LC Paper No. CB(2)715/00-01(02)

Information paper on
18 January 2001

Panel on Security of the Legislative Council

Progress of the Consultation Campaign on the HKSAR Identity Card Project

INTRODUCTION

This paper reports on the results of a consultation campaign launched recently by the Administration in respect of the new identity (ID) card project.

BRIEFINGS TO DISTRICT COUNCILS

2. The first part of the consultation campaign was conducted from 26 October 2000 to 5 December 2000 by way of briefings to the 18 District Councils. Representatives of Security Bureau, Information Technology and Broadcasting Bureau and Immigration Department (ImmD) attended District Council Meetings to explain the need to introduce a new generation of ID cards; the reasons why a smart ID card with multi-application capacity was preferred; what types of immigration applications and other non-immigration applications could be included on the new ID cards; which data items would be printed on the card face or held in the chip; six initial versions of card face design; benefits brought by the new ID cards; measures that would be taken by the Government to protect card security and data privacy; and general arrangements regarding the region-wide ID card replacement exercise.

3. All eighteen District Councils indicated support in principle to the new ID card project.

4. At the District Council meetings, the most frequently asked questions were related to -

- card face design
- the cost for replacing lost and damaged smart ID cards

- durability and capacity of the smart ID card
- technical system options and card options
- data privacy and card security
- possible inclusion of other additional data in the chip (e.g. blood group and medical record)

EXHIBITIONS

5. The second part of the consultation campaign was conducted in the month of November 2000. It consisted of 7 roving exhibitions in shopping malls (including the Immigration Tower) and the launching of a web page on the new ID card project at Immigration Department's web site. Through these activities, we were able to promote public understanding on the proposed multi-application smart ID card and gather their views.

6. During the exhibitions, video documentary explaining the features of the new ID card were shown, posters were displayed, information booklets were distributed and the public were encouraged to vote on the card face design. A team of immigration officers was present at the scene to answer questions and to take note of suggestions. About 31,600 persons attended the exhibitions and some 21,700 votes were cast on the card face design. Amongst them, 6,600 votes (30%) were cast on the design at Annex I. Those who favoured the design were generally of the view that its colour was much softer than the other samples and that it was more gender neutral. They also felt that the background pattern (bearing a HK-shaped design) would provide a more modern and business-like appearance.

7. Some 236 visitors to the exhibitions also gave comments and suggestions primarily on the following issues -

- card face design and card material
- support for a multi-application smart ID card
- privacy protection and security measures
- suggestion of additional data in the chip (e.g. blood group, medical record, organ donor status and next-of-kin information)

ID CARD WEB PAGE

8. From 1 November to 5 December, over 78,400 visits to the ID Card web page were recorded. Around 39,400 votes were received and about 19,000 of them (48%) were in favour of the card design at Annex I. Furthermore, 397 e-mails were received. Most of them were related to opinions on card face design. Other comments touched on measures to protect data privacy and card security and the possibility of putting additional data in the chip.

9. Issues raised by the District Councils and the general public together with the Administration's responses are summarized at Annex II.

SPECIAL MEETING ON 11 NOVEMBER 2000

10. Separately, at the special meeting of the Panel on Security held on 11 November 2000, all the professionals and academics attending the meeting expressed clear support for the smart ID card project. Specific questions raised by some of them requiring our responses and the Administration's responses are summarized at Annex III.

