Malaysian Journal of Computer Science, Vol. 10 No. 2, December 1997, pp. 26-31

CONSIDERATIONS FOR A MALAYSIAN CRADLE-TO-GRAVE IDENTIFICATION PROPOSAL

Elok Robert Tee
Jabatan Sains Komputer
Universiti Putra Malaysia
email: robert@fsas.upm.edu.my

ABSTRACT

Presents a model for a Malaysian CGID and broadly reviews its requirements and issues in authentication, data storage, security, authorization, duplication and recovery.

Keywords: Cradle-to-Grave Identification (CGID), smart-card, Internet identification

1.0 INTRODUCTION

The Malaysian national registration ID card (NRIC) is a mandatory document that distinguishes the holder with ID particulars and citizenship status. The birth certificate normally precedes the issuance of the NRIC, the initial ID paper accorded to a person. Other official IDs that are commonly used are the driving license and the passport which is in the form of a booklet or plastic card for restricted work visa to neighbouring countries.

Yet other types are the bank cards. These cards certify the holders as clients of a bank with credit facilities and provide electronic access to funds, e.g. from automated teller machines and via point-of-sales (POS) networks. Commonly used ID includes student, membership and *notification/medical* cards, e.g. the cornea donor card and the diabetic notification card. ID cards are also utilized to gain access into secured buildings or to activate electronic equipment and devices.

These numerous ID papers and cards that are needed for daily uses are susceptible to fraud (against the issuers or individuals), being lost (misplaced or damaged) and are cumbersome to carry. Advancement in information technology (IT) now permits ID requirements to be consolidated onto a single *smart card*, as is proposed.

The construction of a national information backbone infrastructure, such as the *Multimedia Super Corridor* (MSC) and the electronic government initiative [1], supplicates the study on secured and prioritized exchange of ID data over Internet implementation and protocols, e.g. TCP/IP. Data protection considerations include prioritized demand and security during the exchange of data, e.g. between the ID smart card and the card reader device, or a remote system. ID data is critical when delivered over the Internet and other networks because:

- from intercepting the network traffic, it may be possible to construct a person's identity and profile, thus malice could result in wrongful accusation (*what if the offense carries the capital sentence?*)

- as compared to financial data (which is usually limited to a certain amount transactable, an amount which financiers are prepared to risk), fraudulent use of ID data has *limitless* consequences

- the protection of individual *rights* as provided for in the Constitution must be observed, which include defining procedures and *cyber* legislation on the use of ID data, auditing, logging and tracing of ID demands and responses originating from the ID smart card.

- public confidence and acceptance of the ID system are prerequisites for successful implementation, while distrust could result in its abandonment.

1.1 Problem Statement

Among the major foreseeable obstacles to the CGID proposal is amalgamating the ID issuing process of the relevant authorities. The existing differences in information system implementation, the procedural and bureaucratic requirements, as well as legal implications need to be thoroughly examined, publicly assessed and even revamped.

A central CGID issuing authority may be needed. Communications and systems infrastructure required to support its operations, cost recovery, new legislation and public opinion ought to be carefully studied.

The process of authenticating the CGID card and guaranteeing its validity and performance, ensuring a safe and impartial card will require study as to the authentication procedures, secured card production and distribution facilities.

Various mechanisms are available to authorize the release of data from a smart card. These include the simple password and PIN approach, using passphrase or storing

biometric profiles of the hand signature. Access to the contents on the smart card is made when the smart card validates the user as its rightful owner.

Duplication and recovery of important data other than the authorized ID data (which is already with the government!), are required in the event the card is worn, damaged or lost, or even just changing to a new and better card. It may be permissible to trade in blank ID smart cards with consumers having the choice to select card features over standard recommendations and card cover design, and occasionally change their CGID card with little or no bureaucratic fuss.

Procedures and means for logging, auditing and tracing of ID demands and responses that also safeguard and guarantee the individual rights to privacy and freedom of movement must be thoroughly investigated. The mechanism for tracing is important for verification of card access, and for the prevention, and proof of misuse.

Hence the primary consideration is on the authenticity, security, tracing the use and recovery of the ID smart card content.

