

**立法會**  
**Legislative Council**

LC Paper No. CB(2)1294/11-12(04)

Ref : CB2/PL/SE

**Panel on Security**

**Background brief prepared by the Legislative Council Secretariat  
for the meeting on 13 March 2012**

**Security of Automated Passenger Clearance System (e-Channel)**

**Purpose**

This paper summarizes past discussions by the Panel on Security ("the Panel") on the security of Automated Passenger Clearance System ("e-Channel").

**e-Channel**

2. On 16 December 2004, the Immigration Department ("ImmD") introduced e-Channels, an automated passenger clearance system, for Hong Kong permanent residents. Since then, all passenger control points have been installed with e-Channels, including the control points at the Hong Kong International Airport, Hung Hom, Lo Wu, Lok Ma Chau, Lok Ma Chau Spur Line, Man Kam To, Sha Tau Kok, Shenzhen Bay, China Ferry Terminal, Macau Ferry Terminal and Tuen Mun Ferry Terminal. Hong Kong permanent residents (except those under the age of 11) or Hong Kong residents holding Document of Identity for Visa Purposes can use their smart identity cards to perform self-service immigration clearance.

3. The e-Channel system deploys fingerprint verification technology for authentication of a person's identity. A Hong Kong resident using e-Channel service has to insert his Hong Kong smart identity card into a card reader. The system would verify the fingerprint captured by the scanner on the spot against the fingerprint template stored in the chip of the smart identity card. The clearance time involving e-Channels is around 12 seconds.

## **Express e-Channel**

4. Since March 2009, ImmD has launched a pilot scheme on Express e-Channel at Lo Wu Control Point ("LWCP"). It aims to provide faster e-Channel service to Hong Kong residents aged 18 or above. Enrolment for using Express e-Channel is voluntary.

5. To use the Express e-Channel service, a resident has to enrol in advance. During the enrolment process, his personal data and fingerprint templates will be retrieved from the chip of identity card and stored in a database at the control point. When the resident uses Express e-Channel, he only needs to place the identity card onto an optical reader. The system will read the information on the surface of the identity card and retrieve the relevant data required for clearance from the database at the control point. Since retrieving information from the database at control point is faster, the clearance time can be shortened to eight seconds.

6. To safeguard the security of the personal data involved, the data collected during enrolment will be transmitted via a closed and secure network to back-end servers for storage. All the back-end servers are installed at computer rooms purpose-built in compliance with the relevant security requirements. Only authorized officers of the rank of Immigration Officer or above may gain access to the data at designated computer terminals. The system will keep track of the records of all access to the database for security auditing. Moreover, the computer system has protection devices against hacking and intrusion.

## **Measures to enhance immigration clearance**

7. According to the Administration, ImmD has plans to enhance its automatic clearance system and strengthen the handling capacity of its control points to tie in with the plan of the Mainland authorities to issue electronic "Exit-Entry Permits for Travelling to and from Hong Kong and Macao" ("e-EEP") to Mainland residents. ImmD has secured funding approval from the Finance Committee in July 2010 for upgrading its computer system and installing facilities for enabling Mainland visitors using e-EEP to visit Hong Kong. Meanwhile, ImmD is considering allowing eligible frequent visitors from the Mainland to use the e-Channel service in a trial run so as to provide more efficient clearance.

8. The Administration plans to enhance the clearance facilities at existing cross-boundary control points. For instance, the Administration plans to more than double the number of e-Channels at the Lok Ma Chau Control Point, the busiest land boundary control point, from 20 to around 46. The first phase of

this project (south bound) has commenced in the first half year of 2011 and is expected to be completed by 2012. The second phase (north bound) will follow thereafter. The Administration also plans to conduct similar works at the Man Kam To Control Point and increase the number of e-Channels from 9 to 18. The works have commenced in the first quarter of 2011 and is expected to be completed in 2012.

### **Deliberations of the Panel**

9. The Panel discussed the security of e-Channel at its meetings on 7 December 2004, 6 January 2009, 2 February 2010 and 1 June 2010. The deliberations are summarized below.

10. Concern was raised as to whether there would be measures against the use of false fingers or artificial fingerprints. According to the Administration, the fingerprint scanner was capable of detecting the liveliness of a finger through the detection of electric current and blood flow in the finger.

11. Concern was also raised as to whether there were cases detected involving the use of forged smart identity cards by Hong Kong residents in an attempt to perform self-service immigration clearance through e-Channels. According to the Administration, between the introduction of the e-Channel service in December 2004 and February 2010, ImmD had never discovered any cases of Hong Kong residents using forged identity cards to successfully pass through the e-Channels.

12. Members noted that some people could not use their smart identity cards for automated immigration clearance through the e-Channel system due to fingerprint recognition problem. Information was sought on the estimated number of people who could not use automated immigration clearance at Express e-Channels, and the measures to be introduced to reduce failure in fingerprint verification.

13. According to the Administration, some people with blurred fingerprints might have difficulty in using e-Channels. It was because the fingerprint scanner used on the spot might not be able to capture a good fingerprint image. In some circumstances, for example, when the weather was dry, the fingerprint identification problem was more distinct. Statistics showed that less than 1% of smart identity card holders had such a problem. Passengers who had persistent difficulties in using the e-Channels due to fingerprint recognition problem could visit the enrolment office located at LWCP to provide better fingerprint image for future verification purpose at the Express e-Channel. To address the problem associated with fingerprint capturing and matching, optical fingerprint scanners had been installed at LWCP as a trial measure. It was

later found that many passengers who had fingerprint recognition problem did not have any problem now when performing self-service immigration clearance through e-Channels. Many of the control points had been installed with optical fingerprint scanners.