COMMENTS

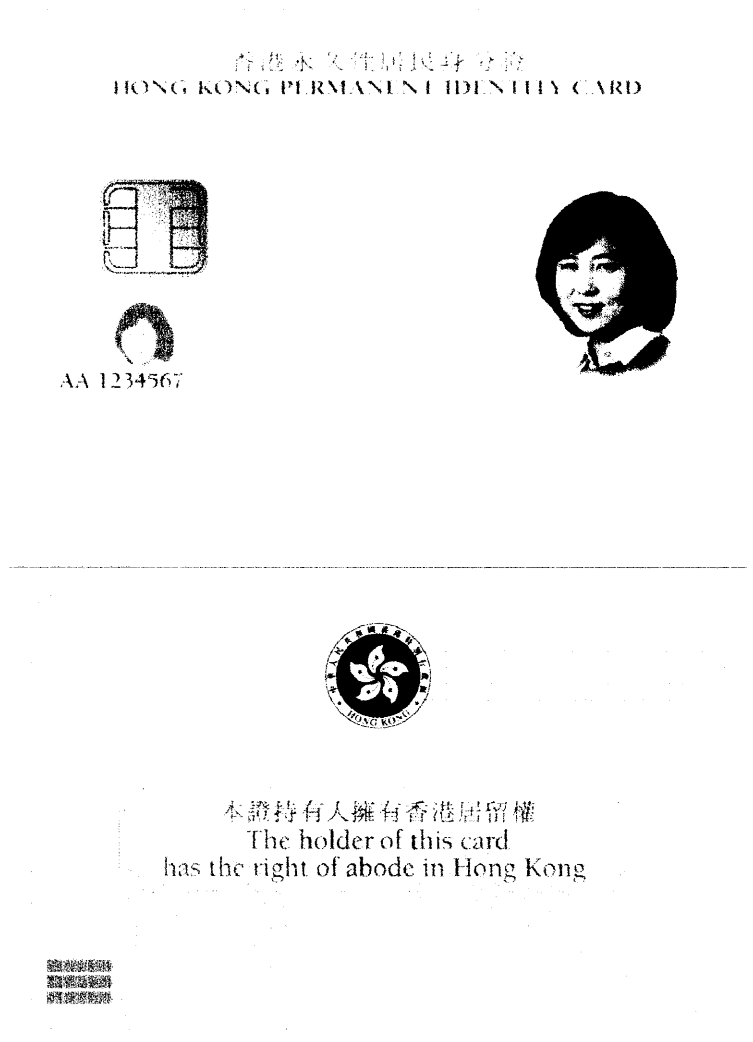
11. Judging from the responses received in the consultation campaign, we can conclude with confidence that there is a strong public support on using a multi-application smart ID card. Although there are concerns on data security and data privacy, the public are in general content with the data protection measures proposed by the Administration. The Administration will ensure that adequate security and privacy protection measures are taken to address the concerns, including liaising closely with the Privacy Commissioner for Personal Data.

12. The polling result on the card face design reveals that the majority are in favour of the design at Annex I. The Administration will take this view into consideration when finalising the design.

Security Bureau
15 January 2001

Annex I

New Identity Card Design No. 6



香港永久性居民身份證
HONG KONG PERMANENT IDENTITY CARD

AA 1234567

本證持有人擁有香港居留權
The holder of this card
has the right of abode in Hong Kong

General Concerns from the Public/District Councillors (DC)

Privacy and Security Concerns	
The Public/DC's Concerns	**ImmD / Government's Reponses**
1. Will the new identity card contain a lot of data?	➢ No. Only the personal information printed on the surface of your existing card, your fingerprint templates, and condition/ limit of stay for non-permanent residents will be stored in the new ID card. ➢ For other value-added applications, only minimum data will be stored in the card and the data will mostly be kept in the back-end computer systems.
2. Do I need to worry about my data privacy? Have I the choice on the value-added applications?	➢ No. Your data privacy rights are protected by law. ➢ Possibly with the exception of the driving licence, you can decide whether or which valued-added applications you want to include in your ID card.
3. New ID card more secured? What measures will be adopted to enhance the security of the entire ID card system? What security features will be incorporated in the card to protect data privacy?	➢ Yes, we will use advanced technology and sophisticated anti-forgery techniques to produce the new ID cards. ➢ The data in the chip and the use of thumbprint identification technology will provide added assurance that you alone can use your identity card. Sophisticated cryptographic techniques will also be employed. ➢ ImmD has engaged consultants to conduct risk assessment and specify the security requirements for the new ID card system. The study covers not only the ID card itself but also at hardware, software and application levels.

