LC Paper No. CB(2)2433/01-02(06)

For Discussion
on 4 July 2002

Legislative Council Panel on Security

Update on Non-immigration Applications for Incorporation into the Smart ID Card

INTRODUCTION

In December 2001 we put forward to Members our conclusions on which non-immigration applications the new smart ID card should be used for and how. This paper seeks to update Members on the progress we have made and sets out some details of how we shall effect the applications.

BACKGROUND

2. On 20 December 2001, we briefed Members on non-immigration aspects of the smart ID card. In summary, we stated that all applications would be voluntary at the choice of the citizen, and would include:

(a) A Hongkong Post Digital Certificate. A digital certificate (e-Cert) can be regarded as an "electronic-ID" of the user. It can be used for authentication of the identity of the parties involved and for ensuring integrity, confidentiality and non-repudiation of the data transmitted in an electronic transaction.

All persons applying for a replacement ID card during the ID card reissue exercise will be offered the choice to have a free e-Cert (free for one year) embedded on the card. The fact

that potentially more than 6 million people will have an e-Cert will, we believe, provide a good boost to people's willingness to adopt e-commerce and hence drive the development of e-applications.

(b) Library card. Citizens will be able to use the smart ID card as a library card, if they wish, and hence no longer need to carry the latter.

(c) Driving licence. With effect from 2005/2006, citizens will no longer be required to carry a driving licence for enforcement purposes, because by then the Police will be able to directly interrogate the Transport Department backend licensing computer system to find out a driver's status. If citizens wish, they need no longer have any physical licence. Citizens will also be able to check their driving licence data in the Transport Department computer system using the e-Cert (or possibly a PIN).

(d) Change of address. Citizens will be able to use the e-Cert on the smart ID card to notify the Government of the change of their address electronically.

PROGRESS

Hongkong Post e-Cert

3. Good progress has been made by the Hongkong Post (HK Post) and Immigration Department (ImmD) to ensure that there are smooth and one-stop arrangements to allow for loading of the e-Cert onto the ID cards of the citizens who want one and that ImmD will not have access to the e-Cert data. The other important strand is to ensure that it is as easy as possible for the public to say "yes" to getting the one-year free e-Cert and to be able to start using it easily and quickly. ImmD and HK Post (with assistance from Management Services Agency) have been working this out. This is intended

to be incorporated as a part of the Internet appointment booking system for booking a time to go to ImmD for renewal of the ID card. Walk-in citizens will be encouraged to approach HK Post service counters set up at ImmD's ID card reissue offices to opt-in for a HK Post e-Cert. To make it user-friendly and convenient so that ID card-holders who have accepted the one-year free e-Cert do not need to approach the HK Post physically only one year afterwards for renewal of their e-Cert, HK Post will offer e-Cert with three-year validity instead of one (i.e. citizens need only to approach HK Post to renew their e-Cert after three years) – although it will be up to individual citizens to pay HK Post after the one-year free period-in order for the e-Cert to remain valid.

4. It is also important that citizens find it easy and user-friendly to start using the e-Cert. When citizens who have opted for e-Cert collect their new smart ID cards at ImmD's ID card reissue offices, they will be given their e-Cert PINs by HK Post representatives. They can choose to use the PINs issued by HK Post or set new PINs themselves using the kiosks in ImmD's offices. The same kiosks can also be used for checking their ROP data through the use of fingerprint. The dual functions of the kiosks are not just user-friendly, but secure. The present system design will ensure that HK Post will not have access to the cardholder's fingerprint record at all, or knowledge of how citizens make use of the Immigration functions – and vice versa for ImmD in respect of knowledge of how citizens make use of the e-Cert functions. Thus using the same kiosk for these two functions will have no adverse security and data privacy implications.

5. Apart from the kiosks at ImmD's offices, citizens can also set new e-Cert PINs using the computer terminals at Post Offices, any other personal computers with Internet connection and smart card readers, or ESD kiosks.

6. On the question of whether digital certificates issued by recognised certification authorities other than HK Post should be allowed to be embedded onto the smart ID card, we have previously advised Members that we consider this should not be allowed at this stage. This is because of possible public unease towards commercially owned applications stored on the smart ID card, certainly initially. This remains our view, and all the on-card applications to be rolled out in mid-2003 will be provided by the

Government. We will review the case if/when there is widespread public support for commercial applications, including e-Certs of other certification authorities.

7. We are very conscious that there will need to be an extensive and good publicity campaign to ensure citizens can make best use of the e-Cert and protect their e-Cert PIN : which may not be a widely known concept at all levels of the community. Members will have noted the greater publicity now being given to e-Certs – both in APIs and in general advertising. This will be very considerably stepped up and the focus will be on smart ID card when we get closer to the reissue period. ITBB will work closely with HK Post and ImmD to take this aspect forward and to avoid any possible confusion in understanding between immigration and non-immigration uses.

Library Card

8. The library card function, while straight forward and non-controversial, has raised two interesting issues of which we would like to apprise Members. These are: use of "card face data" stored in the chip; and how to deal with lost smart ID cards.

Use of Card Face Data

(a) The library card function requires that the Leisure and Cultural Services Department (LCSD) computer system be able to read (or "capture") some of the card face personal data stored in the chip in order that citizens can authenticate their identity electronically to obtain the service. It is also possible to envisage that other future applications may have similar requirements for authenticating citizens before services are provided. Although these applications are yet to be identified and will be subject to consultation with Members and acceptance of the public, we need to make certain decisions now to meet the current requirements of LCSD, while retaining flexibility for possible future applications. Three points arise. We need to ensure that any data read are

securely protected. We also need to consider what data LCSD should be allowed to read. And we need to reassure the public that any data being read are limited solely to such data – and not any other (more sensitive) Immigration data – such as thumbprint or conditions of stay.

