LC Paper No. CB(2)654/14-15(03)

For discussion
on 3 February 2015

Legislative Council Panel on Security

Supplementary Information on the Security and Privacy Protection Features of the Proposed Next Generation Smart Identity Card System

Introduction

This paper provides further information on the security and privacy protection features of the Next Generation Smart Identity Card System (SMARTICS-2).

New Chip Interface

2. The existing smart Hong Kong Identity Card (HKIC) includes a smart card chip designed for high-security use. Developed in the early 2000s, it supports a contact interface only, i.e. in order to access data from the chip, one needs to insert the smart HKIC into a card reader, in which the chip will physically connect with the reader directly to allow communication. In the past ten years, chip hardware, operating system and software technologies have seen significant advancement, such as processing speed, storage capacity, chip interface and security. Opportunity of chip hardware upgrade provides a suitable window for the corresponding and much-needed software upgrade in order to reap the benefits of technology advancement for more robust, convenient and efficient use of the smart HKIC.

3. The benefits of adopting the proposed new chip interface, safeguarded by multi-dimensional security features (see details in paragraphs 4 to 15 below), are faster data retrieval and increased durability, thereby greatly enhancing efficiency in immigration clearance. The clearance speed at e-Channels for Hong Kong residents will be drastically reduced by 33% from twelve to eight seconds. Arithmetically, this translates into an increase of

50% throughput of e-Channels for Hong Kong residents[1]. This is a significant benefit to the entire community given our huge and growing volume of passenger traffic, i.e. up to 114 400 000 movements were recorded from Hong Kong residents entering or leaving Hong Kong using e-Channels in 2014. The new chip interface, which does not require direct physical contact with the chip inside a card reader, will also reduce damages caused to HKICs due to frequent reading of cards. Despite introduction of a new interface, we will need to maintain the existing contact interface under SMARTICS-2 for transition purposes[2].

Security Features

4. There are, however, concerns over the proposed new chip interface, which makes use of radio frequency for data transmission, including whether it will render the future smart HKICs more prone to data leakage and tracking through unauthorised access to the chip. Additional information on the multi-dimensional safeguards set out in the ensuing paragraphs aims to dispel misunderstanding in this respect.

New chip of distinct ISO standard for secured documents

5. Radio Frequency Identification (RFID) 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 RFID tags for item labeling (ISO 15693) and warehouse management (ISO 18000-6), electronic

---

[1] At present, an e-Channel can handle 5 passengers (60s/12s) per minute on average. With the introduction of new smart HKICs with a 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%.

[2] Other than the computer systems in the ImmD, it may take some time for the replacement of all smart HKIC readers (around 6 000 as at end 2014 and estimated to be increased to 17 700 by end 2017) in Leisure and Cultural Services Department (for library card service and booking of leisure facilities), Food and Health Bureau and Department of Health (for eHealth System service), as well as Hospital Authority and private doctors (for electronic patient record sharing). After these services have gradually adopted the new contactless interface, the wear-and-tear of the new smart HKIC arising from using the contact interface will significantly be reduced.

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

6. 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 confirmed before communication; and
(c) all communication and data transmission must be encrypted throughout the process.

7. 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[3] (the reader) authorised with certificate and equipped with the specific algorithm to generate a random encrypted key from a "key text string"[4] 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

---

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

[4] 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.

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.

See **Annex A** for a flowchart illustration of these steps.

8. 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

9. 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).

10. 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[5]. The Immigration Department (ImmD) will ensure that the latest and proven technology is adopted for the new smart HKIC.

(B) Authorised readers

11. 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) Non-unique Key Text String

12. 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[6]. That means even in the extremely unlikely, hypothetical situation

---

[5] 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.

[6] 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".

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

13. 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

14. 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) Proven encryption technology for personal IDs

15. Access to the data stored in the chip through **Steps IV and V** above requires proper (second) authentication with strong encryption technologies (including Public Key Infrastructure, asymmetric and symmetric key encryption algorithms such as RSA, 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.

External Advices

16. As in the implementation of the existing SMARTICS, the ImmD will engage external consultants to conduct Privacy Impact Assessments (PIAs) at different stages of implementing SMARTICS-2. Each PIA report will be submitted to the Privacy Commissioner for Personal Data (PCPD) for comment. The recommendations of the consultants and the PCPD, if any, will be adopted for enhancing the implementation of SMARTICS-2. The security features design will be finalised during the next stage of implementation of System Analysis and Design (SA&D), which will be covered by the next PIA.

