Information paper on
1 June 2000

Panel on Security of the Legislative Council

Progress Report on the HKSAR Identity Card Project

INTRODUCTION

Consultants have completed the feasibility study on the HKSAR identity card (ID card) system and submitted a draft Study Report to Immigration Department (ImmD). While ImmD is considering the draft report, we would like to brief Members of Consultants' key findings and recommendations in the first instance.

CONSULTANTS' KEY FINDINGS AND RECOMMENDATIONS

2. Consultants are of the view that the design of the existing ID card is outdated and prone to forgery. The supporting computer system is aged and would reach the end of its life expectancy by 2002 and some spare parts are no longer available in the market.

3. To address the above problems, Consultants have put forth the following recommendations:-

(a) The new ID card should use a secure base material for card production and utilize the laser engraving technology for card personalisation to ensure, together with a combination of physical card security features, that the card will be highly secure and fraud-resistant;

(b) The new ID card should capture the cardholder's facial image and two thumbprints. This will provide the facility to securely authenticate a cardholder's identity and lay the foundation for automating some currently manual processes (such as passenger clearance procedures);

(c) A new computer system using up-to-date supporting infrastructure, network design and equipment should be developed in order to achieve better response and performance;

(d) The old ID card application records (which are presently stored in microfilms) should be converted into digital images to facilitate on-line retrieval of records. This new mode of document storage will enhance the efficiency and effectiveness of the ID card-issuing offices and achieve savings in resources; and

(e) A region-wide ID card re-issuing exercise should be conducted when the new computer system is up and running so that all Hong Kong residents can obtain a new ID card within a reasonable period of time.

Options for the new ID card

4. As regards the choice of the ID card, there are three options:-

(a) a non-smart ID card; or

(b) a smart ID card which is capable of supporting ImmD's core businesses only; or

(c) a smart ID card which can support multiple applications, i.e. ImmD's core businesses plus other value-added applications. Potential applications include government applications like driving licence, voting, senior citizen card, electronic services delivery and health records like blood group, and non-government applications such as electronic commerce, digital certificate and stored value etc.

5. Consultants are of the view that a smart ID card is preferable to a non-smart ID card because the former can employ more sophisticated cryptographic techniques to protect the data and ensure that it cannot be fraudulently altered. In addition, a smart ID card will enable immigration officers to update the conditions of stay of temporary residents upon granting of extension of stay to them or their re-entry to Hong Kong. In anti-illegal immigration operations, law-enforcing officers in the field can use a special reader to confirm instantly if their permission to stay is valid without holding up the person for further checks. A non-smart ID card cannot achieve these purposes.

6. As to whether a smart ID card should be used for ImmD's core businesses only, or for multiple applications, Consultants recognize that this is a policy matter to be decided by the Administration. If multiple applications outside the core businesses of ImmD are to be pursued, it is essential that an external agency be set up to own and manage the operation and overall security of the smart card scheme. Furthermore, whether or how an individual application should be incorporated into a smart card should be subject to a separate feasibility study.

Data Privacy and Security

7. On data privacy and security, Consultants recommend that the design of the new ID card and the new computer system must have regard to the following issues:-

(a) Compliance with the Personal Data (Privacy) Ordinance;

(b) Designing systems and procedures in a privacy-sensitive manner; and

(c) Use of privacy enhancing technologies to prevent identity theft and to protect the data privacy of the individual.

8. More specifically, Consultants recommend that the following data protection measures should be adopted:-

(a) Protection of data on the card (e.g. biometric data, personal data) against unauthorised access by means of access controls enforced by the card itself, so as to ensure that any request to read the data coming from an unauthorised system will not be entertained;

(b) Protection of data in ImmD systems by means of system access controls that are well-tested, including passwords, different levels of authority and audit trails;

(c) Strong enforcement of access controls on sensitive data, including biometric data, by encryption of the data stored on cards, in computer systems, and during transmission within and between ImmD offices. Even if encrypted data are intercepted by an unauthorized person, they will be in the form of a set of meaningless characters and numbers;

(d) Data may be encrypted in such a way that separate keys are used for each type of data and for each card, so that staff of different departments or if necessary, different staff within the same department, can only have access to those data as are relevant to their scope of work;

(e) Use of tamper-resistant hardware security devices (which will stop functioning if it detects that several unsuccessful attempts have been made to read the data on the card or to gain access control to the system) to strongly protect the cryptographic security of the systems;

(f) Protection of data on the card from fraudulent changes by using cryptographic data integrity so that fraudulent data or fraudulent cards cannot be created;

(g) Provision of self-service kiosks in ImmD offices so that cardholders can view the data on their cards, using biometrics for access control (the card will also check the authenticity of the kiosk before releasing the data);

(h) There will be no facilitation of one-to-many matching of biometric data, which means that the biometric data will be used only for the purpose of authenticating a named person's identity and it will not be possible to use the data to search the entire database for a match; and

(i) If the identity card is to be used for multiple purposes, using smart card and a smart card scheme that guarantees separation of uses from each other, so that immigration data on a card will be protected from access by other departments and vice versa.

9. To ensure that the above measures will be adequately implemented, Consultants further recommend that ImmD should employ consultants with recognised privacy credentials to review the design and planning at specific points and to undertake Privacy Impact Assessments.

WAY FORWARD

10. Upon acceptance of the final Study Report, ImmD will assess the consultants' recommendations and, in light of comments from this Panel and bureaux/departments, firm up a view on the way forward including the choice of a new ID card. Members will be consulted further. Funding approval will be sought in the normal manner.

Security Bureau
May 2000