20

Implementation Aspects of SET/EMV

Pita Jarupunphol* and Chris J. Mitchell
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
P.Jarupunphol@rhul.ac.uk, C.Mitchell@rhul.ac.uk

Abstract: The threat of credit card fraud is arguably one of the most serious issues in e-commerce, since it makes consumers reluctant to engage in this alternative method of shopping. Secure Electronic Transaction (SET) was invented to address this issue, and it provides effective security for the entire Internet e-commerce transaction. However, SET has not really taken off; implementation issues appear to be the main factor restricting its adoption. Given the existing consumer concerns about e-commerce security, SET still appears to be very relevant to the Internet e-commerce transaction environment. The integration of SET with EMV is a possible route for facilitating the wider use of SET in Internet commerce transactions, since it could simplify user registration. The aim of this paper is to evaluate the effectiveness of SET/EMV integration for fraud reduction in e-commerce. In addition, this paper also considers the implementation feasibility of SET/EMV.

Keywords: Electronic Commerce (E-Commerce), Secure Socket Layer (SSL), Secure Electronic Transaction (SET), Transport Layer Security (TLS), EMV, Public Key Infrastructure (PKI), digital certificate, digital signature.

1. INTRODUCTION

The emergence of e-commerce provides consumers with an alternative method of payment via the Internet. E-commerce both offers new opportunities for sales and also potentially reduces the time spent in traditional shopping methods (Whiteley, 2000). For example, there is no need for consumers to visit retail premises in order to purchase goods. However, this non face-to-face shopping method also permits fraudsters to take advantage of the lack of card and cardholder authentication to perform illegal operations, such as use of credit card numbers without the consent of the valid cardholder. This issue makes con-

*Pita Jarupunphol was sponsored by the Rajabhat Institute of Phuket

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: 10.1007/978-0-387-35617-4_48
J. L. Monteiro et al. (eds.), *Towards the Knowledge Society*

sumers reluctant to purchase goods online by credit card and hence restricts the size of the e-commerce market.

According to Treese and Stewart (Treese, 1998), the credit card is the most common method of payment in business-to-consumer (B2C) transactions. In addition, a survey of Internet users conducted by Survey.Net[1] indicates that more than 50% of Internet users purchase products or services by credit card. Therefore, it is inevitable that the secrecy of credit card numbers is a serious issue of concern to Internet purchasers. Many potential consumers are afraid to submit their credit card numbers via the Internet and also perceive Internet shopping as the riskiest method (Jarupunphol et al., 2001).

Several tools and techniques have been used to address consumer fears, such as the IETF's SSL-based Transport Layer Security (TLS) (Rescorla, 2001) and SET (Merkow, 1998). SET is arguably the most secure method of online payment by credit card, since it provides consumer, merchant and card issuer with protection for the entire transaction. However, SET has not been widely adopted, at least partly because of implementation issues. As a consequence, extensions have been proposed to SET to address some of these implementation problems. One such set of extensions to SET are the 'chipcard extensions' (SETCo.Org., 1999), which enable EMV-compliant debit/credit cards to interoperate with the SET protocol, thereby simplifying the end-user initialisation process. We refer to this combination of SET with EMV as SET/EMV. The intention of this paper is to evaluate the effectiveness of SET/EMV in B2C e-commerce.

2. OVERVIEW OF SET/EMV

2.1. SET — background and technical overview

SET was invented by Visa[2] and MasterCard[3], and was designed to address security threats arising to both transmitted and stored data (Stein, 1998). SET employs both symmetric and asymmetric cryptography to protect purchasing information sent among SET participants. Key management for SET is based on the use of a Public Key Infrastructure (PKI) (Adams et al., 1999) to reliably distribute public keys between SET participants (SETCo.Org., 1997).