1.2 The Smart Card

Basically 3 types of secured feature cards are available, namely the *magnetic stripe* card, *optical* card and the *chip* card which is universally known as the *smart card*. The main consideration for the choice of card lies in the storage capacity and security features - the smart card is managed by its onboard microprocessor (CPU). The CPU controls access to storage or memory, and it also provides limited processing capability.

The smart card with CPU, storage, memory, magnetic stripe and card space for embossing characters, and placement of photograph, watermark and other images, are based on the commonly available smart card ISO standards, e.g. the ISO 7811 and the ISO 7816 series. Complementary smart card accessories include the card reader device coupled to desktop computers, *card wallet* which is a palm size card reader with infrared data transmission, and software for card authentication, access and device drivers.

Table 1 exemplifies the prominent feature of various types of ID cards [2, 3, 4].

Table 1: Prominent feature of ID cards

Card type	**Prominent feature**
Plain Paper	visible printed ID
Plain Plastic	secured embossed ID
Magnetic Stripe	multipurpose for simple use
Optical	large storage capacity
Chip	multipurpose secured access
PCMCIA	multipurpose *but bulky*

2.0 PROPOSED CGID MODEL

The CGID system model proposed for the country may be developed on resolving the following major issues as previously introduced:

- amalgamation of ID issuing agencies' procedures
- ID data requirements and specifications
- ID data security and assurance
- constitutional enactment and safeguards pertaining to the use of electronic ID and ID data
- basic communication infrastructure framework that includes costing on the use of ID data facilities

Before the introduction of a common ID card and system model (as a comprehensive proposal) would need to, firstly identify and define all possible ID requirements and issuing procedures, secondly to address the security issues of ID data transmission over the intended carrier protocols, mediums, as well as the choice of access control mechanism to be implemented on the ID smart card. Hence, the process of integration and of the issuing procedures may be studied having defined the broad requirements of ID needs.

The ID categories are defined in terms of ID data to be carried on an ID smart card. Although it may not be possible to include all the proposed ID categories because of limited storage and processing capacity of cards currently available, its provision is in expectation of improvement in technology.

2.1 CGID Card Data Contents

Card users can be categorized as Table 2 that precede determining possible card uses and data content.

Table 2: General card user categories

1.	card holder/owner
2.	government agencies *as official ID data keeper*
3.	important data providers *medical, academic and financial institutions*
4.	transaction recipients *anyone who need to access the card's data store*

The content component areas of the proposed CGID smart card may include the ID data (electronic access) and visible text and images. ID data may include:

- CGID card authentication and *authorities' area*
- tamper proof photographic images of holder
- finger print profiles
- biometrics verification profiles
- restricted access data area
- common or public access data area
- restricted financial data area
- communication credits
- access log

The CGID smart card storage components will consist of the card authentication area, a restricted access area and the common access area which permits general queries such as on the holder's nickname or gender.

The authorities' area is restricted in access to the respective ID data issuers/users. The holder may or may not have access to this area, e.g. there may be no access permitted to the driving licensing board's permanent demerit points record.

ID data reserved for the authorities include:

- national registration ID particulars
- immigration data i.e. passport and visas
- driving license and competency records
- other licensing authorities e.g. medical license
- health - inoculation and notification
- education - enrollment particulars
- taxation particulars
- legal records e.g. courts, police
- welfare - entitlement, dependents and other records

Important data that may be included:

- medical history (may comprise only the necessary information, e.g. allergy) which include *validated insurance data* for medical claim purposes
- academic transcript
- financial account data to identify cardholder as a genuine customer of a financial institution
- marital status and spouse(s)/children particulars
- validated insurance data other than for medical

Table 3 summarizes the content segments and access restrictions of the ID smart card data areas.

Table 3: Access to storage and application examples

Access type	**General application**
Card access	system use for card authentication, e.g. cryptic-keys
Authorities access	e.g. thumb print, ID data *restricted to authorized-party viewing only*
Restricted access	important data, e.g. insurance premium updates *holder partition storage for access, restricted update*
Common access	general data store e.g. nickname

The privilege of the CGID card holder to access to view, or to add new or change data found on the ID smart card would have to be determined. ID data from the authorities' area may be viewed but cannot be changed in any way by the holder. Similarly the holder should be able to control data from being viewed, written or added to the other data store areas, even the authorities' area. The other access areas may be partitioned by the ID smart card holder.

