

立法會
Legislative Council

LC Paper No. CB(2)832/09-10(08)

Ref : CB2/PL/SE

Panel on Security

**Background brief prepared by the Legislative Council Secretariat
for the meeting on 2 February 2010**

Automated Passenger Clearance System

Purpose

This paper provides background information on the Automated Passenger Clearance System (e-Channel) and the pilot scheme on Express e-Channel of the Immigration Department (ImmD).

e-Channel

2. On 16 December 2004, ImmD introduced e-Channels for Hong Kong permanent residents. Since then, all passenger control points had 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 deployed fingerprint verification technology for authentication of a person's identity. A Hong Kong resident using e-Channel service needed 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 traditional e-Channels was around 12 seconds. The installation of e-Channels had significantly increased the overall passenger throughput at control points because every two traditional counters could be converted into three e-Channels and manpower could be redeployed to serve visitors and other identity card holders who used traditional counters.

4. As at December 2008, the Administration had installed 361 e-Channels at various immigration control points. Among the Hong Kong residents crossing the boundary control points, around 80% had used the service.

5. When first launched in 2004, the e-Channel service was only available to Hong Kong permanent residents. Since May 2008, the Administration had extended the service to frequent visitors aged 18 or above. The Administration had installed 10 e-Channels for use by frequent visitors at the Hong Kong International Airport. As at the end of November 2008, about 11 000 visitors had enrolled for the service.

Express e-Channel

6. At the meeting of the Panel on Security held on 6 January 2009, the Administration briefed members on the plan of ImmD to launch a pilot scheme on Express e-Channel in February 2009 at the Lo Wu Control Point (LWCP) with a view to further enhancing the efficiency of the service. At an Express e-Channel, the fingerprint captured by the scanner would be verified against the fingerprint template stored in a back-end server instead of the chip of a smart identity card. Since retrieving information from a back-end server was faster, this would shorten the processing time by about four seconds. Members were informed that -

- (a) ImmD intended to commence the pilot scheme on Express e-Channel in February 2009 at LWCP. As enrolment for using Express e-Channels needed to be done through designated e-Channels, 10 enrolment e-Channels would be installed at LWCP for such purpose;
- (b) after enrolment into the scheme, passengers could complete the clearance procedures through one of the 10 Express e-Channels. ImmD would set up overhead display boards and sign-posts to indicate clearly the locations of the enrolment e-Channels and Express e-Channels;
- (c) enrolment was a one-off exercise. Passengers already enrolled for using Express e-Channels would not be required to register again even if the service was to be extended to other control points in future; and
- (d) ImmD would make available leaflets, posters and videos explaining the enrolment process and the data to be retrieved and stored. Staff of ImmD would be deployed to assist users in enrolling for and using Express e-Channels.

7. Some members pointed out that some people could not use their smart identity cards for automated immigration clearance through the e-Channel system due to fingerprint recognition problem. They asked whether the Administration had estimated the number of people who could not use automated immigration clearance

at Express e-Channels, and whether measures would be introduced to reduce failure in fingerprint verification.

8. The Administration explained that 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. To address the problem associated with fingerprint capturing and matching, ImmD was exploring the feasibility of using optical fingerprint scanners in order to get good fingerprint image. ImmD was in the process of testing these devices. As a trial measure to improve the flow of cross-boundary passengers, a small quantity of optical fingerprint scanners had been installed at LWCP. 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. If optical fingerprint scanners were found to be more effective, ImmD would consider wider use, by phases, of these devices in other boundary control points.

9. Members asked about 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.

10. The Administration advised 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. Regarding the procedures for participants to withdraw from using Express e-Channels, the Administration explained that a passenger who had given consent to enrol in the Express e-Channel system might withdraw from the scheme by completing and returning to ImmD a purposely designed form. On receipt of his written notice, ImmD would delete the relevant data stored in the back-end servers.

11. Members noted that ImmD had appointed an independent contractor to carry out a security audit on its information technology (IT) system. They asked whether

the IT Security Report issued by the contractor on 15 September 2006 had proved to the satisfaction of the Privacy Commissioner for Personal Data (PC) that ImmD had put in place sufficient measures to protect data privacy in launching the pilot scheme on Express e-Channel. They also enquired about the difference in terms of security level between the existing e-Channel system and the Express e-Channel system.

12. The Administration explained that -

- (a) the security audit was carried out by an independent contractor. After examination of the said report, PC was of the view that the privacy concerns appeared to have been properly addressed in the system design of the Express e-Channel system;
- (b) ImmD had commenced another round of IT 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; and
- (c) the security level of the new system would be comparable to that of the e-Channel system. The authentication procedures built into the e-Channel system in relation to retrieval of fingerprint template and identity verification were strict security measures to safeguard the security of data and protect them from unauthorized access or change. Regarding the Express e-Channel system, the back-end servers would be installed at computer rooms purpose-built in compliance with the relevant security requirements. Only authorized officers of the rank of Immigration Officer or above could gain access to the data at designated computer terminals. The new system would keep records of all access to the database for security auditing. Moreover, the computer system of ImmD would have intrusion detection system to prevent hacking and intrusion.

13. 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. They sought information on the safeguards to be put in place to ensure that data stored in the back-end servers at LWCP were afforded appropriate protection.

14. The Administration advised that 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. The Administration assured members that there was no question of data leakage from back-end 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.

15. On the question of whether and when the pilot scheme on Express e-Channel would be extended to other boundary control points, the Administration informed members that it would review the pilot scheme in the second half of 2009. It estimated that some 600 000 frequent travellers, who made cross-boundary journeys to and from LWCP at least once in every two weeks, might find it easier and more convenient to perform self-service immigration clearance through Express e-Channels and hence opt to enrol for the service. If the service was well received by the public, it would consider extending the scheme to other control points.

Relevant papers

16. Members may wish to refer to the following minutes and papers for further details -

- (a) minutes of the meeting of the Panel on Security on 7 December 2004 (LC Paper No. CB(2)666/04-05);
- (b) Administration's paper entitled "Implementation of Phase II of the Updated Information Systems Strategy for the Immigration Department - the Automated Passenger Clearance System and the Automated Vehicle Clearance System" (LC Paper No. CB(2)286/04-05(01));
- (c) supplementary information provided by the Administration on the Automated Passenger Clearance (APC) System and the Automated Vehicle Clearance (AVC) System (LC Paper No. CB(2)893/04-05(01));
- (d) Administration's annual report on the implementation of government computer systems (FCRI(2007-08)16);
- (e) minutes of the meeting of the Panel on Security on 6 January 2009 (LC Paper No. CB(2)963/08-09); and
- (f) Administration's paper entitled "Pilot Scheme on Express e-Channel" (LC Paper No. CB(2)555/08-09(03)).

17. The above minutes and papers are also available on the website of the Legislative Council (<http://www.legco.gov.hk>).