14. Members had sought information on the kind of personal data that would be retrieved and stored in ImmD's back-end servers should a smart identity card holder opt to enrol for using Express e-Channels, and how ImmD would ensure that information newly added to the chip of the Hong Kong smart identity card could be updated to the database kept in the servers.

15. The Administration advised members that when a passenger inserted his identity card into the card reader at an enrolment e-Channel, the passenger would be invited to give his consent regarding the transfer and storage of his personal data. The relevant data required for performing self-service immigration clearance through Express e-Channels, which were stored in the chip of his Hong Kong smart identity card, included Hong Kong identity card number, name, sex, date of birth, date of registration of the identity card, status of Hong Kong residency and fingerprint templates. On obtaining the passenger's consent, these data would then be transferred via a closed and secure network to ImmD's back-end servers for storage. New information thereafter added to the chip of the passenger's smart identity card, except updated information on limit of stay, would not be required for immigration clearance purpose through the Express e-Channel system.

16. Members noted that ImmD had appointed an independent contractor to carry out a security audit on its information technology system. Concern was raised as to whether the Information Technology Security Report issued by the contractor on 15 September 2006 had proved to the satisfaction of the Privacy Commissioner for Personal Data that ImmD had put in place sufficient measures to protect data privacy in launching the pilot scheme on Express e-Channel.

17. According to the Administration, the security audit was carried out by an independent contractor. After examination of the said report, the Privacy Commissioner was of the view that the privacy concerns appeared to have been properly addressed in the system design of the Express e-Channel system. ImmD had commenced another round of information technology security audit in December 2008 to confirm that the security of the system and data as well as access control were in compliance with the Government's security requirements and the personal data protection principles under the Personal Data (Privacy) Ordinance.

18. Members were concerned that many past incidents indicated that the major cause of data leakage was a lack of awareness and understanding among

the staff of the security regulations and the risk of compromising personal data. Information was sought on the safeguards to be put in place to ensure that data stored in the back-end servers at LWCP were afforded appropriate protection.

19. According to the Administration, it attached great importance to the protection of personal data privacy. Apart from the use of security token, password and user name, personal particulars would be encrypted before storage in the servers. As USB connectivity was not provided in the design of the system, all personal data stored in the servers, including fingerprint templates encoded in strings of binary digits, could not be downloaded to portable electronic storage devices.

20. Members noted that Mainland residents holding an Exit-Entry Permit for Travelling to and from Hong Kong and Macao ("EEP") issued by the Mainland authorities might only enter after examination by officers of ImmD at the traditional counters at control points. If Mainland frequent visitors who held an e-EEP to be issued by the Mainland authorities and had enrolled in advance for using e-Channels could use such automated passenger clearance system to perform self-service immigration clearance in the future, there would not be any face-to-face examination in the immigration clearance of these visitors. Concern was raised as to whether the new arrangements would undermine the immigration control over Mainland residents travelling to Hong Kong. Information was also sought on the eligibility criteria for use of the e-Channel service by Mainland frequent visitors.

21. The Administration advised members that -

- (a) to improve the arrangements for Mainland residents travelling to Hong Kong and Macao, the Mainland authorities would introduce a new type of e-EEP to Mainland residents by phases from 2012 onwards. A computer chip would be embedded in the e-EEP containing the holder's personal information and exit endorsement to Hong Kong;
- (b) on the basis of a significant growth in the overall number of Mainland visitors, the Administration anticipated that the number of Mainland frequent visitors would also grow and hence there was a need to enhance the handling capacity as well as efficiency of ImmD by shortening the time required for immigration clearance. The Administration therefore proposed allowing eligible Mainland frequent visitors to use e-Channels after enrolment;
- (c) a visitor from the Mainland was eligible to enrol for using the e-Channel service, if he had visited Hong Kong for three times or

more in the preceding 12 months and held an EEP with a valid multiple-journey exit endorsement to visit Hong Kong. In processing an application for enrolment, ImmD officers would rigorously examine the EEP and endorsement of the applicant to ensure that he met the enrolment criteria, including the absence of adverse records. For those who met the enrolment requirements, ImmD officers would take photos and record their fingerprints. Personal information would be recorded in ImmD's computer system for future immigration verification. When an enrolled Mainland visitor used an e-Channel, the system would retrieve the enrolled information for verification. If the system could not verify the visitor's fingerprint, or detected any other problem, such as adverse records after enrolment, the visitor would not be able to pass through the e-Channel. ImmD officers would conduct face-to-face examination on the visitor or conduct spot checks on enrolled frequent visitors who used the e-Channel service; and

- (d) the Administration would review the eligibility criteria for Mainland frequent visitors using the e-Channel service in the light of actual experience to ensure that effective immigration control was maintained while immigration facilitation was provided.

22. Members considered that ImmD should establish a mutual alert or notification mechanism jointly with its counterparts in the Mainland, Macao and other countries on frequent visitors failing to fulfil the enrolment requirements for whatever reasons, so that frequent visitors successfully enrolled for using e-Channels for self-service immigration clearance at the control points might be scrutinized closely, and approval for enrolment could be cancelled when circumstances so warranted.

### **Relevant papers**

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

**Relevant papers on  
Security of Automated Passenger Clearance System (e-Channel)**

<b>Committee</b>	<b>Date of meeting</b>	<b>Paper</b>
Panel on Security	7.12.2004 (Item IV)	<u>Agenda</u> <u>Minutes</u>
	6.1.2009 (Item IV)	<u>Agenda</u> <u>Minutes</u>
	2.2.2010 (Item IV)	<u>Agenda</u> <u>Minutes</u>
	1.6.2010 (Item IV)	<u>Agenda</u> <u>Minutes</u>

Council Business Division 2  
Legislative Council Secretariat  
7 March 2012