17. The external consultant conducting the first PIA on SMARTICS-2 has confirmed that access protection measures such as BAC and mutual authentication were effective means to prevent unauthorized access to personal data stored in the smart HKIC through contactless interface. Upon the recommendation of the consultant, the ImmD would assess the effectiveness of the proposed access protection measures during the later stages including SA&D of SMARTICS-2. 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 **Annex B**.

18. In addition to PIAs, the ImmD will also engage an independent auditor to conduct information technology security risk assessment and security audit at different stages of implementing SMARTICS-2, namely during SA&D and before and after system rollout to ensure the effectiveness of those security measures in protecting information in SMARTICS-2 and smart HKICs.

Personal Data Privacy Protection

19. Apart from the above designed security features, the existing Registration of Persons Ordinance (Cap. 177) (ROPO) and the Registration of Persons Regulations (Cap. 177A) (ROPR) also provide stringent safeguards against unlawful access to the chip on the smart HKIC and mounts tight control over the collection and use of registration of persons (ROP) data.

Prohibition of unlawful access to chip

20. 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 (of 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. At present, such facilities include *(for immigration-related facilities, which are exclusively controlled by the ImmD)* e-Channels, self-service e-Passport application kiosk, Enrolment kiosk for Macao e-Channels, and SMARTICS kiosks, and *(for non-immigration-related facilities, i.e. Card Face Data (CFD) under Multi-application Smart ID Card (MASC))* public library service, Leisure Link Self-service Kiosks, e-Health System and Public-Private Interface-Electronic Patient Record Sharing Pilot Project[7]. Moreover, Regulation 12(1B)(b) of ROPR provides that a person to whom an identity card relates has lawful authority to gain access to data specified in Schedule 5 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. 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 (HK$25,000) and to imprisonment for 2 years. The proposed new chip interface of the new smart HKIC is entirely consistent with these legal requirements. Relevant legislative provisions are extracted at **Annex C**.

---

[7] For the use of all such facilities, cardholders have to insert the card 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.

Potential new card applications

21. The MASC allows integration of other applications into the smart HKICs for users' convenience. Under the MASC, all applications are added to the smart HKICs subject to the consent of individual cardholders and compliance with the Personal Data (Privacy) Ordinance. Following the same principle, the Office of the Government Chief Information Officer is conducting a separate technical study to review other possible uses of the smart HKICs under the MASC. For any new application to be introduced, the Administration will ensure the lawfulness to access CFD by the proposed application, consult relevant Legislative Council Panels on the intended use of CFD, amend the underlying legislation(s) or regulation(s) of the business if required, and plan for and implement data security and privacy measures.

Collection of ROP information and Storage of data

22. The Commissioner of Registration collects information from individuals strictly in accordance with the requirements under Regulation 4(1)(b) of the ROPR. There will be no change under SMARTICS-2, i.e. the proposed SMARTICS-2 and new smart HKICs collect and store information no more than the existing SMARTICS and smart HKICs. Information contained in any smart HKIC, including information stored in the chip, is set out in Schedule 1 of the ROPR. Apart from gaining access to data stored in a chip, Regulation 12(1A) also provides that any person who, without lawful authority or reasonable excuse stores data in a chip, erases, cancels, alters or adds to any data in a chip, or renders a chip ineffective shall also be guilty of an offence and liable to a fine at level 4 (HK$25,000) and to imprisonment for 2 years.

Other Information

Identity Cards in OECD countries

23. Out of the 34 countries in the Organization for Economic Co-operation and Development (OECD), 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 17 of these countries (50% of all OECD countries). A summary is at **Annex D**.

