LC Paper No. CB(2)534/14-15(03)

For discussion
on 6 January 2015

Legislative Council Panel on Security

The Next Generation Smart Identity Card System

PURPOSE

This paper seeks Members' support for the proposal to implement the Next Generation Smart Identity Card System (SMARTICS-2) and the introduction of the next generation smart Hong Kong Identity Card (HKIC) through a one-off territory-wide identity card replacement exercise to replace the existing smart HKICs for all HKIC holders from 2018 to 2022.

BACKGROUND

2. The current Smart Identity Card System (SMARTICS) was introduced in 2003 when the computerised paper form HKICs were replaced with the polycarbonate smart HKICs through a one-off territory-wide identity card replacement exercise from 2003 to 2007 for all HKIC holders. There are currently around nine million smart HKICs in circulation.

3. SMARTICS is an online computer system supporting registration and production [1] of HKICs and other immigration-related services by the Immigration Department (ImmD) (e.g. identity verification for HKSAR passport applicants, etc.), as well as handling requests of verification of personal data by other government bueaux or departments for specific purposes (e.g. verification of eligibility for government-related initiatives, automatic validation of registration and personal information of applicants for the Elderly Health Care Voucher Scheme by the Department of Health, outstanding fees collection, etc.) as allowed under the law.

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

4. The current smart HKIC is a contact chip-enabled polycarbonate card 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 the ImmD to authenticate cardholder's identity, enabling self-service immigration clearance at control points via e-Channels.

5. Besides, as provided under the Multi-Application Smart Identity Card (MASC) scheme coordinated by the Office of the Government Chief Information Officer (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 scheme 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. All these services are provided on a voluntary basis upon cardholder's consent.

6. In March 2010, the ImmD engaged an external consultant to conduct its third Information Systems Strategy (ISS-3) Review. The ISS-3 review recommended the ImmD to revamp its information technology infrastructure (ITI) to upkeep the ImmD's service quality and enhance its handling capacity to cope with the substantially growing service demands. Members of this Panel endorsed the proposal of the ImmD to develop a new ITI at the meeting on 7 November 2011 (LC Paper No. CB(2)164/11-12(05)). The ITI project received funding support from the Finance Committee on 9 December 2011.

7. Riding on the new ITI, the ISS-3 consultant recommended the ImmD to gradually replace its various existing core computer systems, which were developed and implemented between late 1990s and early 2000s and hence are becoming obsolete approaching the mid-2010s, in order to ensure quality and uninterrupted delivery of the ImmD's critical services to the public. Amongst other things, the ISS-3 consultant recommended implementation of SMARTICS-2 to address the obsolescence of hardware and software of the existing SMARTICS and to cater for possible new business needs. Following the recommendation, the ImmD has completed a feasibility study on the implementation of SMARTICS-2 in October 2014. In addition to implementing a new computer system to replace the existing SMARTICS, the feasibility study also recommended that the opportunity be taken to introduce enhancements to smart HKICs through a one-off territory-wide identity card replacement exercise.

JUSTIFICATIONS

SMARTICS-2

8. As with other major computer systems, SMARTICS was designed for optimal use for about 10 years. Being developed in the early 2000s, its hardware and software are becoming obsolete. It is becoming increasingly difficult 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 ImmD has made strenuous effort in securing extension of the expiry date of the system maintenance agreements from originally December 2013 to end of 2018 at most. Further extension is considered not pragmatic from the perspective of system health and reliability due to the prolonged use of outdated technologies.

9. Without suitable and ongoing maintenance and technical support, the risk of system failure which would lead to serious and large-scale disruption of critical public service will continue to increase. In the event of system failure, apart from suspension of registration of persons (ROP) services including the application, processing and production of smart HKICs, other government systems which depend on SMARTICS to operate, including Electronic Passport System for the processing of HKSAR passport applications, etc., will also be affected. Hence, there is an imminent need to replace the existing system. Moreover, system replacement also provides a window for catering new business demands (e.g. enhancing security features and chip technologies of smart HKICs and enhancing the ROP process, etc.).

10. Apart from upgrading system hardware and software to maintain system sustainability, to ensure smooth business operation and to meet new business needs, SMARTICS-2 would also make the ROP process more efficient. Improvement initiatives on the ROP process that may be introduced under SMARTICS-2 include online form filling, automatic record check for application assessment and self-service collection kiosks with e-cabinet, etc. Subject to detailed system design to be conducted, these measures will provide better service to the public through higher operation efficiency and will achieve cost effectiveness. As a result, the overall processing time for HKIC registration and production will be shortened.