SET requires the e-consumer to have been through an initialisation process, which involves:

- the generation of an asymmetric key pair for the e-consumer;
- the (reliable) transfer of the e-consumer public key to the e-consumer's bank (an issuer), which generates a public key certificate for the e-consumer using its own private signature key;
- the (reliable) transfer of the system 'root' public key to the e-consumer, along with the e-consumer's public key certificate;

- the e-consumer's private key is stored in a 'digital wallet' on the e-consumer's PC, which will typically be password protected.

Recently, several SET extensions have been introduced in order to facilitate greater adoption and use of SET, including the PIN and chip extensions.

2.2. EMV — background and technical overview

The EMV Specifications (named after the three responsible organisations: Europay, MasterCard and Visa International), (EMV.Co.Org., 2000(a)), (Hassler, 2000), (Sherif, 2000), define how compliant IC cards and payment terminals should interact. These specifications were agreed to enable IC cards to be used to replace existing credit and debit magnetic strip cards, without requiring a separate merchant terminal for each card brand. Like SET, EMV employs a PKI mechanism to support the provision of confidentiality and integrity for transactions. EMV has two distinct card authentication methods (EMVCo.Org., 2000(b)): static and dynamic authentication; in this paper we restrict our attention to EMV cards that support dynamic authentication since not only is it more secure but it also offers better integration with SET. The PKI underlying the EMV dynamic authentication scheme operates as follows. An outline of the underlying PKI is also given in Figure 1.

- The root certification authority certifies a card issuing bank's public key and passes this public key certificate back to the issuing bank. In this case, the root CA is operated by the card brand (e.g. Europay/MasterCard).

- When creating an EMV card (supporting dynamic authentication), the card issuer generates a signature key pair for the card. The card issuer then signs a public key certificate for the card, using the card issuer's private signature key. The following three items are loaded into the card: the card's own private key, the certificate for the card public key, signed by the card issuer, and the certificate for the card issuer's public key, signed by the root (brand) CA.

- The public key of the root (brand) CA is distributed to the acquiring bank, who ensures that it is present in every merchant terminal.

- The presence of the brand CA public key in the merchant terminal enables the terminal to verify the two certificates in an EMV card, and hence verify the card's public key. This supports digital signature-based card authentication to the terminal during an EMV transaction.