2.1.1 Authorities Area

Here the authorities may write or amend the ID data, while the holder has the right to only view the ID data and filter view access to a third party, e.g. allow access to verify only the name or residential address.

2.1.2 Restricted Area

The holder may cause partition of the restricted area for *data content providers*. These data are such as academic records, medical history, insurance premium paid and even financial data. The access provision here is that only the data providers may write and amend the data source, the holder may only view the data with the privilege to filter and blind access for viewing by a third party.

2.1.3 Common area

This area is used as a temporary store by the card holder and for general access. Its function may be similar to the restricted area except that the card holder has full access rights, i.e. to amend the data stored here.

2.2 Data Ownership

In addition to access restrictions to the different data store components, data ownership may be classified as strictly for system use, belonging to the authorities, belonging to important data providers and data that are stored by the cardholder.

2.3 Application Example

To recap, consider a possible scenario. A man involved in an accident may have a traffic warrant added onto his CGID card (authorities' area). He may also exchange insurance data (restricted area) with the parties involved in the accident and record incoming data in the common area. Over time the court may remove the warrant and his insurance company may make changes to the insurance record. All the transactions are made only with mutual authorization from the respective card owners, the initial process being system or device authentication of the CGID smart card. During data exchange, the parties involved may learn their names or nicknames (from the common area).

3.0 SECURITY

The assurance of a durable and secured ID smart card that will neither leak ID data nor will be easily tampered with, would ensure its public acceptance and use. Security considerations include card authentication (*is the card genuine?*), authorization of ID data release and also ensuring the data is authorized and not tampered, auditing functions and recovery of ID data.

3.1 CGID Card Authentication

In addition to physical markings e.g. watermark or holographic image, and user access validation procedures, an external card authentication process is required to assure the card that is being used (or transacted with) is veritable. The following may complement the card authentication process (i.e. card verification at application level):

- card manufacturers staking their reputation on tamper proof ID smart cards [5]
- establish legislation governing proper use
- an independent public council to monitor standards and security of applications using the ID smart card, and to make recommendations governing its use

The first ensures that cards that are manufactured by the companies can only be used for the ID system and are safeguarded against requests from unauthenticated cards. The later serves a regulatory function.

3.2 Authorization Procedures

The authorization procedure may:

- include user authorization by means of password, PIN, hand written signature profile or the PIN signature profile [6], the verification process may be performed on encrypted data stored on the smart card or through a central host
- require corresponding ID smart card or *approved* device (in the case of transacting with a machine e.g. cash dispenser) to activate ID data exchange.

While it may require two card-parties or with an approved device to activate ID data exchange, a third party authorization to provide verification of both parties as an *optional request* may be implemented. Fig. 1 indicates two parties requesting independent verification of the other's identity from an independent source.

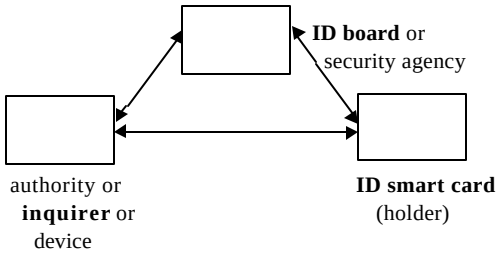

Fig. 1: A proposed verification model with provision for independent audit and trace.

Various mechanisms for security and protection for transmission of data over networks and the Internet are such as the widely used DES or RSA, and Internet security protocols. [7, 8, 9].

3.3 Logging, Auditing and Tracing

The CGID model ought to preserve close similarity to the present day use of ID. It has to maintain low system demand on resources, ensure and safeguard privacy and also provide system accountability for auditing, tracing and the recovery of ID data. Thus, the scope for development of logging ID data procedures.

Among the models that may be adopted is the provision for third party security services that permits the ID smart card holder to access and manage independent transaction logs (as similar to Fig. 1).

