LegCo Panel on Security
Special Meeting on 11 November 2000

Views on the Proposed HKSAR Identity Card

Smart card technology provides a convenient and secure solution for many common problems in a digital society, such as access control, computer logon, secure information exchanges, authentication, digital certificate, credit card and financial authorization. All of these problems are linked to the **authentication** or identification of an individual, and the combining of the smart card technology with the ID card is a natural evolution in the new information age.

However, there are many concerns about the **data privacy** of the cardholder and the security of the smart ID card. I will try to address these concerns strictly from a technical standpoint here, based on today's smart card technology. Concerns of a social or other nature will not be addressed - e.g. will electronic cash stored in smart cards induce more theft?

There are five key points to make:

1) The smart card incorporates the concept of a password or PIN (personal identification number). This concept is currently used in many applications, for example, access to your bank account through ATM machines. As long as the cardholder does not freely reveal his/her PIN to others and the PIN is sufficient long enough and not obvious enough to prevent successful guesses in a few trials, the smart can be as safe as ATM cards. Similar to ATM cards, before the card can be used, the cardholder's identity is verified by a correct PIN entry. The card will block itself against any further use after a pre-set number of consecutive incorrect PIN entries. This feature provides protection against any unauthorized use of the card, e.g. the tampering with lost cards.

2) Smart cards - in contrast to most of today's ATM cards - have, virtually by definition, both memory capacity and computing power within the card itself. Given this functionality, it is possible for the card to check for itself the correctness of the PIN without having the PIN transmitted across any

transmission network and before any connection is made to the host computer responsible for carrying out the operations required. This precludes the PIN from being intercepted during transmission (prevents eavesdropping) and makes the smart card act as a firewall or first line of defense against any attack on the host computer.

3) with computing power and memory capacity, cryptographic algorithms can be incorporated into the smart card to protect the data on the card and to also segregate the data by applying different encryption keys to different pieces of data stored on the smart card. The segregation of data means that each different application can have access to a restricted portion of data. This will ensure that applications/users cannot obtain unauthorised sensitive information of the cardholder even they can bypass the restricted access control imposed by the operating system installed in the card. It is worthwhile to note that cryptography technology is quite mature and have developed to the point where it is very time-consuming and expensive to break the code on encrypted data, and felons would be better off looking for other ways to get at the protected data.

4) To provide added security, biometric authentication can be used in conjunction with the smart card - i.e. a combination of smart card reader and, say, thumbprint reader. The thumbprint scanned is matched against the thumbprint information stored in the smart card. Note that the entire thumbprint is not stored on the card, rather features of the thumbprint. This is both in the interest of keeping storage requirements low and also, in the event that the thumbprint information is retrieved from smart card, the actual thumbprint cannot be reconstructed accurately, which again protects the privacy of the individual.

5) Technology does not stand still and faster and cheaper computing power could make the job easier for code-breakers. However, improvements are also expected in smart card technology. A slight increase in the computing power within the smart card would increase tremendously the effort needed to break cryptographic codes.

In summary, data protection/privacy can be ensured.

- authentication (the verification of the identity of the rightful cardholder) is ensured through PIN, thumbprint of the cardholder and physical possession of the card.

- privacy is ensured through authentication, cryptography and access control.

Submitted by:

Prof. Francis Chin
The University of Hong Kong

November 8, 2000