LC Paper No. CB(2) 214/00-01(04)

Response to the Legislative Council Brief on the New Hong Kong Identity Card

Dit-Yan Yeung（楊跂仁）
Associate Professor
Department of Computer Science
School of Engineering
Hong Kong University of Science and Technology

Let me make my stand clear right at the beginning. I am in favor of the direction towards which the proposed scheme is heading. As an academic who has R&D experience in this as well as some related areas, I would like to address and clarify a few points here, hoping that the society as a whole could work comfortably together with mutual trust to make this project a success and hence a pride of Hong Kong.

1. Cryptographic Smart Cards as Small Yet Very Secure Computers

The proposed type of smart card for use as the new ID Card has so far been presented and perceived mostly as a more secure storage device. This is not wrong; but this is not the complete picture. The most important aspect that makes this the best available choice today is not the fact that this type of card is a very secure *storage* device.

More accurately, cryptographic smart cards are very small computers with processing power, or called *processor cards*. Processor cards do not just store data; they can also process the stored data. Many other smart cards in use are simply *memory cards*, which are pure storage devices with no general-purpose processing power. Such a distinction is very important. Suppose what we use to store our secret information is just a memory card. Then the secret information inside the card has to be retrieved from the card to some other machine with processing power during such operations as user identity authentication based on the secret information. No matter how secure the smart card is as a storage device, having to require the secret information to leave the card for the information to be processed can significantly increase the risk of security threats. On the other hand, if we use a processor card instead, the most critical processing steps can be performed entirely inside the card without having to retrieve the secret information from the card. It is this very aspect that makes processor cards with cryptographic functions obviously the best available choice, if security and privacy are our top concerns.

It is also interesting to note that almost all existing cryptographic smart cards are designed to support multiple applications on the same card. Thus, if we decide to use smart cards with strong cryptographic capabilities, making the right choice for an appropriate type of smart card does not depend on whether we want to support one or

multiple applications on the same card. In fact, supporting multiple applications securely on a single card is a current trend of the smart card industry.

2. A Holistic Approach to Information Security and Privacy

On the issues of security and privacy, I feel that the mass media and the society as a whole have focused on these aspects of the ID Card separately from the rest of the information infrastructure, or at least not to the extent that I think it should be.

Needless to say, data privacy is a top concern in any civilized society. While a mature legal framework is crucial to providing adequate privacy safeguards, various security measures are needed to implement and realize them. As the Government makes more and more of its services available online (as outlined in the Digital 21 IT Strategy), a huge amount of user information and audit trails will exist in various server machines and be transmitted over public networks, though typically in encrypted form. Thus, security and privacy concerns have to be addressed regardless of whether the new ID Card will support applications other than the core business of the Immigration Department. In fact, to a certain extent, smart cards that hold application-specific information can even improve the level of security of the overall system by reducing the need for transmitting such information over the network. Of course, whether or not a user chooses to have information for additional applications stored on the card should be left entirely to the user to decide, after being given a full picture of the pros and cons of each choice.

It should be noted that smart cards have been around for almost two decades. The first patent for the key ideas was filed more than three decades ago. The first successful field trial (for phone cards) was conducted in the mid 1980s. As of now, no successful cases have been found outside research laboratories in breaking into cryptographic smart cards to access the information inside without knowing in advance the cryptographic keys. This is not surprising due to the use of hardware protection schemes in smart cards. As a comparison, over the short history of the World Wide Web (WWW) for just less than a decade, a significant number of successful attacks by hackers have been found due to either improper software configuration or inadequate security measures of many Web sites. The use of software-only protection schemes on these server machines makes successful attacks more likely to occur.

Having said this, I by no means imply that secure transactions cannot be conducted over the Internet/WWW. Proper legal and technological measures can and should be implemented to reduce the chance of successful attacks to be as low as possible. The key point is, such measures should be implemented as more Government services go online, regardless of whether smart cards are used for implementing the new ID Card.

As is always the case, the strength of any security system is just as good as the weakest component in the entire system. A smart card is not itself the entire system. It is just one component in the whole information security infrastructure. As discussed above, many other components in the infrastructure are potentially more vulnerable to attacks than a

cryptographic smart card. Thus, we should take a holistic approach to improving the overall security level of the entire system.

3. Biometric Data on Card

To allow electronic authentication to be performed securely using a smart ID Card, an important step is to authenticate the cardholder's identity reliably in order to avoid being impersonated using a stolen card. Biometric authentication is the most direct and reliable scheme for cardholder verification. To perform biometric authentication, the template of some biometric data collected from the user has to be matched against the template of some previously collected reference data during the registration process. There are two different approaches. *Online biometric authentication* requires that the reference template be stored on a central server, which has to be available online during the authentication process. On the other hand, *offline biometric authentication* does not require a server during the authentication process because the required reference template is stored inside the card. From a security and privacy point of view, offline biometric authentication is preferred because there is no need to transmit sensitive biometric data over the network for cardholder verification. Moreover, since connection to a server is not required, the offline approach typically leads to faster system response since all operations can be performed locally.

Illegal access and usage of biometric data by unauthorized people can be made difficult by three different measures:

a) Although the template is generated from the original biometric data, the template alone does not contain sufficient information to completely recover the original data.

b) The strong access control schemes used in tamper-resistant smart cards makes it extremely difficult, if not impossible, to access the data inside a card without knowing the required cryptographic keys.

c) The biometric template data can be stored inside a smart card in encrypted form.

4. Digital Certificates and Public-Key Cryptographic Support on Card

It is well accepted by the information security community that a public-key infrastructure (PKI) and the associated legal framework are crucial to the success of electronic commerce. It is encouraging to see that the Government is bootstrapping this crucial process through such projects as the e-Cert and Electronic Services Delivery (ESD). A key issue to address is where the digital certificate and the corresponding private key should be stored. As of now, secure hardware tokens such as cryptographic smart cards are the best place to keep such credentials. The question is whether the ID Card or a separately issued smart card should be used for such purposes.

If we realize that a major use of PKI-enabled smart cards is for user identity authentication based on digital signatures, it is not difficult to see that this actually shares a lot of similarities with the first category of applications mentioned in the proposal, namely, *electronic authentication*. In fact, some personal information that is used for electronic authentication is typically also stored as certificate attributes inside a digital certificate, though usually in encryption form. The differences between the two categories of authentication, if any, seem to lie mainly in the target applications, not so much in the nature of the problem. As long as the user has the right to choose whether or not his or her ID Card should also provide PKI support for secure transactions over the Internet, I think this is a very good extension to have in our new ID Card.

5. No Urgency for Electronic Purse

Although technologies that turn a smart card into an electronic purse (or *e-purse*) are already quite mature, I see no urgency to introduce this function to the new ID Card, at least initially. The primary function of an ID Card should remain to be for user identity authentication, including PKI-enabled authentication schemes using digital certificates and digital signatures for secure transactions over public networks.

THE END