4. Will the smart ID card project enable Government departments (particularly law enforcement agencies) to share personal data of citizens more rigorously?	➢ No. There will not be any sharing of data among Government departments. ➢ Data stored in the independent computer systems of the individual departments will continue to be stored separately. ➢ Data to be stored on the smart ID card will be segregated by separate memory area with strong partitions and different access keys. ➢ Data protection principles set out in the Personal Data (Privacy) Ordinance (in particular regarding transfer of data) and the relevant legislation will continue to be strictly adhered to.
5. How can individuals preserve their privacy rights if data of the ID card is accessed and used by other law enforcement agencies?	➢ The access and use of data by other law enforcement agencies must be properly authorized by law. The public need not worry as there are clear provisions in the Personal Data (Privacy) Ordinance to guard against abuses. Besides, only minimum data are stored on card (see item 1).
6. Will the convenience of electronic authentication by smart ID card make it the norm that biometric verification is required for all Government services?	➢ Biometric verification may be required for accessing sensitive data and performing functions, such as the Automated Passenger Clearance at Immigration Control Points. Not all functions would require biometric verification automatically, e.g. borrowing a book from the public libraries may not require biometric verification.
7. Will the new ID card system guard against the use of synthetic devices in the extreme, mutilation of body parts by malicious people for the purpose of gaining access to the data/system?	➢ These risks can be avoided by letting the system execute some anti-spoofing checks, e.g. check the body temperature or blood circulation.
8. Will my personal data in the chip be exposed if I lose my ID card?	➢ No. Nobody can read your data as he does not have your thumbprint. ➢ The personal data will be encrypted and stored in an encrypted form which cannot be read by unauthorized persons.
9. What safeguards are in place to make sure that the data on the card cannot be read by unauthorized persons?	➢ Data of the individual applications are strongly encrypted and segregated with strong partitions and different access keys. They will be protected by using cryptographic data integrity. Only authorized persons will be

	able to read the data that he is authorized to read.

Card Face Design	
The Public/DC's Concerns	**ImmD / Government's Reponses**
1. Why don't you make an open competition for the card face design of new ID card?	➢ In addition to tight project schedule, we need to consider not only the layout and card face of the new ID card but also the incorporation of maximum security features in each of the designs against alteration and forgery. ➢ Apart from having professional artistic experience, designers must have relevant knowledge in security printing, using synthetic material, laser engraving technology and forgery-proof technique. Therefore, it is difficult to meet the requisite standard through an open competition for the card face design.
2. What is the material for the new ID card and why is it chosen?	➢ Polycarbonate is the preferred card material. ➢ Compared to other synthetic materials, polycarbonate offers the highest resistance to mechanical, chemical and thermal stress as well as to environmental influences, ensuring long durability of all its features. ➢ According to experience gained in laboratory tests, only polycarbonate cards offer the durability of 10 years or more necessary for an ID card.
3. How long will the smart ID card last?	➢ The durability of the card depends on the choice of the card material, the chip and most importantly, how the card is used. ➢ We have chosen the most durable material which can last for more than 10 years. For the chip, vendors claim that the chip can also last for 10 years and support 100,000 read/write transactions. Theoretically the card can last for 10 years under normal usage.
4. Will different colour schemes be used on the smart card for male and female residents?	➢ The introduction of different colour scheme may be viewed by some as inducing discrimination among male and female residents. We have to consider this proposal carefully.

Technical System Options and Card Options	
The Public/DC's Concerns	**ImmD / Government's Reponses**
1. Which countries also use multi-application smart card system?	➢ Regarding the multi-application smart ID card system, Finland has started issuing their smart ID card in end 1999. Brunei has started issuing smart ID card in July 2000 and Malaysia in September 2000. Israel plans to issue smart ID card by end 2000. Macau, Italy and South Africa also have plans to issue smart ID cards next year. *[Please refer to the paper on "Experience of Using Smart Identity Cards in Other Countries/Places".]*
2. What is the life expectancy of the new system?	➢ The life expectancy of a system depends on the type of equipment used. Since we have not yet proceeded to the stage of procurement and we do not know what types of equipment will be installed, it is not possible to state precisely the life expectancy of the new system. But it is a normal requirement that a computer system should have 10 years' lifetime.
3. What kind of smart card will be used?	➢ Contact smart card is recommended by the consultants because contactless card currently available in the market cannot support digital signatures and higher memory capacities.
4. What benefits do a smart card has over a non-smart card?	➢ A smart card is more secure and can prevent lost or stolen identity cards from being altered or used by others. ➢ A smart card ensure more efficient and secure authentication of card holder's identity. ➢ A smart card facilitates the introduction of Automated Passenger Clearance and provides the platform and infrastructure for future add-on multi-applications. ➢ Value-added applications can be added to it and the data therein can be updated after it has been issued.

