Multiple Applications With a Single Protocol Smart Card.

D T Shaw[1]

and

S P Maj[2]
Department of Computer Science, Edith Cowan University,
Mt Lawley, Perth, Western Australia

Abstract

Unambiguous identification is essential to any form of transaction in e-commerce. However, credit card transactions rely on the manual identification of parties to the transaction and are inherently insecure. The use of biometrics to improve security is problematic. Smart cards can be used as credit cards with the additional advantages of increased security. The trend is to have multiple heterogeneous applications (access and transit control, electronic purse etc) on Smart cards. However the total number of applications is limited due to both international standards for Smart cards and current fabrication techniques. It is possible to link the different applications on a Smart card however this can be without the explicit knowledge of the user. In order to address these concerns a single protocol smart card is proposed. This result is a Smart card that can support a wide range of applications without the current disadvantages. The protocol has been simulated and tested. The results to date strongly suggest the feasibility of the design. Further testing is needed but along with research into other related issues such as user acceptability, cost etc.

Keywords: Smart Card, Identification, Authentication, Electronic Commerce

1. INTRODUCTION

Currently, Smart Cards allow multiple, heterogeneous applications to reside on a single card. Applications include credit, debit, purse, access control and transit amongst others. Central to all these applications is the necessity of correctly and unambiguously identifying the user prior to commencing any transaction. Identification of the user allows the correct attribution of responsibility, costs and liabilities. Some applications have minor requirements for identification whilst others must provide all possible assurances that the individual is correctly identified.

As the Smart Card is a simple, convenient, low-cost device the trend is to increase the number of resident applications. However, there are substantial constraints to the maximum number of possible applications due both to the inherent size of the card and internationally defined standards. Standards define the both the physical dimensions of the card (ISO 7810, 1995) and the Integrated Circuit (IC) footprint (ISO 7816, 1995 and ISO 10536, 1992). The advantages of complying with International standards are inter-operability and globalisation of supply. Whilst it is accepted that developments in IC fabrication are reducing track width and active component size it is recognised that the limits may be being reached.

The problem therefore is to allow an increased number of resident applications on a Smart Card beyond the current and foreseeable limits. A proposed solution to this limitation is to provide a single application on the Smart Card that is able to interact with any application off the Smart Card.

Shaw and Maj propose *'a smart card with a single protocol that can provide all the functionality of multi-*

[1] dtshaw@echidna.stu.cowan.edu.au
[2] S.Maj@cowan.edu.au

application smart cards but without the associated overheads'. (Shaw and Maj 2001) This model is based upon the conventional credit card transaction protocol. The proposed single protocol Smart Card has been evaluated for a number of applications by means of simulations and the results are presented in this paper.

2. MANUAL CREDIT CARD TRANSACTIONS

Currently, the manual credit card process relies primarily on human diligence to ensure the validity of the transaction. The vendor, after identifying the card as suitable for a transaction, transcribes card details such as account numbers, expiry date and bearer details onto a pro-forma. The description of the goods or services must then be entered on the pro-forma. Authorisation takes the form of a signature that should be compared with a specimen signature on the reverse of the card. Additionally, the vendor may check a list of known stolen cards or make a validation phone call. The vendor and the customer each keep a written copy of the transaction details for audit purposes. Inherent in this type of transaction is the confidence engendered by the user's choice of time and location of the transaction with the vendor.

It is noted that failing to retain and safely store all written copies may provide an opportunity for fraud. The details listed on the written copy are enough to provide opportunity for an unauthorised person to generate a fraudulent transaction. (Jones 2000A) Purchases may also be made over the telephone; however, interception of these credit card details may provide further opportunity for fraud. It should be noted that once the credit card details have been illegally obtained they may be used in multiple fraudulent transactions.

This problem is further exacerbated when credit cards are used for the purchase of goods and services on the Internet.

3. ELECTRONIC CREDIT CARD TRANSACTIONS

Electronic commerce is described as '*The various means and techniques of transacting business online.*' (Jones 2000B) The global availability of 24-hour access to the Internet represents unprecedented potential for electronic commerce. The benefits of electronic transactions include speed, reduced effort and economies of scale in many activities.

