立法會
Legislative Council

Ref : FC/1/1(1)

Finance Committee of the Legislative Council

Minutes of the 46th meeting
held at Conference Room 1 of the Legislative Council Complex
on Friday, 15 May 2015, at 3:30 pm

Members present:

Hon Tommy CHEUNG Yu-yan, SBS, JP (Chairman)
Hon CHAN Kin-por, BBS, JP (Deputy Chairman)
Hon Albert HO Chun-yan
Hon LEE Cheuk-yan
Hon James TO Kun-sun
Hon CHAN Kam-lam, SBS, JP
Hon LEUNG Yiu-chung
Dr Hon LAU Wong-fat, GBM, GBS, JP
Hon Emily LAU Wai-hing, JP
Hon TAM Yiu-chung, GBS, JP
Hon Abraham SHEK Lai-him, GBS, JP
Hon Frederick FUNG Kin-kee, SBS, JP
Prof Hon Joseph LEE Kok-long, SBS, JP, PhD, RN
Hon Jeffrey LAM Kin-fung, GBS, JP
Hon Andrew LEUNG Kwan-yuen, GBS, JP
Hon WONG Ting-kwong, SBS, JP
Hon Cyd HO Sau-lan, JP
Hon Starry LEE Wai-king, JP
Dr Hon LAM Tai-fai, SBS, JP
Hon CHAN Hak-kan, JP
Dr Hon Priscilla LEUNG Mei-fun, SBS, JP
Dr Hon LEUNG Ka-lau
Hon CHEUNG Kwok-che
Hon WONG Kwok-kin, SBS

Hon IP Kwok-him, GBS, JP
Hon Mrs Regina IP LAU Suk-yee, GBS, JP
Hon Alan LEONG Kah-kit, SC
Hon LEUNG Kwok-hung
Hon Albert CHAN Wai-yip
Hon WONG Yuk-man
Hon Claudia MO
Hon Michael TIEN Puk-sun, BBS, JP
Hon James TIEN Pei-chun, GBS, JP
Hon Steven HO Chun-yin
Hon WU Chi-wai, MH
Hon YIU Si-wing
Hon Gary FAN Kwok-wai
Hon Charles Peter MOK, JP
Hon CHAN Chi-chuen
Hon CHAN Han-pan, JP
Dr Hon Kenneth CHAN Ka-lok
Hon LEUNG Che-cheung, BBS, MH, JP
Dr Hon KWOK Ka-ki
Hon Dennis KWOK
Hon Christopher CHEUNG Wah-fung, SBS, JP
Hon SIN Chung-kai, SBS, JP
Hon IP Kin-yuen
Dr Hon Elizabeth QUAT, JP
Hon POON Siu-ping, BBS, MH
Dr Hon CHIANG Lai-wan, JP
Ir Dr Hon LO Wai-kwok, BBS, MH, JP
Hon CHUNG Kwok-pan
Hon Christopher CHUNG Shu-kun, BBS, MH, JP
Hon Tony TSE Wai-chuen, BBS

Members absent:

Hon Vincent FANG Kang, SBS, JP
Hon WONG Kwok-hing, BBS, MH
Hon Ronny TONG Ka-wah, SC
Hon Paul TSE Wai-chun, JP
Hon NG Leung-sing, SBS, JP
Hon Frankie YICK Chi-ming
Hon MA Fung-kwok, SBS, JP
Hon CHAN Yuen-han, SBS, JP

Hon Kenneth LEUNG
Hon Alice MAK Mei-kuen, JP
Hon KWOK Wai-keung
Dr Hon Fernando CHEUNG Chiu-hung
Dr Hon Helena WONG Pik-wan
Hon Martin LIAO Cheung-kong, SBS, JP
Hon TANG Ka-piu, JP

Public officers attending:

Ms Elizabeth TSE Man-yee, JP	Permanent Secretary for Financial Services and the Treasury (Treasury)
Ms Esther LEUNG, JP	Deputy Secretary for Financial Services and the Treasury (Treasury) 1
Mr Alfred ZHI Jian-hong	Principal Executive Officer (General), Financial Services and the Treasury Bureau (The Treasury Branch)
Mr John LEE Ka-chiu, PDSM, PMSM, JP	Under Secretary for Security
Mr Billy WOO	Principal Assistant Secretary for Security (D)
Mr David CHIU Wai-kai, IDSM	Assistant Director of Immigration (Personal Documentation)
Mr Raymond LOK Wai-man	Assistant Director of Immigration (Information Systems)
Miss Caroline FAN Mei-hing	Chief Systems Manager (Technology Services), Immigration Department