(b) We believe that, as long as the data are securely protected, the public in general will find it acceptable that authorised Government departments are allowed to read normal "card face data" – i.e. name (English & Chinese); ID card number; date of birth; and date of issue. After all, citizens are given a choice whether they would like to use smart ID card as a library card and will be invited to give consent for LCSD to access the "card face data". Thus we believe that these four pieces of data should be made available for the library card function - and on a case by case basis for other functions that may be approved in the future.

(c) As regards security protection, we consider that the data must be read or captured only (i.e. not written/updated) and must be protected so that only bodies authorized to be in possession of the relevant unlocking keys can gain access. This can be achieved through designing the storage of card face data in such a way that the data cannot be updated or changed and through managing the distribution of the relevant unlocking keys. This is what we have done: the data in the "card face data box" cannot be updated or changed and there are Secure Access Module (SAM) keys to unlock the box- a tried and tested smart card technology.

There is also the question of where to keep such data on the chip. There are two options. One is as part of the whole immigration data which will contain these four data items. The other is to have the data kept on a separate part of the chip. We strongly believe that it is better to keep the data separate. This is because it preserves the integrity of the

immigration data from the perception point of view. In this way there should be no concerns about LCSD somehow getting access to sensitive immigration data like thumbprint or conditions of stay. We believe citizens will be assured that their legitimate privacy concerns are properly addressed in this way.

<u>How to deal with lost ID card</u>

(d) The public is well used to dealing with lost ID cards but the introduction of non-immigration functions into the card changes the situation. We would like to facilitate citizens alerting both HK Post and LCSD when they have lost their ID card. But not all citizens will accept the one-year free e-Cert and not all citizens will want to use their ID card as a library card. So it would be entirely inappropriate (a misuse of personal data) to allow both HK Post and LCSD to know about the loss of each and every ID card. The Departments should only know if the citizen wants them to know.

Our solution is two fold. First, when citizens report lost card to ImmD, ImmD will give them a simple form asking if they wish to alert HK Post and/or LCSD. ImmD will then on a daily basis forward the forms to HK Post/LCSD so that they can take the necessary action. (Of course, citizens may also choose to report loss of their e-Cert or library card directly to HK Post or LCSD.) Second, because the only change when a person gets a new ID card is the date of issue (all the personal particulars remain the same, including the ID card number), LCSD will need to read the date of issue to establish if the ID card being used as a library card is the new (valid) one or the old (invalid) one. Hence there is a need for the date of issue to be one of the pieces of data in the "card face data box". HK Post do not need such data and HK Post will revoke the e-Cert concerned once card loss is reported to HK Post.

Driving licence

9. Both the Police and Transport Department are taking forward their respective projects: the Police to introduce a new Command and Control Communications System by 2005/06; and the Transport Department to upgrade their licensing computer system VALID III to VALID IV by end 2004. Both exercises are progressing smoothly.

Change of Address

10. This is an application using the e-Cert. We plan to have the participation of more departments in the scheme (i.e. citizens will be able to inform more departments about the change in their address record at one go). We (the Efficiency Unit/Management Services Agency) are also looking at other ways to make electronic notification of change of address more user-friendly and more widespread.

Electronic Purse

11. The situation remains as reported last time – capacity has been reserved in the chip of the smart ID card. The Hong Kong Monetary Authority is of the view that the time is not yet ripe to take forward the implementation of electronic purse in the smart ID card.

Alternative Means of Electronic Authentication

12. Authentication is a basic function of the smart ID card. The e-Cert to be embedded into the smart ID card, at the choice of cardholders, is a very secure method of authenticating electronically. We have been exploring whether other alternative means of electronic authentication for facilitating e-government and e-commerce services should be included. (This has been previously mooted in the context of accessing driving licence data - as mentioned in paragraph 2(c) above.)

13. One possibility is to use a Personal Identification Number (PIN) which could be stored in the smart ID card. In fact this feature has been provided for in the smart ID card infrastructure. Citizens could initially activate the PIN by using their fingerprint and then set their own PIN for subsequent use. The PIN, once set by the cardholder, would be stored in a secure and protected compartment in a chip. In theory the PIN function idea has several attractions:

(a) Everyone is used to PINs of one sort or another in daily life.

(b) This PIN would not expire and would already be there on the chip. Citizens would not need to apply for one or to ensure they keep it valid by renewing it every so often.

(c) The same PIN could potentially be used for any e-services – one PIN for all. Thus, it would be a user-friendly infrastructure for e-services.

14. Although PIN authentication is a feature that we could take forward now (with an additional investment of about $20 million for the necessary support system, organisation, help desk etc.), we do not recommend immediate implementation, for the following reasons:

(a) The e-Cert is capable of providing the electronic authentication function. With the proposal of providing free e-Cert to smart ID card holders, we do not consider it an immediate priority to develop the PIN function.

(b) To justify the additional investment, we would need to identify suitable application(s) for adopting the PIN authentication. Suitable applications should have high transaction volume, in order that the investment is justified and benefits become apparent. Checking driving licence data by 2005/06 is a possibility, but this can well be done by the e-Cert function and citizens might appreciate that such a secure method of authentication is required for checking

such data.

(c) It might cause major confusion to the public if we have to try to explain both the PIN and the e-Cert and ask them to activate both at initial issue. Without an immediate use of the PIN to illustrate its usefulness, we do not think explanation would be very successful.

15. Under the circumstances, we do not intend to develop the PIN function at this stage but rather to reserve the capability in the chip. Should there be public demand or if useful applications or opportunities emerge in the future, we shall revert to Members on the matter.

ADVICE SOUGHT

16. Members are invited to note and comment on the progress.

Information Technology and Broadcasting Bureau
June 2002