However, many potential users perceive the Internet as insecure and are therefore reluctant to use their credit cards to purchase goods and services on the Internet. Norris, West and Gaughan identify 'several challenges' to the increased acceptance of electronic transactions:

1. *Cardholders perceive the Internet as inherently insecure, and will not send card details 'in the clear' over the public network.*

2. *The cardholder and merchant both need to trust that the other is who they purport to be.*

3. *Even with confidence that the merchant is 'genuine', cardholders are reluctant to give their card details to a merchant with whom they have had no face-to-face contact.*

4. *Acquiring banks are reluctant to accept responsibility for 'Cardholder Not Present' (CNP) transactions. Under UK law, the risk for these transactions is taken by the merchant.*

5. *Merchants must be able to cope with refunds to customers.*

(Norris, West and Gaughan 2000)

Central to these concerns is the need for trust based on unambiguous and confidential identification of all parties to the transactions. This lack of this results in the reluctance of banks to accept responsibility for some transactions.

Currently, credit cards are neither unambiguous nor confidential. The identification provided may be as little as card details and expiry date or a signature linked to a name and address. This level of security may be improved by photographic identification on the card, however this is problematic, owing to the ease of changing personal appearance (hair colour, facial hair, contact lenses). Credit cards are often used in public places or over the telephone and the personal and account details may not be secured from unauthorised access. Despite these obvious problems, credit cards offer a convenient and global method of conducting business.

Globally, the cost of credit card fraud is significant and this is generally passed on to the user in the form of higher interest charges. The authors therefore analysed the basic principles of credit card transactions and the associated need for identification of all participants in a transaction.

IDENTIFICATION AND ACCESS CONTROL

Currently, identification of individuals is by mutually accepted artefacts. For example, a recognised uniform and/or Identification Documents (IDs) such as a Vehicle Driver's licence. Inspection of an ID involves determining its information content and context. Primary information fields are the Identification of the bearer and the permitted activities. For example, a driver's licence, where identification may be by text description and/or photograph and may list age, location,

speed or configuration restrictions. These can only be examined manually.

It is proposed that all forms of identification can be classified using the specific/non-specific and unilateral/bilateral as categories. In this context, specific identification means to identify one person or corporate entity by name. A non-specific identification cannot identify the individual by name. Unilateral identification will identify an individual to an individual but is not validated beyond that. Bilateral identification will identify an individual to another individual who must also be identified.

Non-specific, unilateral identification may not formally link the ID with the identity of the individual, for example, a theatre ticket allows access to a service without need to identify the user. Non-specific bilateral identification identifies bearers as members of a known group, for example a uniform or a token such as a badge. Specific unilateral identification links the identity of the individual with the ID, for example, a business card. Specific bilateral identification links the identity on the ID with the bearer and with another person or with a master listing. A Driver's licence may then be used to identify the individual. Further, the identity of the bearer may be confirmed by possession of secret knowledge such as a Personal Identification Number (PIN). This detects possession of fraudulent IDs or unauthorised use of legitimate IDs.

A Credit card may be classified as a non-specific, bilateral identification as neither party is explicitly identified due to lack of further verification.

	Unilateral	Bilateral
Non-Specific	Theatre ticket	Membership
Specific	Business Card	Driver's Licence

Table 1 Identification examples.

By contrast, Smart Cards may be used for all these categories of identification. As a specific bilateral device it can be used to uniquely and unambiguously identify the user. Longley and Shain state:

Smart Cards may have two forms; one for a set of banking operations and the other, termed an intelligent token, can provide access control, perform encryption and authentication operations, etc (Longley and Shain 1987)

4. SMART CARDS

Each Smart Card IC has volatile and non-volatile memory with a Central Processing Unit (CPU) and security mechanisms. Earlier designs, based on 8 bit processors such as the Intel 8051 architecture had storage limitations. For example, the Philips P83C855 Smart Card *'has 20 kilobytes of ROM, 2 kilobytes of EEPROM and 512 bytes of RAM.* (Rankl & Effing 1997) Recent developments in Smart cards now provide 32 bit processors such as the Motorola Jupiter Card with 48 Kbytes ROM, 3 Kbytes RAM and up to 16 Kbytes EEPROM with single or triple Data Encryption Standard (DES) (FIPS 1997) and Rivest Shamir and Adelman (RSA) encryption capabilities. (Motorola, 2001)

Multiple applications may reside on the Smart Card and be accessed on demand by the user. Access is typically by means of a PIN. Additionally, the embedded DES or RSA cryptographic capabilities may provide communications and information security not only for the transaction but also the data stored on the Smart Card. Consequently, a Smart Card may provide very secure facilities to the legitimate user. Unauthorised access to the Smart Card typically involves determining the PIN. In order to increase security, the trend is towards biometric identification eg thumbprint or retina scan but these remain problematic at present. Difficulties exist in consistently obtaining clear images. For example, any cuts and temporary blemishes on the thumb may result in rejection of the valid user.