Clerk in attendance:

Ms Anita SIT	Assistant Secretary General 1

Staff in attendance:

Mr Derek LO	Chief Council Secretary (1)5
Mr Daniel SIN	Senior Council Secretary (1)7
Mr Frankie WOO	Senior Legislative Assistant (1)3
Ms Michelle NIEN	Legislative Assistant (1)5
Miss Yannes HO	Legislative Assistant (1)6

Item No. 1 – FCR(2015-16)7
CAPITAL WORKS RESERVE FUND
HEAD 710 – COMPUTERISATION
Immigration Department
New Subhead "Next Generation Smart Identity Card System"

The Committee continued with the deliberation on the item FCR(2015-16)7 which was carried over from the meeting on 8 May 2015. The item sought the Committee's approval of a new commitment of $1,448,786,000 for the proposed Next Generation Smart Identity Card System ("SMARTICS-2").

Technical problems in using smart identity cards

2.   Mr Charles MOK said that there were reports of mutual interference when a smart identity card, which used Radio Frequency Identification ("RFID") technology, was stacked with other cards, such as Octopus Card, using the same technology.   He asked how the Administration would tackle such problem which might occur in SMARTICS-2.   Mr SIN Chung-kai and Mr LEE Cheuk-yan raised a similar query.

3.   Assistant Director of Immigration (Information Systems) ("AD of Imm(IS)") said that the degree of interference could be reduced significantly by staggering RFID cards similarly embedded with ISO 14443-compliant chips. The Administration would also conduct tests on the effectiveness of other available means (such as a specially-designed card holder) that would minimize interference between cards, and would publicize the proper use and storage of smart identity cards when SMARTICS-2 was launched as needed.

Security and reliability issues of SMARTICS-2

4.   Mr Charles MOK noted that the proposed SMARTICS-2 would adopt the Basic Access Control technology to protect data security of the new smart identity cards.   He asked if the Administration would consider using more sophisticated and secured technology, such as Supplemental Access Control or Password Authenticated Connection Establishment mechanisms, instead.   AD of Imm(IS) assured members that the Administration would adopt the latest and proven data security technology for SMARTICS-2.

5.   Mr CHAN Chi-Chuen asked whether the Immigration Department would solely be responsible for loading cardholders' personal data into blank smart identity cards.   AD of Imm(IS) confirmed that only the authorized Immigration Department staff would handle the loading of cardholders' personal

data into blank smart identity cards in a secured area of the Immigration Department.

6.　　　　Mr Dennis KWOK expressed concern about the physical location of the repository for holding personal data that were stored in the smart identity cards, and how secure the relevant facilities were.　AD of Imm(IS) responded that the database of personal data was located in a high-security area inside the Immigration Department headquarters.

7.　　　　Mr Gary FAN noted from media sources that the contractor currently engaged to produce the Hong Kong Special Administrative Region ("HKSAR") passports was a majority-owned subsidiary of the Liaison Office of the Central People's Government in HKSAR ("Liaison Office"), and that the contractor might be involved in the design, development, installation and subsequent management and maintenance of SMARTICS-2.　He asked how the Administration would ensure that no personal data of smart identity cardholders would be passed to the Liaison Office.

8.　　　　Under Secretary for Security ("US for S") replied that the production of HKSAR passports and Hong Kong Identity Cards involved completely different procedures.　SMARTICS-2 would be implemented through open tender and any company, local or overseas, could participate in bidding for the contract.　There were established tendering procedures and monitoring mechanism and the tender results were subject to approval of the Central Tender Board.

9.　　　　Mr SIN Chung-kai expressed concern about the possibility that a person could read information stored in a smart identity card from a distance with a device employing RFID technology.　He asked how far above a card reader should the smart identity card be placed before data from the card could be read.

