Supplementary Note on
24 October 2000

Panel on Security of the Legislative Council

Progress of the HKSAR Identity Card Project

(Supplementary Note)

INTRODUCTION

On 19 October 2000, Secretary for Security informed this Panel of Government's decision to introduce a smart ID card with multi-application capacity in early 2003. A Legislative Council Brief on this subject was distributed to Members on the same day.

2. One of the major concerns as reflected by the mass media in the past few days is whether there will be sufficient safeguards to protect the card holder's data privacy, particularly if the new smart ID card is capable of supporting multiple applications. This note provides supplementary information on measures that will be taken by the Administration to protect data privacy.

PROPOSED DATA PRIVACY PROTECTION MEASURES

3. From the outset, we recognize that data privacy is a key issue that must be addressed most carefully. We have therefore taken a comprehensive approach to deal with this issue -

Card

- Data to be printed on card surface will be no more than that in the current card
- Only minimal data will be collected and stored in the chip
- More sensitive data will be kept at back-end computer systems as at present
- Thumbprints stored on card will be in the form of a set of meaningless digits (a template) and cannot be used to reconstruct the original thumbprints
- Data for different applications will be segregated
- Data will be encrypted to prevent unauthorized access or alteration
- Only authorized persons can have access to the data/applications on card which they are authorized to access
- Card will be protected by advanced security features and cryptographic technology

Back-end computer system

- There will be stringent system access control, including passwords, different levels of access authority and audit trails
- Sensitive data will be encrypted in the database and during transmission
- Individual departments involved will maintain their own database as at present so as to guarantee separation of uses from each other
- Advanced technology will be employed to protect integrity of the data at hardware, software and application level
- Use of tamper-resistant hardware security devices to protect security of system

Card holders

- For the great majority of non-immigration applications, card holders will have a choice on whether to include the applications on the card, i.e. they will have a genuine and non-discriminatory choice
- Card holders can view what data are stored on the smart ID card through self-service kiosks

No identity theft

- Use of biometrics to authenticate card holder
- Card can be used only if card holder is authenticated

Government users

- The collection, storage, use and release of data must comply with the law, in particular, the Personal Data (Privacy) Ordinance
- Only authorized departments can have access to the relevant database
- No access to data at the backend systems or on card across departments providing services under the card scheme
- No sharing of database by Government departments. The situation will be the same as at present
- Immigration Department will conduct Privacy Impact Assessments at different stages of the project
- The Privacy Commissioner for Personal Data will be informed of the findings of each assessment and his views will be taken into account in formulating and revising the data protection measures

4. A highly secure smart ID card is itself privacy-positive. It will bring more benefits and convenience to the community.

Security Bureau
23 October 2000