemented to prevent the contactless interface from being compromised.

Area	Potential Risk	Assessment/Recommendations
		We noted that these logical access protection measures are effective means to prevent unauthorised access to the personal data stored in HKIC through the contactless interface. **No exception noted.**
Card Materials /Security Features on Card Body	Counterfeit HKIC is produced to degrade the integrity of HKIC.	Through inspection of Selected Business System Options, we noted that security features are proposed to be applied to the card body of HKIC to prevent production of counterfeit HKIC. <u>Protection already exists on current HKIC:</u> 1. Guilloches 2. Optical Variable Ink 3. Relief 4. Rainbow printing 5. Multiple Laser Image 6. Micro printing 7. UV image 8. Invisible Personal Information in the holder's portrait <u>New security features are considered to be applied on SMARTICS-2:</u> 1. See-through windows 2. Hologram effect 3. Lenticular effect 4. Full-color UV image We noted that the proposed material is a laser-compatible polycarbonate material which allows the security feature to be added to the card body.

Area	Potential Risk	Assessment/Recommendations
		Through our review of the current practices on the card materials and security features on card body of smart ID cards, we noted that the German ID card is relevant to be used as a bench mark. The German ID card was introduced in November 2010 with an RFID chip that is embedded into the card. Further there are no significant issues identified regarding the card materials and the security features on card body. We recommend that at the later stages, ImmD implement advanced security features on the card body (which should be made with multi layers and materials which allow laser printing of security features, such as the polycarbonate proposed in the Feasibility Study) and perform testing to ensure the features are properly applied to the card body. **No exception noted.**

Cost-Benefit Analysis for the Implementation of the Next Generation Smart Identity Card System (SMARTICS-2)

($'000)

	2015-16	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26	2026-27	2027-28	Total
Cost														
Non-recurrent														
Capital Expenditure	532	32,384	188,063	620,406	193,694	196,574	194,863	22,270	-	-	-	-	-	1,448,786
Staff Cost	14,956	39,330	38,840	219,211	235,236	235,236	235,236	19,603	-	-	-	-	-	1,037,648
Contract Staff Cost				110,088	120,096	120,096	120,096	10,008						480,384
Sub-total	15,488	71,714	226,903	949,705	549,026	551,906	550,195	51,881	-	-	-	-	-	2,966,818
Recurrent														
Expenditure	-	-	1,754	59,056	84,439	84,439	84,439	84,439	84,439	84,439	84,439	84,439	84,439	820,761
Staff Cost	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Sub-total	-	-	1,754	59,056	84,439	84,439	84,439	84,439	84,439	84,439	84,439	84,439	84,439	820,761
Total Cost	**15,488**	**71,714**	**228,657**	**1,008,761**	**633,465**	**636,345**	**634,634**	**136,320**	**84,439**	**84,439**	**84,439**	**84,439**	**84,439**	**3,787,579**
Saving														
Non-recurrent														
Cost Avoidance	-	-	242,961	938,191	641,124	641,324	639,769	60,542	-	-	-	-	-	3,163,911
Sub-total	-	-	242,961	938,191	641,124	641,324	639,769	60,542	-	-	-	-	-	3,163,911
Recurrent														
Cost Avoidance	-	-	-	12,788	28,226	28,226	28,226	28,226	28,226	28,226	28,226	28,226	28,226	266,822
Staff Cost Avoidance	-	-	82	327	327	327	327	327	532	1,218	1,517	1,763	1,763	8,510
Realisable Savings	-	-	8,141	39,100	45,637	45,637	45,637	45,637	45,637	45,637	45,637	45,637	45,637	457,974
Notional Savings	-	-	409	1,634	1,634	1,634	1,634	1,634	1,634	1,634	1,634	1,634	1,634	16,749
Sub-total	-	-	8,632	53,849	75,824	75,824	75,824	75,824	76,029	76,715	77,014	77,260	77,260	750,055
Total Savings	**-**	**-**	**251,593**	**992,040**	**716,948**	**717,148**	**715,593**	**136,366**	**76,029**	**76,715**	**77,014**	**77,260**	**77,260**	**3,913,966**
Net Savings	**-15,488**	**-71,714**	**22,936**	**-16,721**	**83,483**	**80,803**	**80,959**	**46**	**-8,410**	**-7,724**	**-7,425**	**-7,179**	**-7,179**	**126,387**
Net Cumulative Savings	**-15,488**	**-87,202**	**-64,266**	**-80,987**	**2,496**	**83,299**	**164,258**	**164,304**	**155,894**	**148,170**	**140,745**	**133,566**	**126,387**	**-**