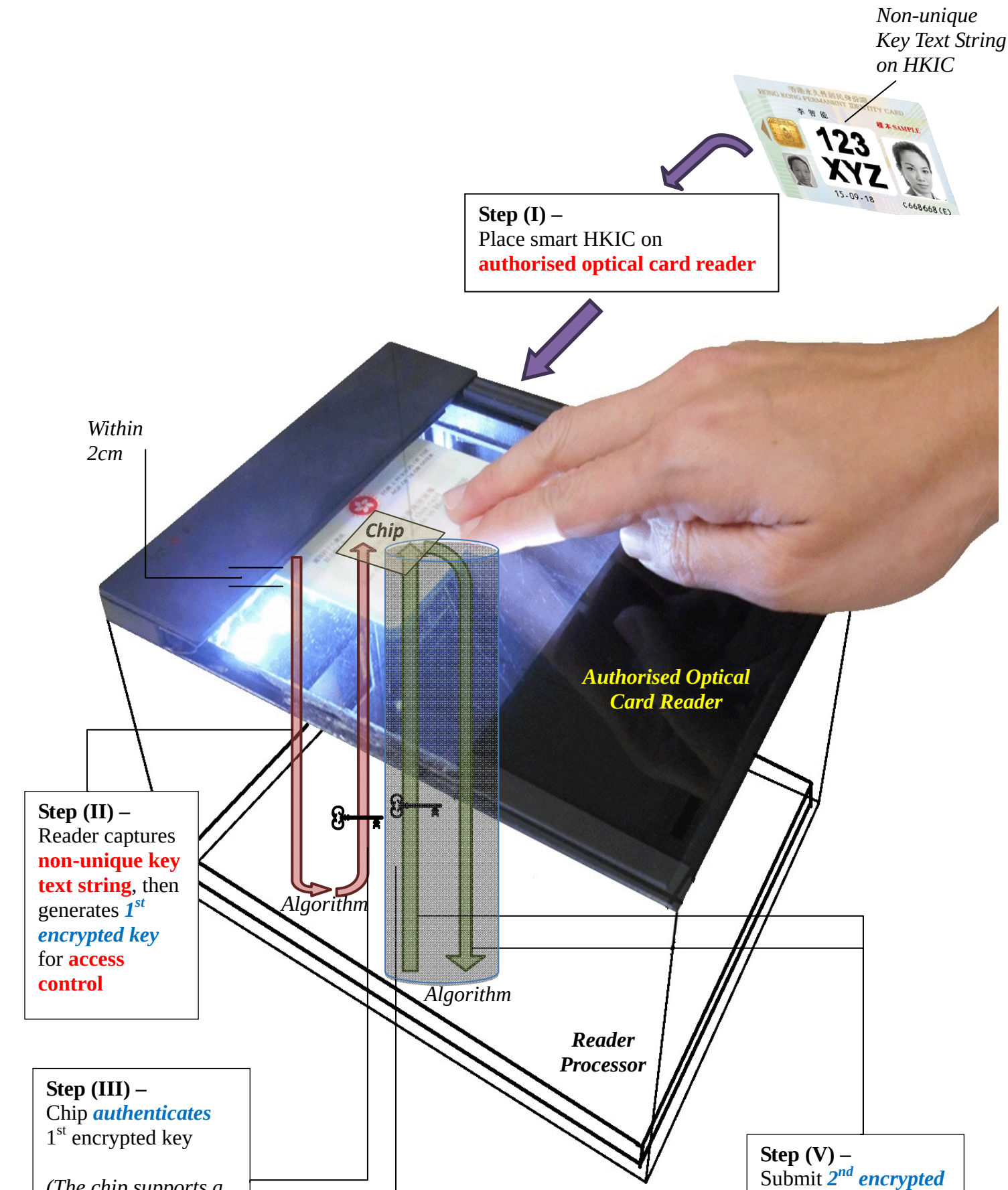
Amongst countries where identity cards are issued, wireless technology is adopted in Germany, the Netherlands, Chile, Finland and Sweden.

Card durability

24. The first batch of the smart HKICs in Hong Kong issued in 2003 would have reached 15 years of age by the year 2018. In 2012, the ImmD commissioned two independent laboratories in Europe to ascertain the durability of the existing smart HKIC, which is made up of polycarbonate material, through a series of ageing test, such as thermal, chemical, humidity, ultra violet light and dynamic bending stress tests, which aimed to simulate the extension of normal usage. Neither laboratory was able to conclude that the extended durability of the smart HKIC could go beyond 10 years within the framework of the international standards such as ISO/IEC 24789 *Identification cards – Cards service life* and ISO/IEC 10373 *Identification cards – Test methods* in testing cycles representing usage after 10 years. The ImmD will keep a close eye on the market development and take this into account during the upcoming tendering exercise.

Security Bureau
January 2015

Annex A


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) –
Establish **real-time** and **exclusive encrypted communication channel** between chip and reader
Step (V) –
Submit ***2nd encrypted key*** to turn on data transmission upon ***authentication*** with **proven encryption**

Annex B

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.**

Area	Potential Risk	Assessment/ Recommendations
Card interface	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. 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 (OVI) 3. Relief 4. Rainbow printing 5. Multiple Laser Image 6. Micro printing 7. UV image 8. Invisible Personal Information (IPI) in the holder's portrait

Area	Potential Risk	Assessment/ Recommendations
		<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. 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 Feasbility Study) and perform testing to ensure the features are properly applied to the card body. **No exception noted.**

Annex C

Chapter:	177A	Title:	**REGISTRATION OF PERSONS REGULATIONS**	Gazette Number:	9 of 2003
Schedule:	1	Heading:	**CONTENTS OF FORMS OF IDENTITY CARD**	Version Date:	12/05/2003

[regulations 2(1), 4A, 5, 11A & 12(1B)]
(9 of 2003 s. 20)