5. It is proposed that a region-wide ID card replacement exercise will begin in early 2003 and complete within 4 years. In view of rapid technological change, will the design of the new ID card and the backend system become outdated when the whole replacement completes in 2007?	➢ When we procure a system, the most important point is that it serves the purpose. ➢ When selecting the equipment, we will have to make sure that the selected product should have upward compatibility and can be further upgraded in the future to keep it up to date with the technology change.
6. How long will it take to get an identity card in the future?	➢ At the moment, it takes 15 working days to issue an identity card. ➢ With the new system, we hope to deliver the identity card in a shorter time span but details have yet to be worked out.

Putting Additional Data in the Chip	
The Public/DC's Concerns	**ImmD / Government's Reponses**
1. Will the public have the choice of additional applications?	➢ Apart from immigration-purpose applications and possibly with the exception of the driving licence, card holders can have the right to choose whether or which additional applications will be added to their cards.
2. Can ID card be used as an entry permit to the Mainland?	➢ Technically, it is feasible to store the data on the Home Visit Permit in the chip of a smart ID card. ➢ However, it is too early to say if this idea is workable as there are a host of complicated issues to be considered, e.g. the difference in legislation between Hong Kong and the Mainland, whether the Mainland authorities can set up a compatible system to cope with the change, public view, etc.
3. Will blood group, organ donation card, health and medical record be incorporated in the smart card?	➢ While these are not proposed as early applications, they could be considered at a later stage if the public are in favour of this idea.

Inquired about the replacement cost for lost and damaged smart ID card	
The Public/DC's Concerns	**ImmD / Government's Reponses**
1. What is the fee for a replacement of smart ID card?	➢ Cards issued under the region wide ID card replacement exercise will be free of charge. ➢ As for other replacements due to loss or damage of card, fees will be levied. ➢ Detailed costing is not available. Approval from LegCo will be required for any fees adjustments.
2. Why the existing ID cards need to be replaced?	➢ The existing form of ID card was introduced in 1987 and the supporting system was installed in 1982. ➢ With the passage of time, both of them have become aged and outdated. The use of counterfeit or unlawfully obtained identity cards has been detected from time to time. ➢ This calls for the need to replace the existing ID card and supporting computer system.

Inquiry about the durability and capacity of card	
The Public/DC's Concerns	**ImmD / Government's Reponses**
1. Will the chip of the future smart ID card be damage if it is stored or kept together with another contact smart card?	➢ No. But the public will be reminded to take good care of their new smart ID cards through publicity campaign and intensive programmes as the ID card is an important document.
2. Will the data/programs inside the chip be lost if there is a magnet closed to the chip?	➢ No. Vendors claim that the functioning of the chip will normally not be affected by a magnet.
3. What is the optimum temperature range and tolerance of the smart ID card?	➢ The card material (polycarbonate) to be used for the smart ID card can endure high temperature range from -40°C to +120°C.
4. If the new ID card is used for multiple purposes, will it lead to the frequent replacement of ID cards?	➢ According to vendors, if the smart cards are properly handled, it can support 100,000 read/write transactions. Increased usage should not lead to chip failure and the replacement of ID cards.

Other views suggested	
The Public/DC's Concerns	**ImmD / Government's Reponses**
1. Does it mean that some people will lose their ROA as a result of the region-wide ID card replacement exercise?	➢ Under the law, Chinese citizens will never lose their right of abode as long as they remain Chinese citizens. ➢ Non-Chinese nationals may lose their right of abode only if they have been absent from Hong Kong for a continuous period of 36 months or more. ➢ Persons working or studying overseas but maintaining their home base in Hong Kong will not be regarded as being absent from Hong Kong.
2. What criteria will Immigration department use to determine their eligibility to continue to hold a PIC?	➢ The ID card replacement exercise will work on a trust basis. We will publicize the circumstances under which a person will lose his ROA and it is up to the PIC holder to report to us if he considers that he may have lost his ROA.
3. What will happen if a person is unable to enroll because of deformity or physical injury?	➢ If a person is unable to use his thumbprint to enrol, the prints of other fingers will be captured. ➢ In case the person cannot enrol with any of his fingerprints or has no finger at all, this fact will be recorded and an indicator will be included in the smart card to denote this. Details will be worked out in the detailed design stage.
4. In the case of non-enrolment, can the person concerned enjoyed the automated passenger clearance system?	➢ The automated passenger clearance works on the basis of matching of fingerprints. If a person cannot enrol with any of his fingerprints or has no finger to enrol, it seems that he may have to resort to the existing form of manual immigration clearance. We will look at this issue further when conducting feasibility study on the automated passenger clearance system.