3.4 ID Data Duplication and Recovery

An ID document cannot be produced in duplicate, hence the CGID system model must be able to prevent duplication of the ID smart card and its content. But it must also provide the capability for the recovery of ID data and sanction duplication of ID data, as the provision for replacing ID smart cards.

4.0 APPLICATIONS

The CGID affords secured ID procedures and artifact, and provides convenience to the holder to include essential information which may be validated by the data providers concerned, e.g. insurance certificate (data) or academic qualification validated by an examination board. The system may encourage market development and use of multipurpose ID smart cards, providing consumers the option to choose the preferred ID smart card, e.g. card features/options or card cover design.

5.0 DISCUSSION

This paper has indicated broadly the conceptual feasibility of introducing an all encompassing ID smart card system. The potential areas for exploration, and the application design have been briefly introduced. The ID smart card concept that is proposed is in line with the objectives of the MSC master plan which includes the promotion of on-line authentication of ID devices and ID verification.

Multipurpose CGID must be unreservedly accepted by the different ID issuing authorities and the public. Hence, the CGID system model would need to be certified of its security potential and ability to preserve the rights and privacy of individuals. In addition, the model must be reliant with tamper proof, tamper detection and ID data recovery features.

Adaptation and uses of IT and communication systems in bureaucratic government agencies that would support the implementation of the CGID, must be studied, along with the established legislation such as the legality of electronic data/documents. The ID system data interface component must be made compatible with international standards and similar ID systems using smart cards. At present the card designs are proprietary and standards have yet to be defined for common interface and data exchange between different proprietary systems.

Initial cost of implementing a nationwide multipurpose ID system may be prohibitive, though the running cost may be recouped through tax collection from the private sector from projected expenses in using plastic cards, from card purchases and on-line ID inquiries.

The present ID card (laminated plastic and bar coded) has limited space for ID particulars and lacks secured authentication features. The right to disclose only essential information is not possible, e.g. to disclose sufficiently to indicate name or citizenship status only. The use of a smart card would allow the holder greater control over ID information that may be exchanged.

REFERENCES

[1] K. Kramer, "Competing in Computers: Business and Government Strategies in East Asia", in *Persidangan Infotech Malaysia '95, Kuala Lumpur,* 1 November 1992.

[2] J. L. Zoreda, and J. M. Oton, *Smart Cards.* Artech House, 1994.

[3] Bull, "Bull CP8: It's a Smart Card world", *http://www.cp8.bull.net/*, 1996.

[4] J. Walker, "Unicard". *http://ftp.fourmilab.ch/documents/unicard.doc*, 1994.

[5] D. Chaum, "Achieving Electronic Privacy". *Scientific American*, 1992, pp. 96-101.

[6] E. R. Tee, and N. Selvanathan "PIN Signature". *http://fsas.upm.edu.my/~robert/pinsign.html*.

[7] W. Stallings, "*Network and Internetwork Security: Principles and Practice*". Prentice Hall, 1995.

[8] M. A. Miller, *"Troubleshooting TCP/IP"* 2nd Ed. M & T Books, 1996.

[9] R. Atkinson, "Security Architecture for the Internet Protocol". *RFC 1825*, Internet Architecture Board (IAB), 1995.

[10] E. R. Tee, et al. "The CGID in multimedia application". *Prosiding Kolokium Teknologi Maklumat Jab. Sains Komputer: UPM Serdang*, 20 May 1997, pp. D55-60.

BIOGRAPHY

Elok Robert Tee is a Ph.D. candidate at the Universiti Putra Malaysia (UPM). His current interests among others are biometrics verification systems, and the impact of information technology in the Asean context.

ACKNOWLEDGMENT

To UPM for the facilities and the funding provided for this project from the *short-term grant* no. 50437-97-03. Appreciation to Dr. A. K. Ramani, Dr. Abu Talib Othman and Dr. Yazid Mohd Saman for commenting on the first draft of this paper.

ADDENDUM

Since the acceptance of this article, the Malaysian government has announced that a comprehensive smart card identification system which incorporates financial and identification functions be implemented beginning with the issuance of smart cards for newborn infants. *Editor*