1. Every identity card shall include-

(a) the full personal name and surname of the applicant in English or in English and Chinese;

(b) the Chinese commercial code (if applicable);

(c) the date of birth of the applicant;

(d) a number for identification purposes;

(e) the date of issue of the card;

(f) a photograph of the applicant, unless the applicant is under the age of 11 years; (9 of 2003 s. 20)

(g) such data, symbols, letters or numbers representing prescribed information, particulars or data within the meaning of section 7(2A)(b) of the Ordinance as the Commissioner may determine; and (9 of 2003 s. 20)

(h) in the form of data stored in the chip in the identity card-

(i) template of the applicant's thumb-prints or other fingerprints taken under regulation 4(1)(a); and

(ii) (where the applicant does not have a right of abode in Hong Kong) the conditions of stay (including a limit of stay) imposed in relation to him under section 11 of the Immigration Ordinance (Cap 115). (9 of 2003 s. 20)

Chapter: 177A	Title:	**REGISTRATION OF PERSONS REGULATIONS**	Gazette Number:	9 of 2003
Schedule:5	Heading:	**PURPOSES, INFORMATION, PARTICULARS AND DATA REFERRED TO IN REGULATION 4A**	Version Date:	12/05/2003

[regulations 4A & 12(1B)]

	Column 1 Purposes	Column 2 Information, Particulars and Data
1.	Storage of a certificate defined in section 2(1) of the Electronic Transactions Ordinance (Cap 553) issued by the Postmaster General and recognized under section 22 of that Ordinance.	A certificate defined in section 2(1) of the Electronic Transactions Ordinance (Cap 553) issued by the Postmaster General and recognized under section 22 of that Ordinance.

(Schedule 5 added 9 of 2003 s. 22)

Chapter:	177A	Title:	**REGISTRATION OF PERSONS REGULATIONS**	Gazette Number:	9 of 2003
Regulation:	12	Heading:	**Prohibition against making alteration to identity card**	Version Date:	12/05/2003

(1A) Any person who, without lawful authority or reasonable excuse-

(a) stores data in a chip;

(b) gains access to any data stored in a chip;

(c) erases, cancels, alters or adds to any data stored in a chip; or

(d) renders a chip ineffective,

shall be guilty of an offence. (9 of 2003 s. 14)

(1B) For the purposes of subregulation (1A), a person to whom an identity card relates has lawful authority to gain access to-

(a) data specified in Schedule 1 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; or

(b) data specified in Schedule 5 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. (9 of 2003 s. 14)

Annex D

National Identity Card Policies of Organisation for Economic Co-operation and Development (OECD) Countries

	COMPULSORY identity cards Note 2	NON-COMPULSORY identity cards Note 3	NO identity cards Note 4
OECD member countries Note 1	- Belgium - Chile Note 5 - Czech Republic - Estonia - Germany Note 5 - Greece - Hungary - Israel - Korea - Luxembourg - Netherlands Note 5 - Poland - Portugal - Slovakia - Slovenia - Spain - Turkey	- Austria - Canada - Finland Note 5 - France - Iceland - Italy - Japan - Mexico - Sweden Note 5 - Switzerland - United States	- Australia - Denmark - Ireland - New Zealand - Norway - United Kingdom Note 6
Total (34)	**17**	**11**	**6**

Note 1 List of member states are referred to OECD's official website, i.e. www.OECD.org

Note 2 **Countries with compulsory identity cards** –
Under specified circumstances, the card must be produced upon demand by the authorised personnel. Alternative proof of identity, such as a driving licence, might be acceptable. The term "compulsory" may have different meanings and implications in different countries. (Source: Wikipedia)

Note 3 **Countries with non-compulsory identity cards** –
These are countries where official authorities issue identity cards to those who request them, but where it is not illegal to be without an official identity document. (Source: Wikipedia)

Note 4 **Countries with no identity cards** –
These are countries where official authorities do not issue any identity cards. When

identification is needed, e.g. passports, identity cards issued by banks, etc., or cards that are not mainly identity cards like driver's licenses can be used. (Source: Wikipedia)

Note 5 **Countries with identity cards employing contactless interface** are highlighted in GREY. Identity cards of these five countries contain contactless chip interface which supports Basic Access Control and/or related technologies.

Note 6 The Identity Documents Act 2010 reverses the introduction of identity cards in United Kingdom in 2010.

References

1. Council of the European Union, Public Register of Authentic Travel Documents online http://prado.consilium.europa.eu/EN/8391/docHome.html
2. Wikipedia hyperlink: http://en.wikipedia.org/wiki/List_of_national_identity_card_policies_by_country
3. OECD's official website, i.e. www.OECD.org