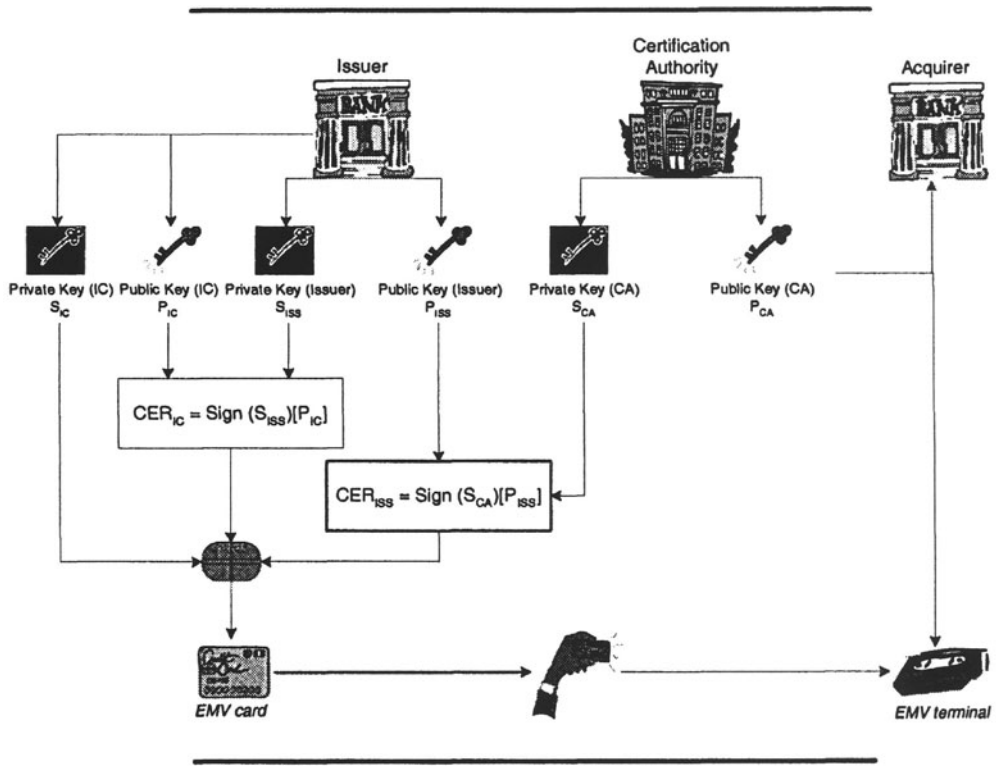

Figure 1. The PKI supporting EMV dynamic authentication (EMVCo.Org., 2000(b)).

2.3. The integration of SET with EMV

The integration of SET with EMV is feasible, since the two systems share a number of features.

Credit card fraud reduction Both SET and EMV were devised to try and reduce credit card fraud, albeit for rather different types of transaction, namely remote (e-commerce) transactions and 'in person' transactions at merchant premises, respectively.

Use of PKI As discussed above, SET and EMV are both based on the use of a hierarchical PKI in which brands sign public key certificates for banks, and banks sign public key certificates for end users.

PIN entry and verification SET requires a cardholder to enter a PIN as part of the cardholder verification process before initiating an e-commerce transaction. Similarly, EMV requires a cardholder to verify themselves via a PIN entry process at an EMV-compliant merchant terminal.

3. SET/EMV PROCESS IN E-COMMERCE TRANSACTIONS

We next sketch the main steps in a SET/EMV transaction (EMVCo.Org., 1999). The transaction process is outlined in Figure 2, and in the text below we refer to the numbered steps marked in the figure.

Step 1 The consumer and merchant exchange a SET initiation message. At this stage, the merchant invokes the cardholder system and informs the consumer of the payment brands accepted.

Steps 2 and 3 A cardholder selects the payment card to be used to initiate a SET/EMV transaction. Then, the cardholder system selects an application from the card. In some cases, additional input from the cardholder may be required.

Steps 4 and 5 The cardholder system initiates the card application and reads the application data from the card. This process will involve communication between the EMV card and the reader to verify the consumer credit card information stored in the EMV card.

Steps 6 and 7 The consumer requests a purchase initialisation. The merchant then responds to the consumer request. The cardholder system will inform the merchant server of the payment method, and the merchant server responds with the information relevant to purchase completion.

Step 8 The Cardholder System retrieves authentication information from the cardholder, e.g. a PIN, and either presents it to the card or transmits it to the card issuer for verification.

Step 9 At this point the Cardholder System may request the card to initiate an online authorisation of the transaction. The card has the option of either declining the transaction offline, or requesting an online authorisation.

Step 10 The Cardholder System now requests a purchase, and provides the Merchant Server with the data that it, the Payment Gateway, and the card issuer require to be able to respond to the request.

Steps 11 and 12 The merchant passes an authorisation request to the acquirer via the payment gateway. The acquirer forwards an authorisation request to the consumer bank (issuer) through the banking payment network.

Steps 13 and 14 The issuer returns a payment authorisation to the merchant via the acquirer.

Step 15 The Merchant passes a purchase response to the consumer for a confirmation of purchase.

Step 16 The Cardholder System communicates with the card to terminate the transaction process.

Steps 17 and 18 The merchant requests the acquirer to capture the transaction. The acquirer responds to the merchant request.