New Smart HKIC

11. There is no expiry date for smart HKICs[2], but the serviceable lifespan of the card material, as guaranteed by the manufacturing contractor and subsequently confirmed by an independent laboratory test commissioned by the ImmD, is 10 years under normal usage. That means the designed serviceable lifespan of smart HKICs issued between 2003 and 2007 are due to expire between 2013 and 2017. Although it does not mean that smart HKICs would break or malfunction by default once the ten-year mark after they were issued is reached, the likelihood of them requiring replacement would continue to increase over time.

12. Moreover, although the number of forged smart HKICs detected in recent years has continued to remain on the low side, there have been cases of seizure of forged smart identity cards in Europe with card materials and security features similar to our existing smart HKICs. We expect that as technology continues to advance, cases of forgery of our smart HKICs may become more prevalent if we do not introduce any new security features and chip architecture technology.

13. As recommended by the feasibility study, we agree that the opportunity of implementing SMARTICS-2 should be taken to introduce the next generation smart HKIC as well, for the following benefits –

(a) Avoiding possible massive failure. As mentioned in paragraph 11 above, smart HKICs issued since 2003 are gradually exceeding their serviceable lifespan, which means that they are becoming more susceptible to damages and malfunction. To introduce a new smart HKIC to replace the existing ones in an orderly fashion will avoid circumstances where a large number of smart HKICs failing together in a short period of time, in which case the ImmD might not be able to handle all replacement applications within the normal pledged timeframe and in turn causing grave public inconvenience.

(b) Enhancing security features. As of today, the security features against forgeries adopted in the current smart HKIC are still effective. However, their effectiveness may deteriorate in the next decade or so. It is imperative that we keep up with the advancing technology in order to keep the forgery rate low. Apart from chip security, the ImmD also plans to

[2] Similar smart identity cards issued by other jurisdictions, including Germany, Belgium, Malaysia and the Macao SAR, are all set for replacement within 5 to 10 years of issuance for various reasons, including ensuring card durability.

enhance security features to the smart HKIC card body which will be subject to further detailed design of the new smart HKIC.[3]

(c) Improving card durability. The use of latest card material can bring about better visual appearance, improved text printing quality and increased durability of card under normal usage.

(d) Upgrading chip technology. The chip on card will be enhanced with latest technologies enabling better security and faster data retrieval by introducing an additional interface supporting the use of wireless technology[4]. The new chip will have a higher storage capacity than the current smart HKIC one, allowing storage of a higher resolution photo image (to support facial recognition technology and provide a platform for alternative biometric authentication on top of fingerprint verification[5]) and updated fingerprint templates for more secure and accurate identity verification. The new chip will also enable potential new card applications for more robust and convenient use of the smart HKIC in future. In this regard, the OGCIO is conducting a separate Technical Study[6] to review other possible uses of the smart HKIC under the MASC scheme.

---

[3] 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.

[4] To provide additional safeguard on data protection, we will consider introducing access control mechanism through optical means before enabling wireless communication of the chip. Should such access control be enabled, one would need to physically place the smart HKIC onto an optical card reader (OCR), which will capture certain unique card face data to start the communication. Such unique card face data will be transmitted to the system reading the HKIC, where the access key will be generated and verified by the HKIC and the system. The data stored in the chip can only be read once the inspection system has offered a proper access key and successful authentication. That means retrieval of data from the chip of a smart HKIC requires physical contact between that particular smart HKIC and the OCR. For the OCR to capture card face data, the card has to be placed firmly onto the OCR. For the chip reader to retrieve data from the chip, the distance between the reader and the chip has to be within about 2 cm. (This is different from the data retrieval model of an Octopus card, from which data may be retrieved even if the card is stored in a wallet or purse.) As the access key is derived from card face data of a given smart HKIC, it will not enable access to a different smart HKIC. Similar technologies to prevent "eavesdropping" have been adopted by many other jurisdictions (e.g. Germany, Malaysia, the Macao SAR, etc.) where wireless chips in smart identity cards were introduced in the past decade.

[5] While fingerprint verification remains very effective, 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.

[6] 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.

Territory-wide replacement exercise

14. Drawing reference to the previous identity card replacement exercise, a one-off territory-wide identity card replacement exercise will be implemented to replace the existing smart HKICs for all HKIC holders by phase from 2018 to 2022 in an orderly manner[7]. Since the workload of the existing five ROP offices of the ImmD in handling day-to-day registration work is already close to the maximum capacity of those offices, additional replacement centres will need to be set up for the replacement exercise. The ImmD estimates that nine replacement centres will need to be set up across the territory during the replacement exercise.