However, in extreme cases, physical access to the card is possible. Determining information from the card by these means is not simple. Kommerling and Kuhn identify the process and provide some guidelines for securing the contents of the IC against physical attacks. (Kommerling and Kuhn, 1999)

5. CREDIT CARD APPLICATIONS ON A SMART CARD

A Smart Card can function as a credit card with the inherent advantages in access security and difficulty of forging. Adoption of this technology may be constrained by the pre-existing investment in magnetic stripe technologies on a global basis. It should further be noted that the disparity in costs between the magnetic stripe credit card and the Smart Card are substantial. However, potential reduction in the costs of fraud may ameliorate this disparity.

As a device that can act in specific/non-specific unilateral/bilateral modes the Smart Card can also support multiple heterogeneous applications residing on the same Smart Card. However, the total number of applications remain limited by the amount of memory on the Smart Card. Kingdon cited by Davis states, '*The price depends upon the amount of memory taken up by the application. Cards with 8 to 16 kilobytes of memory can hold between 3 and 10 applications, and larger chunks of code limit the number of potential partners.'* (Card Technology, 1999A)

User choices of useful applications on a given Smart Card may be restricted by the card provider. Card

providers may offer cooperative applications on a card. A cooperative application is where business is directed to a preferred source by making access to it easy or even mandatory without out the explicit consent of the card user.

Oulds cited by Davis, states '*London transport has been guaranteed an undisclosed sum in excess of 10 million pounds ($US16.1 million) per year from third parties putting applications on the 3 million to 5 million smart cards expected to be issued in its Prestige project, which is set for launch in August 2002,* (Card Technology, 1999B).

In conclusion, the current implementations have two major disadvantages. Firstly, a limited number of applications that may appear of the card and secondly the opportunities for cooperative applications to limit the user's choices.

6. A SINGLE PROTOCOL SMART CARD OPERATION

To address these concerns, Shaw and Maj propose a single protocol Smart Card (Figure 1) that may be used in all electronic transactions in the categories previously identified (specific/non-specific and unilateral/bilateral). Analysis of these different transactions yielded a set of requirements for a Smart Card. The functional requirements of the proposed Smart Card are:

1. *identify the bearer (external personalisation)*
2. *perform data input and output*
3. *identify the card (electronic serial number)*
4. *control access to card services*
5. *compute a secure hash value*
6. *compute a signature value*
7. *perform an encryption algorithm*
8. *store a transaction record*
9. *limit the number of new operations.*

(Shaw and Maj, 2001)

Additionally, a protocol is proposed based on a signature process (Figure 2). The signature process uniquely, unambiguously and securely links transaction details and the individuals by the associated Smart Card signatures. In every signature process a set sequence of events occurs as follows:

An input sequence (Contract, bill of sale, hash value of contract, text or numeric sequence etc) is used to produce the Output Sequence.

The output sequence is used as an electronic verification of each input sequence.
An input sequence may be a random or non-random interrogation sequence and is used to produce an output sequence for the purposes of identifying the Smart Card and by association its user. Additionally, the input sequence may be the bill of sale or transaction record to produce a hash value that can be used to verify the details of the transaction. The unique signature value can then be produced using the hash value as an input sequence. Consequently, the Smart Card signature generator can be used to provide unique, unambiguous verification of transactions.

6. A SINGLE PROTOCOL SMART CARD-USE

Non-specific, unilateral identification such as a theatre ticket requires just the output sequence of the signature generator to be recorded. The input sequence is the transaction record such as the performance title, date and time and the signature sequence can then be stored on the Smart Card and also by the proprietors of the Venue. Interrogation of the Smart Card with the same input sequence will produce the identical output sequence. Confirmation may be had by either checking the venue records or by checking the transaction records on the Smart Card.