5. What are the tangible benefits of automated passenger clearance at control points?	➢ More counters will be available for immigration clearance without increase of staff since one immigration officer can man a few counters at the same time. ➢ There will be savings in the number of counter officers. ➢ Fingerprint matching is a more secured means of authentication.
6. How will the automated passenger clearance system operate?	➢ When a traveller presents for immigration clearance, he will have to insert his smart ID card into a reader and apply his live thumbprint on another reader. The matching of thumbprints will then be conducted. If there is a match, the card holder will be allowed to pass through the counter. Otherwise, he will be stopped for further enquiries.
7. When will old card be replaced?	➢ A regional wide replacement exercise will commence from mid-2003. ➢ All ID cards will be replaced by phases according to age groups. Replacement exercise to complete in 4 years' time.
8. Why are the public not given a voluntary choice to incorporate driving licence in the smart ID card?	➢ The use of a driving licence is very often accompanied with the need for identification. So, there are duplicating functions between an ID card and a driving licence. To minimize the operational inconvenience arising from the need to maintain a dual system, we consider that incorporation of the driving licence onto the smart ID card should best be proceeded on the basis that no separate paper-based driving licence should be issued. ➢ In many countries, the driving licence is also issued as a proof of identity documents.

Response to Hong Kong Computer Society's (HKCS) Submissions

Points made by HKCS	**Administration's Response**
The policy should set the use of the smart card as a **storage device for personal identity data only**, in support of facility at application level to verify personal identification and authenticate personal identity.	It is our goal to store minimum data on the smart ID card. Personal identity data (e.g. name, DOB, etc.) will be stored on the card to facilitate the electronic authentication purpose. Most application specific data would be stored in the back end systems of the Government as with the current practice.
There will be a need to pay particular attention to the issue of **data ownership**, and the **rights and obligations of the data subjects**.	We will strictly comply with the data protection principles set out in the Personal Data (Privacy) Ordinance.
It is necessary to set some legal guidance as to the **data subjects' rights and onus of proof**. In particular, it should address specific issues associated with the onus of proof of use of the card in terms of a transaction, or in terms of binding the "digital signature" to a document.	We will strictly comply with the data protection principles set out in the Personal Data (Privacy) Ordinance. We will consider legislative amendments where appropriate. The legal status of digital signature has been clearly defined in the Electronic Transactions Ordinance (Cap. 553)

Points made by HKCS	Administration's Response
There will be a space for storage of personal data that is not initiated or collected under Ordinances e.g. credit card or bank account details. In such cases, there is a need to provide policy guidance as to **data ownership**, and legal implications arising from, or in connection with, the use of such data by non-Government related transactions, bearing in mind the card, as a data storage device, is owned by Government.	Noted. However, among the early applications, we do not propose any non-Government applications which would hold such personal data.
The Legislative Council Brief seems to have insufficient coverage of the issues associated with **risk management and information security management**. It will be important for Government to set an unambiguous and practical framework for managing risk and security.	The Immigration Department has contracted security specialists to define the security requirements for the new system. As part of the study, they will provide recommendations on risk management and information security management.
There is rapid technology advancement that could make **evaluation of options** difficult. Further complexity could arise from the fact that there will be substantial resources necessary to run both the new HKSAR identity card system and existing ROP system over an extended time frame.	We appreciate the difficulties in evaluating different options and we will make careful considerations in assessing the proposals from vendors. It is unlikely that we will have to run both old and new system over an extend period of time as we will arrange for migration of the old database to the new system. All ID cards issued after a designated date will be in the new smart card format.