10.　　　　US for S said that to access information, the smart identity card with the face printed with the "key text string" must be placed within two centimetres on the authorized optical card reader.　This would allow the optical card reader to capture optically the "key text string" from the identity card to generate an encrypted key.　After the subsequent mutual authentication between the smart identity card and the optical card reader, an encrypted communication channel would be established.　Before accessing the information stored in the smart identity card, a second, separate mutual authentication between the smart identity card and the optical card reader would be performed.　The chip in the smart identity card supported a close communication range of around 10 centimetres.

11. <u>US for S</u> and <u>AD of Imm(IS)</u> supplemented that only optical card readers authorized with certificate and equipped with the specific algorithm to generate a random encrypted key from a "key text string" captured optically from an identity card would be able to establish an encrypted communication channel. Only after successful second mutual authentication between the smart identity card chip and the optical card reader, the data transmission function would be turned on, and then the information could be read from the smart identity card chip. The question of passive or remote reading of information stored in a new smart ID card with RFID technology would not arise.

12. <u>Dr KWOK Ka-ki</u> asked if it was technically possible to decrypt and read off data from the proposed new smart identity card without an authorized reader, or using a hacked device. <u>AD of Imm(IS)</u> said that the proposed new smart identity cards would adopt a bi-level encryption mechanism and the possibility of someone, without being authorized, reading information stored in the smart identity card chip would not arise. To enable access to information in a new smart identity card chip, it would be necessary for the cardholder to initiate the process by physically placing the card onto an optical card reader. There had not been any reports about access to information stored inside the chip of a smart card without the knowledge of the cardholder.

<u>Tendering of the Next Generation Smart Identity Card System</u>

13. <u>Mr CHAN Chi-Chuen</u> noted that $482.21 million would be used for procuring customized blank smart identity cards. He asked whether the cards were readily available in the market or whether they had to be custom-manufactured on demand. <u>Mr CHAN</u> also asked whether the SMARTICS-2 system hardware and the blank smart identity cards would be sourced from the same supplier.

14. <u>US for S</u> explained that the proposed new system and smart identity cards would be procured under the government's tendering process. <u>US for S</u> added that the tender for SMARTICS-2 would be designed in such a manner as to encourage more companies to participate in implementing different components of the system. In response to Mr CHAN Chi-chuen, <u>AD of Imm(IS)</u> supplemented that the current smart identity cards were supplied by a local company but the technology was European-based.

15. <u>Mr Albert CHAN</u> asked what precaution would be introduced in the tendering process to ensure that the contracts would not be awarded to the same few contractors. He also asked whether there was certain technology or

equipment required for SMARTICS-2 that could not be supplied to Hong Kong due to their sensitivity or strategic nature.

16.   AD of Imm(IS) said that detailed system specifications would be set out clearly in the tender documents which would be available to all suppliers and contractors, so that any interested company could participate in the tendering process. AD of Imm(IS) supplemented that the smart identity card technology was quite commonly in use in a number of countries. The technology and equipment should be readily available in the market.

17.   Mr WU Chi-wai noted that the Administration would put the acquisition of software for the system and the implementation of it under separate tenders. He enquired how the Administration would ensure compatibility among different components of the proposed system.

18.   Chief System Manager (Technology Services) ("CSM(TS)") said that SMARTICS-2 needed to be tailor-designed to match various steps in the workflow of the Immigration Department for processing identity card applications and performing system testing, including compatibility among different components to   be conducted during the implementation.

Permanent resident status

19.   Mr Dennis KWOK noted cases where expatriates' children born in Hong Kong but had resided overseas for an extended period, encountered difficulties when applying for a smart identity card or replacement card after returning to settle in Hong Kong. Mr KWOK queried if it was the Administration's objective to reduce the number of non-Chinese citizens with permanent resident status gradually.

20.   Assistant Director of Immigration (Personal Documentation) ("AD of Imm(PD)") responded that children born in Hong Kong might be entitled to the Hong Kong permanent resident status in accordance with the Basic Law and the Immigration Ordinance (Cap. 115). However, non-Chinese citizens who had been absent from Hong Kong for a continuous period of not less than 36 months might lose the status of a permanent resident and the right of abode in Hong Kong. AD of Imm(PD) supplemented that a person who had lost the right of abode by operation of the Immigration Ordinance (Cap. 115) would still enjoy the right to land in Hong Kong, and would become a permanent resident and enjoy the right of abode in Hong Kong again if he or she could fulfill the relevant conditions. There were also established appeal mechanisms against the decision of the Director of Immigration. AD of Imm(PD) said that members could refer specific cases to the Immigration

Department for follow-up. He assured members that it was not the intention of the Administration to deny any person of their right of abode in Hong Kong or permanent resident status.