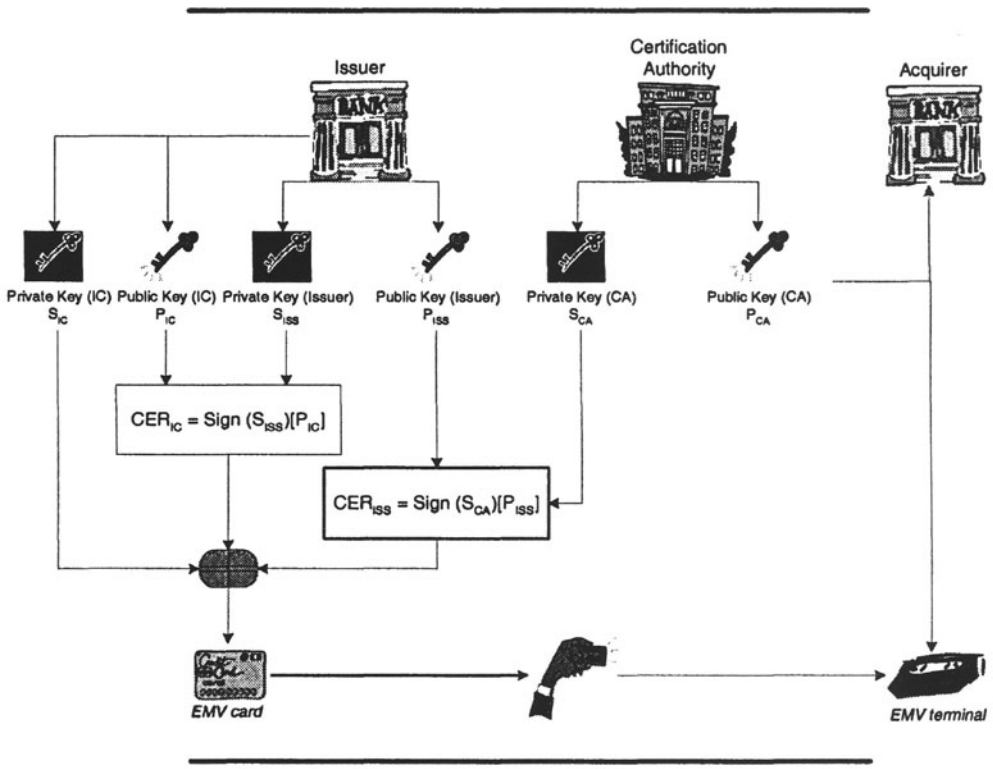

Figure 2. The PKI supporting EMV dynamic authentication (EMVCo.Org., 2000(b)).

4. SET/EMV IMPLEMENTATION ISSUES

We next evaluate the effectiveness of SET/EMV integration for fraud reduction in e-commerce and also consider what makes SET/EMV different from traditional SET.

There is no significant difference between SET/EMV and the traditional SET scheme as far as credit card fraud reduction is concerned, since most SET/EMV processes are the same as the traditional SET scheme. However, there is a significant difference in practice, since traditional SET requires a cardholder to register for a public key certificate prior to engaging in any transactions. A cardholder then needs to perform PIN entry to activate a private key stored at his/her computer in order to initiate SET. Some problems with traditional SET implementations are as follows (Jarupunphol et al., 2002).

- The cardholder may not be able to participate in SET, since the process of public key registration is one of major factors restricting the adoption of SET (Lieb, 1999).
- The cardholder's private key is at risk of compromise if third parties can access the cardholder PC.
- The cardholder must use his/her own computer in order to initiate SET.

SET/EMV avoids these issues by making use of the key pair present in an EMV card, thus avoiding the need for initial registration and reducing the risk of key compromise.

4.1. Benefit analysis

SET/EMV is likely to be beneficial to both consumers and merchants in e-commerce transactions since it prevents most conceivable types of credit card fraud. In particular, the consumer can be confident that:

- There is no means for an interceptor to steal or disclose consumer financial information when SET/EMV is employed.
- The merchant is legitimate and unable to access or modify the payment information, since the merchant is certified by an acquirer and the payment information is signed using the consumer private key and encrypted using the acquirer public key.
- Sensitive cardholder information, including the cardholder private key, is stored in the consumer's EMV card and is thus protected by the smartcard physical security features.

Although credit card companies will typically reimburse consumers in the event of a disputed transaction, this insurance does not cover the merchant for e-commerce transactions. The merchant is generally responsible for card-not-present costs associated with fraudulent transactions (Treese, 1998), (Caunter, 2001). The benefits that e-merchants receive from the use of SET/EMV include the following.

