

Letterhead of HONG KONG INSTITUTION OF ENGINEERS

Submission From Information Technology Division, The Hong Kong Institution of Engineers for the LegCo Panel on Security

HKSAR Identity Card

General Comments

- We support the position that a smart ID card system with multi-application capacity would provide a new infrastructure for innovative IT applications.
- The smart ID card should be divided into a basic core, containing "backbone" information essential to identity authentication purposes, and an optional component that enables the development of open applications in the future. Residents should have complete freedom to decide whether to engage any optional applications.
- The confidentiality and security risks of the data stored on the smart ID card should be fully analyzed. Risks due to fraudulent or illegal usage of the core data should be comparable to the risks experienced in the current ID card system. The public should be properly informed of the risks involved in the usage of optional applications enabled by the smart ID card.
- The smart ID card should be designed to allow for interoperability between different Government (and for optional applications, between different enterprise) systems. A feasibility of the interoperability feature and its impact on various operations of the Government should be studied.
- Monitoring and ensuring proper usage of the data stored on the smart ID card should be a continuing process. The public's concern on this issue should be carefully addressed. Efficient dissemination of relevant information on users' rights and proper card usage is of great importance.
- The smart ID card system has a stated goal of enhancing Hong Kong's financial infrastructure and to promote the development of e-commerce. The Council should also consider the positive impact of such a system on local IT development. The Government should consider the question to what extent local IT industry would be able to contribute and participate in the development and delivery of the proposed system. In particular, the Government should encourage the development of optional applications locally.

Other Countries' Experiences

- It is very important that Hong Kong should learn from the experiences of other countries. Very few countries have adopted the smart ID card system; the underlying reasons should be studied carefully.
- In this vein, it is worth noting that the Taiwanese and Malaysian pilot experiments on smart ID cards (in 1998/99) were not that successful. We were told that both countries have pended the initiative at the moment. Some people consider their systems to be too ambitious. Their experiences should be valuable input to Hong Kong.

Common Pitfalls

- "Technology" is not the major hurdle. The pitfalls would most likely come from human issues such as improper card usage, and most importantly, the implementation process.

Recommended Approach

- To ensure successful implementation, it is recommended that there should be initial trials limiting usage to a small pool of the population. Similarly, optional applications should be introduced gradually to minimize risks due to unforeseen problems.
- The Octopus system is a good example of how to introduce a smart card technology. The application was very focused at the very beginning. Diversification comes only when the system has been widely accepted and the technology has become more mature.

Technical Issues

- The life cycle of smart card technology is very short, a typical figure is six months.
- No smart card is perfectly secured.
- The success of this project will definitely be affected by developments in the smart card technology. Some people hold the view that the Government should wait until the emergence of an open standard e.g. EVM in 2006.
- Adequate attention should be given to interoperability and compatibility issues.
- The technical requirements are not clearly defined in the Brief.
- The development path and the overall life cycle cost should be considered in details.
- Data synchronization is a general issue applicable to the databases in the all smart card systems. To guarantee data accuracy, updates have to be error-free

and require relatively short latency. A reasonable objective is to achieve manageable latency over a technically advanced architecture and to provide latency bounds so that application developers are fully aware of the system capability and limitations.

Contact Vs Contactless Card

- Contact card has high error rates due to the possibility of multiple contacts (dirts, etc.). Theoretically, they can last for ten years but in practice they usually only last for three to four years.
- Contactless card is relatively slow and presently does not support PKI. This should not be considered as a hurdle in adopting this technology. It is expected that this would become a key development area in where the local IT industry may prosper.

PKI Encryption

- PKI encryption is a desirable feature and it allows multi-agency compatibility and multi-sourcing benefits.
- By the time the smart ID card is in production in 2004, there is a possibility that a system with 2048-bit key length is needed to provide adequate protection.
- At present, the e-certs issued by Hongkong Post have to be updated annually at a cost. The fee structure of e-cert services has not been announced.

User option

- The Brief suggested that "...adoption of a smart ID card with multi-application capacity also presents us with a unique opportunity to enhance our financial infrastructure". Will the Government consider reserving capacity in the smart ID card for other non-financial or commercial applications, e.g. Air Mileage Record?
- Reserving capacity for commercial application will definitely promote electronic transaction and worth further study. The liability issues have to be investigated carefully.
- We support that if the smart ID card will serve multi purposes, the card holders should have a discretionary choice on the optional applications on offer.
- Optional applications should be purely optional. However, there is a possibility, no matter how remote, that some service providers may restrict services only through the smart ID card, thus restricting the user option. The implication of this should be studied.

Presented by Ir Prof Wing Wong, the Information Engineering Discipline Representative and Ir Jolly Wong, the Past Chairman, IT Division at the Special Meeting of the LegCo Panel of Security on 11 November 2000

IT Division Study Group on the HKSAR Identity Card

Convenor

Ir Jolly Wong Past Chairman, IT Division

Members

Ir Prof Wing Wong Information Engineering Discipline Representative

Ir Raymond Ho Past Chairman, IT Division

Ir W F Chan Past Chairman, IT Division

Ir Albert Chu Committee Member, IT Division

Ir Lee Wan-lik Committee Member, IT Division

Ir Dr L M Cheng Member, IT Division

Ir K C Lai Hon. Secretary, IT Division