Security Features of the SMARTICS in Response to Amendments of the ROP Ordinance

Professor Kwok-Yan Lam

11 October 2002

From the security and privacy angle, the SMARTICS system is required to include the following features:

- Access control to ensure that the ROP data is not disclosed in an unauthorized manner when they are being transmitted over the network or stored in the database.
- ROP data stored in the smart chip of the ID card cannot be accessed and modified in an unauthorized manner after the ID card is issued to the card holder.
- Thumbprints being captured for identity verification cannot be used for other purposes not authorized by the ROP Ordinance.

The SMARTICS system addresses the above requirements by means of a combination of a security infrastructure, a sophisticated card operating system and widespread adoption of tamper-resistant card-receiving devices. Besides, additional security feature is included in the smart ID card to cater for contingent situations when the security of the underlying cryptographic algorithm is in question.

The security infrastructure implements and enforces stringent control of access to ROP data when they are stored, processed and transmitted by the SMARTICS system. Access control and communication security are provided by a combination of privilege management technology and end-to-end security schemes. The adoption of end-to-end security ensures that ROP data transmitted over the government network, i.e. from the issuing offices to the main servers at ImmD HQ, are protected by strong encryption and cannot be intercepted in the course of transmission.

The MULTOS card operating system which is adopted as the card platform of the smart ID card, provides built-in security mechanisms to segregate multiple applications resident on the chip of the smart card. It also provides mechanisms for securely loading and deleting applications to/from the chip at the post-issuance stage of the card. These security features ensure that the smart ID card may support multiple applications without worrying interference among on-card applications (interference refers to the situation that one on-card application accesses data belonging to another on-card application). Furthermore, future loading and deleting of on-card applications can only be conducted by parties authorized by the SMARTICS system. For on-field use of the smart ID card i.e. when the ID is being used for verifying identity of the card holder, sensitive activities, e.g. capturing of thumbprint, are conducted within a physically secured environment such that attempts to access the sensitive data by tampering the device will lead to erasure of the data inside the device.

To summarize, the SMARTICS system adopts a combination of security technologies to implement security and risk management features to meet the security requirements of the ROP data. The use of smart card technology allows the future ID card to possess stronger forgery prevention capability. The adoption of the MULTOS card operating system allows multiple applications to co-exist in the card chip in a secure manner. The use of tamper-resistant technology provides physically secured environment for processing of sensitive data such as thumbprint templates captured from the card holder.