- The merchant can be confident that the cardholder is genuine, since the cardholder must input their PIN to the card via their PC and card reader.
- Merchants pay nothing for disputed card-not-present transactions, since SET scheme transactions are regarded in the same way as face-to-face traditional transactions.
- Merchants know that nobody can access consumer order information, including the acquirer, thus retaining merchant privacy.

4.2. Potential barriers

As already mentioned, SET/EMV can remove the complexity of end-user initialisation, a significant barrier to the use of traditional SET (Jarupunphol et al., 2002). However, one factor remains that can restrict the implementation of SET/EMV, namely the cost of implementation.

According to Donnelly (Donnelly, 2000, p.9), 'E-tailers don't want to spend the money because they are already spending more money on credit card transactions than traditional retailers'. Similarly, e-consumers are likely to be reluctant to buy extra PC peripherals, e.g. a card reader, just to perform e-commerce transactions.

Other potential issues with traditional SET are its low transaction speed, and novel e-payment infrastructure. We now analyse the potential effect of all these criticisms on SET/EMV in more detail.

4.2.1 Transaction speed. The speed of transactions is an important factor, since this can make e-commerce end-users reluctant to use SET/EMV. According to Whinnett (Whinnett, 1997, p. 449), 'Insufficient speed also discourages on-line shopping and creates the danger that users will interrupt transactions if they are not implemented quickly enough'.

In traditional SET implementations, in order to achieve the necessary transaction throughput at the merchant server, SET may need support from special hardware devices, such as cryptographic accelerators. An alternative to deploying special hardware is to select public key cryptosystems which minimise computational workload, e.g. elliptic curve cryptosystems (Gartner, 1998).

SET/EMV suffers from very similar cryptographic computation overheads at the merchant, and exactly the same implementation issues arise for the merchant.

4.2.2 Cost of investment. SET/EMV obviously requires additional investment for both merchant and consumer.

Merchant The merchant may need to set up a cryptographic accelerator at his/her server in order to provide support for peak load transactions, since the cryptographic mechanisms used in SET/EMV are complex.

Consumer The implementation of SET/EMV requires not only merchants but also consumers to purchase additional hardware devices. The cardholder needs to have a smartcard reader installed at their PC.

4.2.3 E-payment infrastructure. The existing e-payment infrastructure is one of the main barriers to traditional SET implementation. Treese and Stewart (1998) argue that SET is not compatible with the existing e-payment

infrastructure, since SET prevents merchants from seeing consumer credit card numbers.

This issue also seems to be a factor that may restrict the implementation of SET/EMV, as most current e-payment systems require the merchant to access consumer credit card numbers.

5. SET/EMV IMPLEMENTATION FEASIBILITY

5.1. The FINREAD project

Conducting e-commerce with a combination of SET and EMV is currently a little complicated for consumers since it requires an additional device (an IC card reader) to be connected to the user PC. However, a number of smart card manufacturers are attempting to facilitate the use of smart cards by PC owners.

The emergence of the FINREAD (Financial transactional IC card reader) project (CWA, 2001) would appear to facilitate SET/EMV implementation, since it is designed to establish a secure smart card reader for use in consumer e-commerce, including home banking and Internet shopping. Aspects of FINREAD which are particularly relevant to SET/EMV implementation are as follows.

- The FINREAD specifications are designed to support all forms of secure financial transaction, including SET.
- The FINREAD ICC reader will be compatible with the EMV specifications.
- Consumers will be able to purchase smart card readers at low costs without limiting the security and usability of the products.

Hence it is feasible that through FINREAD or by other means the IC card reader will become a widely adopted PC peripheral.

5.2. Public/private sector support

In a climate where none of the parties are prepared to commit to the investment necessary to make SET or SET/EMV a reality, an extra impetus is required to realise the potentially large benefits from its use. Given potential e-commerce participants are very concerned about the threat of credit card fraud, cooperation between the public and private sectors would seem to be a possible enabler for the future adoption of this alternative scheme. One way in which the adoption of SET/EMV could be facilitated would be if governments or trade bodies positively encouraged merchants and card issuers to adopt SET/EMV, e.g. by requiring its use for their e-business.