Non-specific bilateral identification such as a membership token may be achieved by creating a number of identical Smart Card signature generators. Each signature generator will produce an identical output sequence for an identical input sequence. Identification results when the respondent produces the correct output sequence for any input sequence provided by the interrogator. For increased protection against false identification multiple random sequences may be taken.

Specific unilateral identification occurs when the card identification (Electronic serial number etc) is recorded. To verify that the card details have not been copied an interrogation sequence can be used to generate a signature from the card to verify that the specific card has been used. While these details may be stored on the Smart Card the interrogator can also verify the card by repeating the sequence or by generating a new sequence.

Specific bilateral identification occurs when all parties to a transaction provide the card identification details and the signature that corresponds to a particular interrogation sequence.

In addition to the above the proposed single protocol Smart Card can provide secure data transmission. The document to be transmitted is hashed. The document hash value is used to generate a signature value for use as an encryption key, for example DES requires 64 bits, for the document transmission. The hash value may be transmitted as a header to the encrypted document to permit the receiver to generate a key to decrypt the document. Additionally, the hash value may be retained and transmitted separately ensuring that document may only be decrypted according to the sender's instructions.

For a credit card application with an electronic signature the process may be as follows. After identifying the credit card as suitable, the vendor produces an electronic bill of sale (BOS) that describes the goods or services. The electronic version of the BOS stimulates the Smart Card to produce a BOS hash sequence to compare against the BOS hash value produced by the vendor. If the two hash values are equal then the user can initiate the signature generator. The hash sequence is used to produce an electronic signature that is related to the BOS and is unique to the smart card. This hash of the BOS and the electronic signature can then be forwarded with other information (such as payer and payee account details) to the financial institution where the hash value can be used to regenerate a signature for comparison and payment.

7. SIMULATIONS

Non-specific unilateral identification results when the Smart Card signature generator is repeatedly interrogated by a single input sequence. Regardless of the whether the input sequence is random or coherent (human readable) the simulation produces identical sequences for each repeat of an input sequence. Interspersing the identification input sequence with other sequences does not alter the correct response from the signature generator when the identification input sequence is repeated. Additionally, inspection of the simulation transaction records indicate whether the simulation has been used to respond to a particular input sequence.

Non-specific bilateral identification simulations occur when two separate instances of the signature generator are created. Multiple input sequences are created and the output sequences are recorded and compared. Both simulations return identical output sequences in the correct order to various input sequences. This indicates that the signature generators are identical.

Specific Unilateral identification was simulated with multiple non-identical signature generators. Each generator is interrogated with a particular input sequence. The results were then stored. The output sequence contained the card identification and the signature sequence that is used to verify that a particular card was used. To reverify the identification, the sequence may be repeated. A sequence of interrogations may be used. For example, if the numeric value of the interrogation sequence is '1000' then repeating the signature is possible. Incrementing the interrogation sequence by a specific value eg '1001' will generate a second signature that is related to the first signature.
Specific bilateral identification was simulated by creating two unique simulations and using them in a simulated transaction sequence. The simulations stored the signature of each different transaction. Each signature was different from each other.

Simulation of access control is either non-specific or specific bilateral identification. Simulation of secure document transfer involved creating two identical signature generators and using them as key generators. A test message was correctly decrypted.

An E-Commerce simulation used an electronic Bill of Sale containing the date and time of the transaction, the name of the card holder, the card serial number, the name of the vendor and card serial number followed by a short description of the item and the price.

For example, '01AUG98J0900 Fred Bloggs 0123456789ABCDEF Bill Bloggs ABCDEF0123456789 Commodore S sedan 3300 registration number 123456 blue with grey trim $50' describes the purchase of a car by Fred from Bill on the first of August 1998 at nine am for fifty dollars.

This sequence was hashed and the hash value of the BOS was processed by the Smart Card simulation to produce an output sequence that was retained by both parties as proof of the transaction. It may also be used by financial institutions to verify the account details and values.