Questions	Administration's Response
What is the expected life of a smart card and the supporting computer system that the feasibility study was based upon?	The feasibility study has recommended a card material that last for at least ten years and the chip can also support ten years. As for the supporting system, there is no expected life provided as it is our usual practice to upgrade the system from time to time and it would be difficult to explicitly state an expected life of a system.
Is there any particular reason for the proposed development and testing phases to elapse from June 2001 to November 2002 ?	We hope to award the contract for the new system in mid 2001 after which development and testing can start. As we need to implement the new system in early 2003 when the current system becomes obsolete, we hope to complete the testing in end 2002.
Any idea how stress testing of the system will be planned and conducted?	For the smart card system, stress testing includes testing of the durability of the card and performing load test on the system. For the smart card, the card manufacturers and Government Laboratory will both conduct stress test on the cards. As for load testing of the system, it is our normal practice to test the performance of the system at full loading. When doing so, we will deploy a certain number of terminals to generate workload as well as generating transactions by the system to simulate the live environment. More than one load tests will be conducted.

Questions	**Administration's Response**
What would be the likely size of the pilot phase?	Pilot is usually conducted for two purposes, viz. testing of usability and smoothing out corners before implementation. On the testing of usability, as we have already conducted a comprehensive market research during the feasibility study stage and we will also tap on the experience of other large smart card installation, we will not be conducting pilot for this purpose. As for smoothing of corners, instead of conduct a pilot, we will have prototype at the design phase to make sure that the card and system is usable. Before the system goes life, we will also conduct trial runs to ensure the system and procedure are all properly in place and working smoothly.
Is there any scope for shortening the ID Card replacement exercise?	We have considered shortening the replacement exercise but substantial resources will have to be added, thus making the exercise not cost-effective. Since a four year replacement exercise already required a daily throughput of 8,000 cards per day, shortening the replacement exercise will easily lead to a bunching effect which will be difficult to manage if there are disruptions to daily work, i.e. typhoon, black rain storm etc.

Questions	Administration's Response
Is there a breakdown available in support of the cost estimates, especially in relation to the staff costs of $943 million for 364 staff who will be appointed to time limited posts?	The 364 time limited posts are mainly Immigration in-house staff who will be deployed to manage the system development as well as running of the new identity card re-issue centers during the four year replacement exercise. It also includes a number of ITSD staff who will provide technical support and advice during the system implementation period.
What will be the controlling measures to ensure successful and smooth project implementation?	There are standard control procedures in place in government to control project implementation. Indeed, ImmD has sufficient experience in implementing world class systems, e.g. control point system, passport system, and there should be no problem for them to implement the new ID card system.
What is the reason for storing two thumb prints?	This is for redundancy purpose. The smart ID card will support the future Automated Passenger Clearance system whereby the thumbprint will be used to authenticate the card holder. An additional thumbprint will be useful if one thumbprint is not readable because of injury or other reasons.

Response to Hong Kong Institution of Engineers' (HKIE) Submissions

Points made by HKIE	Administration's Response
The confidentiality and security risks of the data stored on the smart ID card should be fully analysed.	We have contracted consultants to look into these areas.
The smart ID card should be designed to allow for interoperability between different Government systems.	Will comply through the adoption of open industry technology standards.
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.	Will look into this issue. Tender invitations will be open to all.
It is recommended that there should be initial trials limiting usage to a small pool of population.	We will conduct trial runs before the system is implemented. The region-wide ID card replacement exercise will only be carried out after the system is up and running for sometime and a certain number of cards are issued.
Similarly, optional applications should be introduced gradually to minimise risks due to unforeseen problems.	It is our aim to implement additional applications in a prudent and gradual manner.
The development path and overall life cycle cost should be considered in details.	Already considered in the feasibility study.
Data synchronisation is a general issue applicable to the databases in all smart card systems.	This will be looked into at the system design and development stage.

Points made by HKIE	**Administration's Response**
Contact card has high error rates due to the possibility of multiple contacts. Theoretically, they can last for ten years but in practice they usually only last for three to four years.	Terminals where cards may be frequently inserted may consider using landing contact technology (not wipe contacts). This will significantly extend the life of the cards. Developments in materials and the smart card chip itself now allow the possibility of an extended life.
Contactless card is relatively slow and presently does not support PKI. This should not be considered as a hurdle in adopting this technology.	Contactless card was not at present recommended partly because it cannot support digital certificate and partly because of privacy concerns.
At present, the e-cert issued by Hong Kong Post have to be updated annually at a cost. The fee structure of e-cert services has not been announced.	Noted. Will be addressed separately.