Serviceable lifespan of the proposed smart identity card system

21. Mr Gary FAN noted that the current smart identity card system, which would have to be replaced under the funding proposal, was only introduced in 2003. He enquired about the expected serviceable lifespan of the proposed SMARTICS-2 and, if it was similar to that of the current one, whether it would be cost-effective. Dr KWOK Ka-ki raised a similar query.

22. US for S and AD of Imm(IS) said that there was no fixed operational lifespan for SMARTICS-2, although in considering tenders, additional credits would be given to bids which offered service maintenance and technical support for periods longer than 10 years. They said that given the rapid change in technology, suppliers might not be willing to offer a product maintenance and technical support for a period of more than ten years. Inevitably, component parts of system hardware might go out of stock after the expiry of contract service period, rendering repair and maintenance difficult.

23. Mr Alan LEONG cast doubt on the urgency of the funding proposal and the risk of a major system failure should there be delay in the funding process. He commented that the Administration had deployed similar arguments to justify funding for the acquisition of air traffic control system for the Civil Aviation Department and fixed-wing aircraft for the Government Flying Services several years before. Both projects were subsequently delayed rather significantly, but there were no reports of serious disruption to services of the two departments.

24. US for S said that the existing smart card system was designed for optimal use for about ten years. It has become increasingly difficult to secure system maintenance and technical support due to limited and dwindling supply of the obsolete technologies and spare components in the market. He added that the replacement of the existing smart identity card system was not a sudden idea, as SMARTICS-2 was one of the eight strategic information technology projects recommended in the third Information System Strategy Review conducted in March 2010.

25. Mr Albert HO asked whether the Administration could simply extend the operational lifespan of the current smart identity card system for, say, five more years without replacing the whole system and without augmenting the current scope of service. US for S explained that extending the existing

SMARTICS would not be cost-effective. Not only would it involve higher maintenance cost, such approach might also be impractical because some of the core components parts of the current system would eventually be out of stock and no longer manufactured. The obsolete software would eventually be operated without maintenance support.

26.   Mr Michael TIEN queried about the consequence of continued operation of the current smart identity card system beyond the warranty or maintenance contract period. US for S and AD of Imm(IS) replied that extra expenditure would be incurred from increasing rate of repair or maintenance works due to more frequent failure or breakdown of hardware components as the system aged. At some point in time, the required spare parts would be out of stock and the repair could not be carried out.

27.   Mr Michael TIEN considered that as technology was developing fast, the Administration would still face the risk of forged identity cards within a few years after it had awarded the SMARTICS-2 contract to a contractor who could offer a warranty period of 15 years or more. AD of Imm(IS) said that the Administration would enhance anti-forgery features in SMARTICS-2 with a view to facilitating frontline staff to identify forged identity cards, thereby reducing the possibility of forged cards.

28.   Dr LO Wai-kwok agreed that there was a need to replace the current smart identity cards as the existing system had become obsolete and a new system with updated security features would offer better protection of personal data. Dr LO asked what the consequences would be if the tendering proposal was rejected by the Committee.

29.   US for S said that with the aging of existing smart identity cards, the possibility of massive card failure would increase, and if that happened, the public might encounter much inconvenience in immigration clearance. AD of Imm(PD) added that current smart identity cards had a serviceable lifespan of around 10 years. If a majority of these cards in use malfunctioned, the Immigration Department might not have sufficient manpower to handle the sharp increase in applications for replacement of identity cards in a timely manner. He added that the Immigration Department's stock of empty cards could only last until 2018, and there might not be sufficient cards in stock to meet the demand for replacement when there was a massive card failure.

Financial implications of SMARTICS-2

30.   Mr Albert CHAN noted that the implementation of SMARTICS-2 would incur a total expenditure of about $3.79 billion but would achieve a total

saving of about $3.91 billion from 2015-16 up to 2027-28 and expressed skepticism about these estimates. AD of Imm(IS) advised that independent evaluation was conducted by consultants based on market research on the cost of similar systems in use.