All transactions have been categorised as non-specific /specific, unilateral/bilateral identification processes that rely on positive unambiguous identification. The credit card is classified as a non-specific unilateral identification and is intrinsically insecure. Smart Cards are able to perform credit card functions in addition to other multiple heterogeneous applications. Limited space and cooperation between applications results in limited choices for the users. A single protocol Smart Card has been proposed to address these issues.

The simulation was tested in all 4 categories of use and the results to date indicate that that it is feasible. Further research is needed into the implementation issues (costs, user acceptance etc.) and further testing is needed in a wide range of topics relating to analysis of the security and the reliability of the proposal. The proposed protocol may be used for a wide range of electronic transactions in all identified categories.

8. CONCLUSIONS

Smart Cards have applications in many aspects of education administration, particularly in simplifying the extensive administrative burden for each student. Further, the growth of e-commerce and electronic transactions requires some understanding of the nature and capabilities of Smart Cards for both students and teachers alike.

9. REFERENCES

Card Technology 1999A Card Technology July/August. Faulkner & Gray Publications. p39

Card Technology 1999B Card Technology July/August. Faulkner & Gray Publications. p38

FIPS, 1977, "FIPS Pub 46:1977 Data Encryption Standard (DES)" Federal Information Processing Standard United States Government.

ISO 7810, 1995, "ISO 7810 : Identification Cards -. Physical Characteristics" International Standards Organisation.

ISO 7816-1, 1995, "ISO 7816-1 : Identification Cards - Integrated Circuit Card with Contacts Part 1. Physical Characteristics" International Standards Organisation.

ISO 10536 – 1, 1992, "ISO10536 –1 : Identification Cards – contactless integrated circuit(s) cards" International Standards Organisation

Jones G., 2000A "Using Credit Cards on the Internet" Internet Handbooks United Kingdom. p13

Jones G., 2000B "Using Credit Cards on the Internet" Internet Handbooks United Kingdom. p93

Kommerling, O. and MG Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, USA, May 10-11, 1999, USENIX Association, pp. 9-20, ISBN 1-880446-34-0.

Longley, D and M. Shain, 1987, "Data and Computer Security – dictionary of Standards, concepts and terms" Macmillan Publishers

Motorola, 2001, "Smart Card Product Portfolio" URL: http://www.motorola.com/smartcard/121Ascppplatforms .htm Mar4 2001

Norris, M, S.West and K. Gaughan, 2000, "eBusiness Essentials – Technology and Network Requirements for the Electronic Marketplace" John Wiley and Sons United Kingdom.

Rankl, W. and W. Effing, 1997 "Smart Card Handbook" John Wiley and Son United Kingdom ISBN 0-471-96720-3 p430.

Schneier, B., 1996, "Applied Cryptology" 2nd Edition. John Wiley and Sons ISBN 0-471-12845-7

Shaw, DT and SP Maj, 2001, "A Single Protocol Smart Card for Multiple Applications." Proceedings of Information Systems Innovations 2001 American University of Dubai UAE Mar 19-21 2001 p3