Response to Hong Kong Information Technology Federation's (HKITF) Submissions

Points made by HKITF	Administration's Response
The protection of security and privacy is of vital importance and must first be addressed. We must remember that there is no 100% security in any system, we must target 100% risk management to strike a balance.	We fully agree with this and will pursue 100% risk management.
The government should take the Keep It Simple Steady (KISS) approach in project implementation to avoid any pitfall.	Will comply.
The smart ID card be used for personal identification only and storing only the minimum essential data on the card. Any other nice to have transactional data should be stored outside the ID card in a secure system. We suggest the use of 'contact type' cards to eliminate the risk of unauthorised information retrieval using a wireless device.	We will only store the minimal necessary data on the card. Our consultants also recommended us to adopt contact smart card.
The project be "start small" so that the project can be manageable and gets moving promptly. Then, scale up the project to include applications after Hong Kong people have built up their confidence in the smart ID card. A prudent system implementation plan with close monitoring and constant reporting is required. Increasing the project transparency is of equal importance to gain user acceptance and co-operation.	Will comply. We plan to scale up the project after Hong Kong people have built up their confidence in the smart ID card. The project will be closely monitored and there will be wide consultation, education and publicity to gain user acceptance and support.

Points made by HKITF	Administration's Response
As an integral part of the global economy, the success of Hong Kong depends on the innovative use of information technology. Provision of community and financial infrastructure (such as e-purse and library card) should be encouraged. But this extra data must be stored in a separate and optional daughter card.	Extra applications, e.g. e-purse and library card, will be optional applications for the card holder to choose for including in the card, if pursued. The use of daughter card will need further exploration.
The intelligent ID card system is mature. It is imperative for the success of the project that there is a keen sense of timing and should not be delayed any more.	As the current ID card system need to be replaced by 2003, we aim for early introduction without any delay.

Response to Motorola's Submissions

Points made by Motorola	Administration's Response
Chips itself are rarely the cause of failure. Failure in the long term is due primarily to material degradation in how the chip is bonded to the card and cardholder treatment of the card. The latter is a function of flex and exposure to the elements such as washing machines.	Noted. We will be using a card base material that will last for over ten years. Proper care should be taken with the card. This will also be addressed through education and publicity.
Library card – This contains only an account number. Converting to a smart card would require all libraries to upgrade their systems as well as with no incremental benefits.	The exact implementation details and cost benefit analysis would be subject to separate feasibility studies.
It becomes necessary for a third party agency to broker the consolidated requirements.	The Steering Committee on Multi-application Smart ID Card chaired by the Secretary for Information Technology and Broadcasting would coordinate implementation of the multi-application smart ID card.
It is good business practice to have one agency to assume primary responsibility for cardholder support irrespective of how many applications are on the card.	ImmD will continue to be the card issuer. An overall scheme operator will be designated to take care of the technical aspect of the card system, e.g. certify equipment, help-desk, etc. Individual government agencies would be responsible for their own applications, so as to help address concerns relating function creep and privacy.
Role-based security …. is highly complex as the authorised parties must be registered and issued credentials so the card can authenticate the request.	To ensure proper security of the card regime, high level of security (including card authenticating the reader) is necessary.

Response to Professor D Y Yeung's Submissions

Points made by Professor Yeung	Administration's Response
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, …. As the Government makes more and more of its services available online.	Agreed. Security concerns addressed by technology (e.g. firewall and public key infrastructure) and procedure. Privacy concerns addressed by the Personal Data (Privacy) Ordinance and related Code of Practice. ImmD will consult the Privacy Commissioner for Personal Data in formulating the data protection measures.
We should take a holistic approach to improving the overall security level of the entire system.	Agreed
Offline biometric authentication is preferred because there is no need to transmit sensitive biometric data over the network for cardholder verification.	Will consider
I see no urgency to introduce (electronic purse) 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.	We are only reserving the capacity on the smart ID card for electronic purse, as the smart ID card will likely last for some years. Issuance of e-money would only be considered when it is necessary from public point of view, and will be subject to separate feasibility study and public consultation.

