MULTIPLE APPLICATIONS WITH A SINGLE SMART CARD

David T. Shaw, Stanislaw P. Maj

Department of Computer Science, Edith Cowan University

Bradford Street, Mt. Lawley Perth

Western Australia

S.Maj@cowan.edu.au

Abstract: Smart Cards have limited resources to meet conflicting demands. Each application, such as identification, electronic purse etc. requires processing and separate storage. Credit card transactions rely on identification of parties to the transaction and are inherently insecure. Unambiguous identification is essential to any form of commercial transaction. Identification categories vary but include non-specific/specific and unilateral/bilateral. A single protocol Smart Card is proposed for use in all identification categories and may be used in credit transactions. Simulation results to date of the transactions indicate the feasibility of the proposal.

Keywords: Smart Card, credit card, identification, single protocol

1. INTRODUCTION

Currently, Smart Cards allow multiple, heterogeneous applications to reside on a single card such as credit, debit, purse, access control and transit. User identification is central to all these applications and allows the correct attribution of responsibility, costs and liabilities. Varying levels of identification are needed.

Though the Smart Card is a simple, convenient, low-cost device the trend is to increase the number of resident applications in spite of constraints defined by international standards. A proposed solution is to provide a single application on the Smart Card to interact with any application off the Smart Card.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35696-9_19](https://doi.org/10.1007/978-0-387-35696-9_19)

E. Nardelli et al. (eds.), *Certification and Security in E-Services*

© IFIP International Federation for Information Processing 2003

Shaw and Maj propose '*a smart card with a single protocol that can provide all the functionality of multi-application smart cards but without the associated overheads*'. (Shaw and Maj, 2001)

2. PROBLEMS WITH MANUAL CREDIT CARD TRANSACTIONS

Currently, the manual credit card process relies primarily on human diligence to ensure the validity of the transaction. Authorisation takes the form of a signature that should be compared with a specimen signature on the reverse of the card. Failing to safely store all written copies may permit fraud, as the written details are enough to generate a fraudulent transaction. (Jones, 2000, p 13) Electronic commerce is described as '*The various means and techniques of transacting business online.*' (Jones 2000 p93) The benefits of electronic transactions include: speed, reduced effort and economies of scale in many activities.

Many potential users perceive the Internet as insecure and there is the need for trust based on unambiguous and confidential identification of all parties to the 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, p 63)

It may be concluded that currently credit cards are neither unambiguous nor confidential. Despite 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.

3. IDENTIFICATION AND ACCESS CONTROL

Smart Cards may be used for identification and other applications. Additionally, optional embedded DES or RSA cryptographic capabilities may be provided. 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.

4. A PROPOSED SINGLE PROTOCOL SMART CARD - OPERATION

Shaw and Maj propose a single protocol Smart Card that may be used in all electronic transactions. 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 (internal personalisation such as 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, p3)

Additionally, a protocol is proposed based on a signature process that 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 and is used to produce an output sequence as a unique signature value. Consequently, the Smart Card signature generator can be used to provide unique, unambiguous verification of transactions.

5. A SINGLE PROTOCOL SMART CARD – USE

For a credit card application with an electronic signature the specific, bilateral 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.

This unified and semi-automated process may expedite credit card transactions as well as provide unambiguous identification of all participants. Software simulations show that the process is feasible.

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. This complete 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. In keeping with the wide acceptability of the credit card, a wide range of simple commercial transactions may be addressed with this proposal.

6. CONCLUSIONS

Smart Cards are able to perform credit card functions in addition to other multiple heterogeneous applications. However, a single protocol Smart Card with potentially wide application has been proposed to address these issues. The use of unambiguous identification is now integrated into the proposed credit card transaction. Further research is needed into the implementation issues (costs, user acceptance etc.) and further testing is needed. The proposed protocol may be used for a wide range of electronic transactions in all identified categories.

REFERENCES

- Jones G. (2000) Using Credit Cards on the internet Internet Handbooks United Kingdom
- Norris, M, West, S and Gaughan, K. (2000) eBusiness Essentials – Technology and Network Requirements for the Electronic Marketplace John Wiley and Sons United Kingdom.
- Shaw, DT and Maj SP (2001) A Single Protocol Smart Card for Multiple Applications. Proceedings of Information Systems Innovations 2001 American University of Dubai UAE Mar 19-21 2001