Requirement of carrying and producing identity cards

31. Mr LEE Cheuk-yan queried there was still a need for identity card at all, and he said that the policy on identity card should be reviewed. The Chairman dismissed Mr LEE Cheuk-yan's question as irrelevant as it involved board policy issues that should not be brought up for discussion at FC's meetings.

Scope of information stored in a smart identity card

32. Mr LEE Cheuk-yan asked whether personal information other than that required under existing legislation would be stored in the proposed smart identity cards. US for S said that information stored in a smart identity card was provided for in the Registration of Persons Regulations (Cap. 177A). Reading of information from smart identity cards would require the consent of the cardholder concerned. The Office of the Government Chief Information Officer was conducting a separate technical study to review the other possible uses of smart identity cards.

33. Ms Emily LAU expressed concern about privacy issues when personal information such as medical records were stored in the chip embodied in the identity card. Ms LAU noted that the personal data stored in an identity card could be accessed by a third party when the cardholder used certain facilities or services. She enquired how the arrangements operated in practice.

34. US for S stressed that a person's medical records would not be stored in the smart identity cards. Only basic data necessary for determining the cardholder's identity would be accessed from an identity card when a person used any of the specified facilities. Data such as medical records and library loan history were stored in separate databases owned by relevant facilities. AD of Imm(IS) and Principal Assistant Secretary for Security(D) ("PAS(S)D") explained the basic operations of accessing data stored in the identity card by the cardholder when using the various facilities highlighted in (a) to (h) of paragraph 15 of the Administration's paper on the item FCR(2015-16)7.

35. The Chairman directed that members' speaking time for the second round of questions, including the Administration's response, should not exceed three minutes each.

36.　　　In response to Ms Emily LAU and the Chairman, PAS(S)D said that the Public Private Interface-Electronic Patient Record Sharing Pilot Project ("PPI-EPR") rolled out by the Hospital Authority ("HA") provided a secure platform for registered private practitioners to access electronic patient records ("EPR") of consenting individual patients.　HA's patients could enroll in the pilot project on a voluntary basis by inserting the identity card into a government-approved card reader where relevant data would be accessed for generation of an application form for signature by the patient.　Thereafter, with the patient's consent, private healthcare provider registered in the project could view the patient's clinical information online.

37.　　　AD of Imm(PD) supplemented that according to information provided by HA, up to April 2015, the PPI-EPR pilot had enrolled more than 428 000 patients, 3 300 private healthcare professionals and more than 1 172 000 numbers or EPR access had been made by the participating private hospitals, etc.

Personal data privacy protection

38.　　　Mr WU Chi-wai asked if the Administration would conduct risk assessment of the existing smart identity card system to identity areas for enhancing personal data protection in SMARTICS-2.　AD of Imm(IS) advised that a Privacy Impact Assessment ("PIA") had been conducted upon completion of the feasibility study of SMARTICS-2.　The PIA report had been submitted to the Office of the Privacy Commissioner for Personal Data ("PCPD") for comments.　Further PIAs would be conducted during system analysis and design, pre-implementation and post-implementation stages and PCPD would be consulted on the findings of the PIAs.

39.　　　AD of Imm(IS) supplemented that the Administration would also engage an independent auditor to conduct information technology security risk assessment and security audit at different stages of implementation to ensure the effectiveness of those security measures in protecting information in SMARTICS-2 and smart Hong Kong identity cards.

40.　　　Mr WU Chi-wai asked how many of the existing generation smart identity cards had been damaged and required replacement so far, and what the causes of damage were.

41.　　　US for S advised that up to the end of March 2015, a total of 66 200 smart identity cards had been damaged and replaced.　AD of Imm(PD) added that no further analysis on the causes of damage had been conducted.　He

explained that any such analysis would need to be carried out by the identity card supplier, and might risk leaking the personal data of the card holders.

42.   There being no further question, the Chairman put the item to vote. The Chairman declared that the Committee approved the item.

43.   The Chairman declared that the meeting be adjourned.

44.   The meeting was adjourned at 5:00 pm.

Legislative Council Secretariat
14 August 2015