立法會
Legislative Council

LC Paper No. CB(2)897/18-19(04)

Ref : CB2/PL/SE

Panel on Security

Background brief prepared by the Legislative Council Secretariat for the meeting on 5 March 2019

Next generation electronic passport

Purpose

This paper provides background information and summarizes discussion of the Panel on Security ("the Panel") on issues relating to the implementation of the Next Generation Electronic Passport System ("e-Passport-2 system") and issuance of the electronic Hong Kong Special Administrative Region Passport ("e-Passport").

Background

2. The International Civil Aviation Organization ("ICAO") is a specialized agency of the United Nations responsible for, among other things, devising travel document standards for compliance by contracting members with a view to enhancing the effectiveness of control on passport fraud and maintaining the integrity and security of passports and other travel documents. In May 2004, ICAO published a new standard for biometric passports. ICAO also recommended that passport issuing authorities should introduce changes to passport designs and security features every 10 years.

3. The Immigration Department ("ImmD") started to implement the existing Electronic Passport System ("e-Passport system") in 2005 and issue the e-Passport since February 2007, with a view to enhancing its security standards. In compliance with the ICAO standard, the existing e-Passport contains a contactless chip that store information including those printed in the machine readable zone of the bio-data page, as well as the holder's image, full name in English and Chinese, place of birth, issuing authority and date of issue.

4. In March 2010, ImmD engaged an external consultant to conduct the third Information Systems Strategy Review. Amongst other things, the consultant recommended implementation of the e-Passport-2 system to address the obsolescence of hardware and software of the existing e-Passport system and to cater for potential new business needs. Following the recommendation, ImmD completed a feasibility study on the implementation of the e-Passport-2 system in October 2014.

Members' deliberations

5. The Panel was briefed on the Administration's proposal to implement the e-Passport-2 system and related funding proposal on 5 May 2015.

Need for the new e-Passport-2 system

6. Members were advised that the existing e-Passport system would have been in use for 10 years by 2017. As the system was built on technologies prevailing about a decade ago, ImmD was facing increasing difficulties in securing critical maintenance of the major hardware and software of the system. Moreover, implementation of the e-Passport-2 system would enable ImmD to increase the efficiency in the overall processing and issuance of e-Passports and cope with the growing service demands in the next 10 years. For instance, electronic submission of applications, which was available to selected types of e-Passport applicants, could be extended to all eligible applicants regardless of their age. Electronic submission of e-Passport applications could also be extended from the web-based platform to the mobile platform, making it more accessible to applicants in completing and submitting e-Passport applications at their convenience. Self-service kiosks would be introduced to provide flexibility of extending service hours and allow eligible applicants to collect their passports at their convenience. Members had no objection to the implementation of the proposed e-Passport-2 system.

Security features of e-Passports

7. Some members expressed concern about whether existing e-Passport holders would be required to replace their passports with the next generation e-Passport following the implementation of e-Passport-2 system. The Administration advised that ICAO recommended that passport issuing authorities should introduce changes to passport designs and security features every 10 years. Implementing the e-Passport-2 system would enable ImmD to enhance the security features of existing e-Passports, such as see-through

window, which could be easily distinguished by law enforcement agencies. That said, holders of existing e-Passports could renew their passports according to the expiry dates of their respective passports. Members were further advised that ImmD would keep in view the latest ICAO recommendations and standards, including those on security features and chip technology, and update the e-Passport accordingly.

8. Some members were concerned about the security of personal data stored in e-Passports and the possibility of leakage of such data to a third party. The Administration advised that all personal data pages of existing e-Passports were printed at the Travel Document Personalisation Centre of ImmD where the security level was high. The personal data of e-Passports were only accessible by authorized personnel of ImmD. According to the Administration, since the introduction of the existing e-Passport in 2007, only one case involving a faked e-Passport of a low quality had so far been identified, and there was no known case of leakage of personal data stored in e-Passports.

9. The Administration would brief the Panel on the next generation e-Passport at the meeting on 5 March 2019.

Relevant papers

10. A list of the relevant papers available on the Legislative Council website is in the **Appendix**.

Council Business Division 2
Legislative Council Secretariat
28 February 2019

Appendix

Relevant papers on next generation electronic passport

Committee	Date of meeting	Paper
Panel on Security	5.5.2015 (Item VI)	Agenda Minutes

Council Business Division 2
Legislative Council Secretariat
28 February 2019