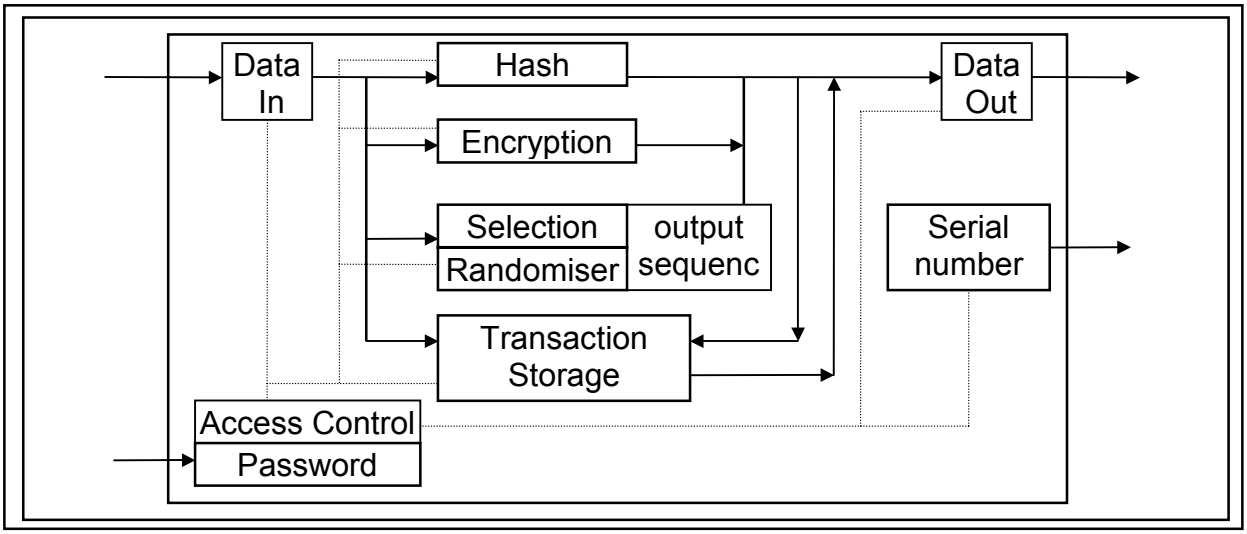

Figure 1 Proposed Smart Card Design

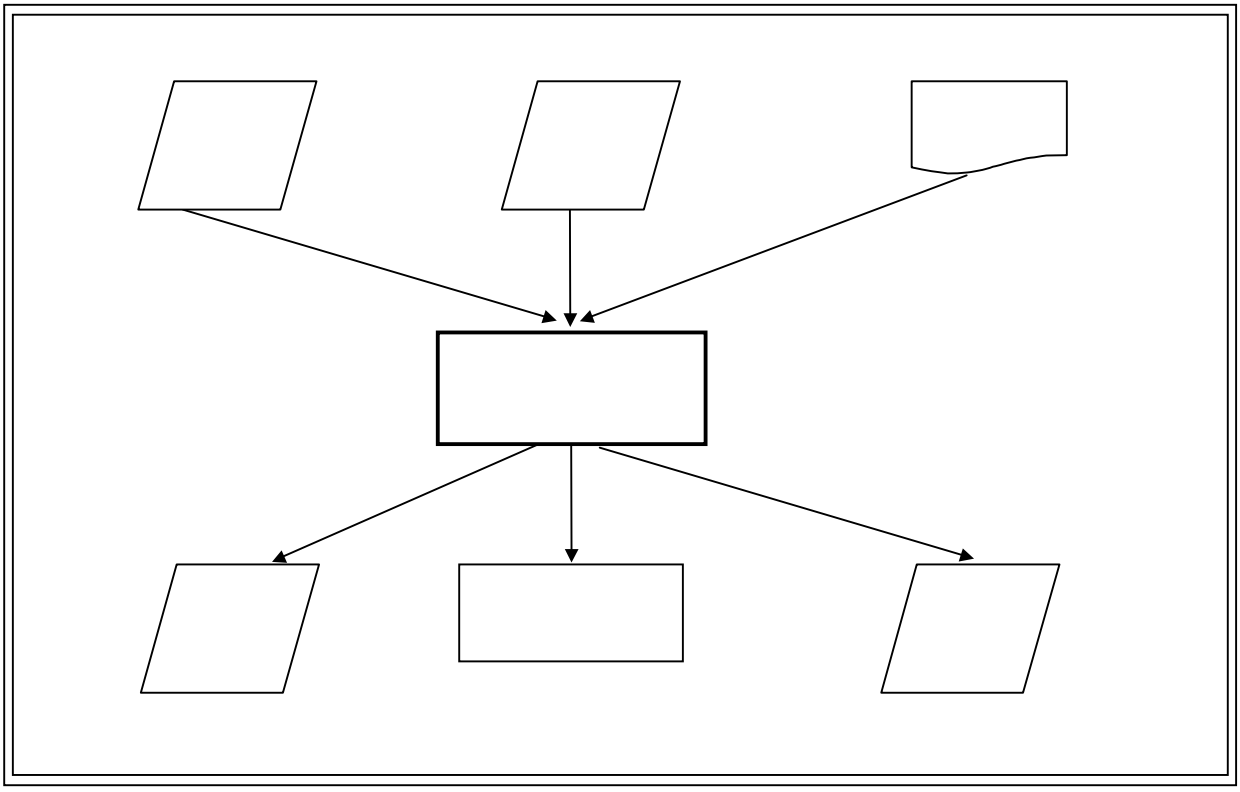

Figure 2 Signature Process