Consultation with the Office of the Privacy Commissioner for Personal Data (PCPD)

15. The ImmD will closely engage the PCPD during implementation of SMARTICS-2 to ensure that the collection, handling, storage and disclosure of personal data by the ImmD under SMARTICS-2 will be in accordance with law, and will continue to be in compliance with the data protection principles and other requirements under the Personal Data (Privacy) Ordinance (Cap. 486). Drawing reference to the experience of the first generation of SMARTICS in the early 2000s, the ImmD will commission qualified independent consultants to conduct Privacy Impact Assessment (PIA) during each critical stage of the implementation of SMARTICS-2, including feasibility study, system analysis and design, pre-implementation and post-implementation. Recommendations of each PIA and comments from the PCPD, if any, would contribute to the work of the subsequent stage in regard to the protection of personal data. The ImmD will continue to perform regular self-compliance checks, and, on the advice of the PCPD, will in due course engage an independent consultant to conduct a further privacy compliance audit after completion of the one-off territory-wide identity card replacement exercise. We have, in this regard, already been in contact with the PCPD on our plans set out above.

SAVINGS AND COST AVOIDANCE

16. The implementation of SMARTICS-2 (including the introduction of the next generation smart HKIC card through a one-off territory-wide identity card replacement exercise) will bring about the following savings and cost avoidance –

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

(a) **Non-recurrent cost avoidance** of $3,123.3 million accumulated from 2017-18 to 2022-23, being the cost required to revamp the existing system for sustaining the current business operations, as well as the cost avoidance arising from system upgrade and staff efforts which would otherwise have to be incurred by using the existing system and mode of operation for carrying out the card replacement exercise;

(b) **Recurrent cost avoidance** of $12.8 million in 2018-19 and $28.2 million from 2019-20 onwards, being an additional recurrent cost required for the maintenance of the revamped system mentioned in item (a) above;

(c) **Recurrent staff cost avoidance** of $82,000 in 2017-18 and increasing to $1.7 million in 2026-27 and onwards, being the staff cost required to cope with the growth of the projected additional workload arising from handling additional workflow of the revamped system;

(d) **Recurrent realisable savings** of $8.1 million in 2017-18, $39.1 million in 2018-19 and $45.6 million from 2019-20 onwards, being the annual cost required for procurement of existing HKIC and for the maintenance of the existing system; and

(e) **Recurrent notional savings** of $409,000 in 2017-18 and $1.6 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.

FINANCIAL IMPLICATIONS

Non-Recurrent Expenditure

17. It is estimated that the implementation of SMARTICS-2 [8] will incur a total non-recurrent expenditure of $1,448.8 million 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

[8] Including the introduction of the next generation smart HKC through a one-off territory-wide identity card replacement exercise.

(c)	Communication Network	-	-	547	2,982	3,058	3,058	3,058	255	12,958
(d)	Implementation Services	-	6,605	31,263	107,027	-	-	-	-	144,895
(e)	Contract Staff for Implementation Team	483	5,888	7,764	975	-	-	-	-	15,110
(f)	Site Preparation	-	-	46,103	40,384	-	-	-	5,760	92,247
(g)	Training	-	-	1,528	-	-	-	-	-	1,528
(h)	Consumables	-	-	33,405	114,847	115,088	115,088	115,088	241	493,757
(i)	Publicity	-	-	1,816	3,661	4,004	4,204	2,649	2,040	18,374
(j)	Accommodation	-	-	17,000	26,000	26,000	26,000	26,000	7,000	128,000
(k)	Miscellaneous	-	-	-	1,225	1,336	1,336	1,336	112	5,345
(l)	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**

Other Non-Recurrent Cost

18. A total non-recurrent staff cost of $1,462.1 million will be incurred for the planning, co-ordination, implementation of the project and conducting the one-off territory-wide identity card replacement exercise.

Recurrent Costs

19. The proposal will entail an annual recurrent expenditure of $1.8 million in 2017-18, increasing to $84.4 million from 2019-20 onwards. This covers the costs for hardware and software maintenance, smart cards, on-going support services, communication network, other 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 Cards	-	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**

ESTIMATED IMPLEMENTATION PLAN

20. The estimated schedule for implementing the proposed SMARTICS-2 [9] is as follows –

Activity	**Estimated Schedule**
Seek funding approval from the LegCo Finance Committee	First half of 2015
Tendering	Q3/2015 to Q1/2016
System Development and Implementation	
System Analysis & Design	Q2 to Q3/2016
System Development	Q3/2016 to Q2/2017
User Acceptance Test	Q2 to Q4/2017
Site Preparation	Q2/2017 to Q2/2018
Training	Q4/2017 to Q2/2018
Production Rollout	Q1/2018
Territory-wide Replacement Exercise	Q2/2018 to Q2/2022

ADVICE SOUGHT

21. Members' views are invited on our proposal to implement SMARTICS-2 [10] and on our plan to seek funding approval from the Finance Committee.

Security Bureau
December 2014

[9] Same as footnote 8.
[10] Same as footnote 8.