Letterhead of THE ASIA PACIFIC SMART CARD ASSOCIATION

THE VIEWS OF THE ASIA PACIFIC SMART CARD ASSOCIATION ON THE PROPOSED HONG KONG SPECIAL ADMINISTRATIVE IDENTITY CARD

Smart cards are set to become the premier consumer token for the future, with an expected world card population in excess of 4 billion by the year 2002. Smart cards are unique in their ability to store data securely in a portable card form, whether that data be information or monetary value. Businesses and governments worldwide are therefore starting to use this technology for many different applications where security and portable data storage capability are important. In giving the views of the Asia Pacific Smart Card Association, it may be appropriate to present some background on the increasing adoption of smart card technology by organisations in the private and public sectors.

Currently the world's largest application of smart cards is still the original application of payphone cards for public telephony. This is followed by GSM mobile telephony, the most popular mobile telephony standard. With the advent of third generation (3G) networks and the convergence towards the Universal Mobile Telephone Service (UMTS), all digital mobile telephony will eventually incorporate smart cards. Transit operators worldwide are already following the example of Hong Kong and launching smart card based automatic fare collection systems to reduce costs and provide increased convenience to travellers. Banks and card payments associations are now beginning to migrate their magnetic stripe payment card infrastructures to smart bank payment cards in national implementations, largely as a means of combating counterfeit cards and card fraud. The new world of electronic commerce cannot succeed without the use of smart cards as authentication and payment tokens. From a commercial perspective these market sectors, as well as many other businesses not mentioned here, see two key advantages offered by smart cards. The first is their ability to reduce fraud due to higher levels of security over other card technologies. The second is their ability to securely support multiple applications which can be used to deliver a wide range of value added services to consumers. These points, taken together, provide a means for these commercial organisations to broaden the range of services which they are able to offer to consumers. The above industry sectors, including telecommunications, financial instutions, transit operators and governments, are already now planning or issuing smart multi-application cards for a wide range of applications.

It is therefore not surprising that governments should exhibit an increasing interest in the application of smart card technology. In a growing number of countries, governments and other public sector bodies are now either planning or implementing nationwide schemes including provision of health, ID, benefits and other public and private sector applications. Some of the countries implementing smart cards for public sector applications are well known through the media. Many others considering the use of smart cards have not yet made a final decision or have not yet publicised their plans and initiatives. It is the view of the Asia Pacific Smart Card Association that all countries worldwide will eventually need to consider smart card technology if they plan to modernise government and upgrade the level of public sector services. While an increasing number of countries are likely to make use of smart cards to deliver government services, it is not certain that all countries will include a dedicated identity function simply because many of these countries do not currently make use of a national identity card. Some countries offer an optional ID card to the public and the decision whether or not to convert this to a smart ID card will be based on various factors, many of which are different to the factors faced in Hong Kong. There are also a number of countries which have no dedicated identity card but which use another government issued card as a de facto identity, such as a driving license, and these other government issued cards are likely to be upgraded to smart card cards over time. Lastly, a number of countries worldwide, as well as international travel organisations, are now considering

incorporating smart chips into national passport programmes to secure and facilitate international travel for citizens.

A common requirement of public and private sector organisations that provide services to the public is the need to interact and perform transactions with individuals on a regular basis. These transactions usually take the form of identity verification (who is the individual?), authentication (is the individual allowed to do this?) and authorisation (go ahead and do this). Not all three will always be necessary. Some of the established cardholder verification methods which are used on a daily basis are the signing of a credit card voucher, the inputting of a PIN at an ATM, or the visual matching of a photograph on an identity card with the face of the cardholder. It is now widely accepted that the most secure, effective and reliable card holder verification method is the use of a biometric provided by the card holder and carried by the card holder in a secure tamper-resistant device such as a smart card. Biometrics are able to identify a person with greater accuracy than other technique, they cannot be forgotten and they are difficult to forge. They are therefore being implemented or considered by many governments worldwide as a means to protect individuals and governments against identity fraud, and provide increased convenience for citizens in dealing with the government. The biometric which is expected to be used most widely is the fingerprint. The use of biometrics should involve no invasion of privacy since the biometric will be carried and held by the cardholder. Biometric based systems can be designed which do not require storing of biometrics in central databases (indeed this is illegal in some countries) although Hong Kong has a legacy of storing fingerprints centrally. By storing one fingerprint biometric from each hand, a two level identity verification can be provided to improve accuracy as well as to provide redundancy in case a citizen is unable to use one finger for biometric verification in the future. The concept of biometrics is new and will take some time to be accepted by the general public. Certainly a well designed public education programme will be required to inform citizens about the facts of biometrics and counter sensationalistic reports in the media. In the longer term biometrics are expected to gain public acceptance as commercial organisations also begin to adopt biometrics to improve their cardholder verification methods.