Furthermore, since SET and EMV rely on the use of PKI, governments or trade bodies could also help by enhancing public trust in PKI technologies.

As argued by Tobias (Tobias, 2000, p.10), 'Governments must play a key part in ensuring that users can trust the technologies that produce secure digital certificates and the commercial organizations providing it'.

However, for such moves to become reality would require a positive decision in favour of SET by official bodies, which seems to be some way from reality in the current climate.

6. CONCLUSIONS

The integration of SET with EMV arguably provides both consumers and merchants with the highest possible security for the entire online transaction process. However, serious issues remain that may adversely affect SET/EMV implementation as they have affected traditional SET. SET/EMV implementation requires e-commerce end-users to make an investment in the technology, which they may not be prepared to make. Support from governments and cooperation between the public and private sectors is potentially a critical factor in the possible success of SET/EMV. In addition, the emergence of the FINREAD project potentially helps the implementation of this integrated technology, since it was designed to support both SET and EMV in e-commerce transactions.

7. REFERENCES

CWA 14174-1 Financial transactional IC card reader (FINREAD) — Part 1: Business requirements, May 2001.

C. Adams and S. Lloyd. *Understanding Public-Key Infrastructure*. New Riders, 1999.

N. Caunter. The real cost of fraud to e-tailers. *Computer Fraud and Security*, 2001(8):17, August 2001.

A. Donnelly. Online credit card fraud outpaces physical world. *Computer Fraud and Security*, 2000(10):9, October 2000.

EMVCo.Org. *EMV '96 Chip Electronic Commerce Specification*, December 1999.

EMVCo.Org. *EMV 2000 Integrated Circuit Card Specification for Payment Systems — Book 1: Application Independent ICC to Terminal Interface Requirements*, December 2000.

EMVCo.Org. *EMV 2000 Integrated Circuit Card Specification for Payment Systems — Book 2: Security and Key Management*, December 2000.

Gartner Group. *SET Comparative Performance Analysis*, November 1998.

V. Hassler. *Security Fundamentals for E-Commerce*. Artech House, 2000.

P. Jarupunphol and C. Mitchell. Actual and perceived levels of risk in consumer e-commerce. In *Proceedings of 2nd International We-B Conference*, pages 207–216. Edith Cowan University Press, November 2001.

P. Jarupunphol and C. J. Mitchell. The Future of SET. In *Proceedings of UKAIS2002*. Leeds Metropolitan University, April 2002.

J. Lieb. Getting secure online — an overview. *CommerceNet — The Strategies Report*, 1(3):1–4, July 1999.

M. S. Merkow, J. Breithaupt, and K. L. Wheeler. *Building SET Applications for Secure Transactions*. John Wiley and Sons, 1998.

E. Rescorla. *SSL and TLS — Designing and Building Secure Systems*. Addison-Wesley, 2001.

SETCo.Org. *SET Secure Electronic Transaction Specification — Book 1: Business Description*, May 1997.

SetCo.Org. *Common Chip Extension — Application for SETCo Approval*, September 1999.

M. H. Sherif. *Protocols for Secure Electronic Commerce*. CRC Press, 2000.

L. D. Stein. *Web Security*. Addison-Wesley, 1998.

H. Tobias. To be or not to be — legally binding digital certificates. *Network Security*, 2000(6):9–11, June 2000.

G. W. Treese and L. C. Stewart. *Designing Systems for Internet Commerce*. Massachusetts: Addison-Wesley, 1998.

D. Whinnett. End user acceptance of security technology for electronic commerce. In *Proceedings of IS&N '97*, pages 447–457. Springer-Verlag, 1997.

D. Whiteley. *E-Commerce: Strategy, Technologies and Applications*. McGraw-Hill, 2000.