Response to Dr L M Cheng's Submissions

Points made by Dr L M Cheng	**Administration's Response**
Life time – will not meet the 10 year requirements	Developments in materials and the smart card chip itself now allow the possibility of an extended life. We will be using a card base material which guarantee a life time of over ten years and the chip can guarantee 100,000 read/write cycle.
Security issue – smart card currently is not entirely secure	After a formal risk analysis has been performed, a minimum evaluation level and security profile can be specified for the smart card to give public confidence that it is suitable for the task from a security standpoint. There are currently two main mutually recognised security standards that smart cards are evaluated : ITSEC and Common Criteria. Many smart cards have either received accreditation to these standards or are in the process of accreditation. As security is a significant feature of smart cards, all device manufacturers and platform developers are continuously working to improve the security of their products. Establishing local production fabrication plants is not an answer to security issues because the benefit of wide international scrutiny of the underlying technology platform will be lost.

Points made by Dr L M Cheng	Administration's Response
Multiple applications – ambitious but not practical	Other organisations, e.g. financial institutions and telecommunication companies are launching multi-application cards on a wide scale. It is a worldwide trend for smart card technology to support multi-applications. Given that the ID card is a very important identity document, we will implement the multi-application smart ID card in an incremental manner.
1. It is not a compulsory requirement	1. Non-immigration applications are voluntary (probably except driving licence).
2. There are alternative cheaper solutions	2. The solutions provided by the smart ID card will be of greater efficiency and higher quality and bring greater convenience to the public.
3. Overall administration, granting and defining of a protection common mechanism for multiple application file allocation can be a problem.	3. We reckoned the need for comprehensive and secure card management scheme for a multiple application card. We will conduct a consultancy study to study the requirements in detail.

Points made by Dr L M Cheng	Administration's Response
4. Mixing of secured and non-secured data can be a potential security risk	4. Yes, this is a potential risk which needs to be managed through risk analysis and security specification and design. Modern multi-application smart cards provide advanced firewalls between applications to ensure that one application cannot interfere with, or access, another's data. Within an application, the design of the application itself should ensure that the accidental release of confidential data does not occur. A well-designed application running on a secure multi-application platform does not represent a security risk.
5. The future EMV Smart Card Payment Infrastructure compatibility cannot be easily resolved.	5. EMV has little relevance to this project.
6. The lost card percentage increases	6. It is just a speculation without any figure to substantiate. Indeed, if the card has more value-added functions on it, the card holder should be more careful in handling it and the lost card percentage may even reduce.

Points made by Dr L M Cheng	Administration's Response
7. No sharing of database will not maximise the IT benefits and will not promote effectiveness between government departments	7. There will not be sharing of database. This is in line with community expectations. The smart ID card will provide a vehicle for Government to provide more efficient, quality and convenient public service (e.g. minimizing in-person transactions and introduction of automated passenger clearance etc). It will also contribute significantly to the enhancement of the information infrastructure in Hong Kong.
Is it the right thing for the HKSAR Government takes the lead in introducing compulsory multiple applications ID card and creates disturbance to the free market?	For the great majority of non-immigration applications, cardholders will be offered a genuine choice. We will not interfere with the free market as the initial applications are confined to Government applications only.

Frequently Asked Questions floated by Dr L M Cheng	**Administration's Response**
1. Can ID cards help to control illegal immigration?	The primary purpose of requiring ID card in Hong Kong is to combat illegal immigration.
2. Do ID cards facilitate an increase in police powers?	No. Police checks on ID cards are conducted in accordance with law. The change in the format of the ID card will not lend to any increase in Police powers.
3. Do ID cards facilitate discrimination?	No. All legal residents in Hong Kong have ID cards and there is no question of discriminating checking.
4. What happens if an ID card is lost or stolen?	ImmD will issue a receipt to a card holder who reports loss of his card. This can be used in lieu of an ID card. One-stop service will be provided for replacement of ID cards and the applicant will not have to approach different government departments to reload their applications. The inconvenience caused to the applicant because of loss of ID card will be reduced.
5. What are the privacy implications of an ID card?	In Hong Kong, need for an ID card has been well established. Most Hong Kong residents recognize that it is a convenient means to authenticate their identity in day-to-day life. The Administration recognizes that privacy is an important issue and will take every possible measure to protect the privacy rights of ID card holders.

Frequently Asked Questions floated by Dr L M Cheng	**Administration's Response**
6. Has any country rejected proposals for Smart ID cards?	As far as we know, no country has abandoned its smart ID card project after running it half-way. Taiwan has decided not to take forward its smart ID card project because there were problems with their business model. Their intention to put the operation of the card scheme in the hands of the commercial sector raised privacy concerns.