It is the view of the Asia Pacific Smart Card Association (and most other industry analysts) that the future of all card products lies with smart cards which contain microcontrollers and support multiple applications on open multi-application operating systems or platforms. These smart card software platforms also provide upward migration paths to important international smart card standards such as the EMV (Europay-MasterCard-Visa) specification for smart payment card infrastructures and the UMTS (Universal Mobile Telephony Standard). Businesses are already starting to take advantage of multi-application smart cards by locating more that one application from the same card issuer in the same card. It is a prime requirement of these multi-application smart cards that, for security reasons as well as data privacy reasons, applications are kept entirely separate and cannot interfere with other applications in the same card. This requirement becomes particularly stringent in the case where applications in the multi-application smart card are provided by, and interact with, completely separate commercial organisations. Many of these commercial smart card initiatives, particularly those involving financial transactions, have security concerns which are at least as high as those required by governments worldwide. The result is that there are today commercially available multi-application smart cards and multi-application smart card platforms which can support secure multiple applications which are not able to interfere with each other or to gain access to the data used by or stored in other applications in the same smart card. The two most important security standards to which smart cards should be evaluated are ITSEC and the Common Criteria. The *Information Technique System Evaluation Criteria* (ITSEC), published in 1991, are a catalogue of criteria for the evaluation and certification of the security of information technology systems in Europe. The further development of the ITSEC and its combination with various national criteria resulted in the *Common Criteria.* Version 1.0 of the Common Criteria was published in 1996 by the American National Institute of Standards and Technology (NIST). Since

then they have been internationally standardised as ISO 15408. Many smart cards (chips and multi-application smart card software platforms) have either received accreditation to these standards or are in the process of achieving it. Security is one of the most important benefits of smart cards and chip, terminal and device manufacturers and smart card application and platform developers are continually working to improve the security of their products. Before embarking on any smart card scheme, a thorough risk analysis should be carried out and a complete security specification written. This enables all security issues to be properly addressed at the design stage. A properly designed smart card application running in a secure multi-application platform does not represent a security risk. One of the major advantages of the open and secure multi-application smart card platforms which are now becoming prevalent is that they allow smart cards to support secure loading of new applications (and deletion of old applications) to the card over public networks. This enables the smart card issuer to replace existing applications already in the field, without the need to re-issue the card.

The biggest challenge in developing multi-application smart cards for government services will be in designing systems with the long lifetimes required by public sector organisations. It is the opinion of the world's largest smart chip manufacturers that, with the latest developments, the chips employed in smart cards can achieve a lifetime of 10 years. It is also the opinion of the world's largest card manufacturers that there are card materials available that can achieve a lifetime exceeding 10 years. It is important to note that comparisons with the lifetimes of smart cards issued by commercial organisations is irrelevant since these cards incorporate features (magnetic stripes, embossing, low-cost printing) that shorten the life of the card to around 3-5 years. There is also usually no business case for issuing commercial cards with lifetimes of much longer than 3 years. We are now beginning to see the first national government smart card schemes around the world and these have so far been designed for lifetimes of 5 years. With the continual improvements in manufacturing and design processes expected over the next few years, it should be possible to issue a smart card with a 10 year lifetime (subject to correct usage) in 2003. Smart card technology does advance rapidly (although not quite as fast as "Moores Law" which applies more to personal computers). However it is important to note that "Moores Law" does not apply to *Functional Specifications.* The functional specifications for any smart card scheme are determined by the *User Requirements* of the smart card scheme operator, in this case the Immigration Department of the Hong Kong Government. The Immigration Department's user requirements (an ID function) are not expected to change dramatically over the next 10 years. Additional government applications may be developed which may be suitable for loading onto the card and that is a good reason for using a secure, open multi-application smart card software platform. Which secure, open multi-application smart card software platform should be implemented to support these features is one of many decisions that can only be handled at the design stage, not during the preparation of the functional specification. Similarly the decisions on how to implement the security requirements detailed in the functional specification can only be made at the design stage.

A key trend in the development of future government services is the need to be able to deliver services to the public over networks, thereby providing increased efficiency and convenience to citizens, as well as cost savings to the government. Government systems involving remote transactions with citizens require methods which will provide security and integrity. Authentic transaction instructions must not be able to be copied, altered or deleted by fraudsters. Some types of payment also require the payer to be authenticated, and for incorrect repudiation to be defeated. All of the above issues can be solved using a combination of encryption, message authentication, digital signatures and certification. These require the deployment and use of digital certificates, and it is important to protect the associated secret keys from unauthorised access. Hence online government services will require citizens to have digital certificates and these must be able to be carried securely by the citizen from place to place if they are to be able to effect

transactions from any location. The most portable and most secure storage medium for digital certificates is a properly designed smart card chip.

In summary it is the view of the Asia Pacific Smart Card Association that a well-designed multi-application smart card and infrastructure could provide improved government services to Hong Kong citizens. There should be potential for increased services and benefits for cardholders which can be upgraded over time as requirements change. It would be possible to design most of these applications to be optional, and to be loaded onto the smart card at the request of the cardholder. The Immigration Department's smart identity card application and biometrics will provide much greater protection against identity theft than is currently available from the existing non-smart identity card.

It is important to note that the new ID card and infrastructure which will be launched in 2003 will have to last for over ten years. In ten years time it is highly likely that most other governments around the world will have already launched smart card based systems for delivering secure government services, both physically and online. A decision not to incorporate these new technologies now could have important consequences at a later date, both for counterfeiting of identity cards as well as acting as a major impediment to the modernisation of government and the delivery of improved, lower cost services to the public.

I have tried to keep the views in this document as short as possible. I would be happy to answer any questions and provide further information at the special meeting of the Legislative Council Panel on Security on November 11th.

Greg Pote
The Asia Pacific Samrt Card Association