Secure Electronic Transaction (SET protocol)

**Yang Li &
Yun Wang**

1. Introduction

Electronic commerce, as exemplified by the popularity of the Internet, is going to have an enormous impact on the financial services industry. No financial institution will be left unaffected by the explosion of electronic commerce. Even though SSL is extremely effective and widely accepted as the online payment standard, it requires the customer and merchant to trust each other: an undesirable requirement even in face-to-face transactions, and across the Internet it admits unacceptable risks.

Visa and MasterCard and a consortium of 11 technology companies made a promise to banks, merchants, and consumers: they would make the Internet safe for credit card transactions and send electronic commerce revenues skyward. With great fanfare, they introduced the Secure Electronic Transaction protocol for processing online credit card purchases [1].

2. Overview of SET Protocol

Secure payment systems are critical to the success of E-commerce. There are four essential security requirements for safe electronic payments (Authentication, Encryption, Integrity and Non-repudiation). Encryption is the key security schemes adopted for electronic payment systems, which is used in protocols like SSL and SET.

2.1 Problem with SSL

The SSL protocol, widely deployed today on the Internet, has helped create a basic level of security sufficient for some hearty souls to begin conducting business over the Web. SSL is implemented in most major Web browsers used by consumers, as well as in merchant server software, which supports the seller's virtual storefront in cyberspace. Hundreds of millions of dollars are already changing hands when cybershoppers enter their credit card numbers on Web pages secured with SSL technology.

In this sense, SSL provides a secure channel to between the consumer and the merchant for exchanging payment information. This means any data sent through this channel is encrypted, so that no one other than these two parties will be able to read it. In other words, SSL can give us confidential communications, it also introduces huge risks:

- The cardholder is protected from eavesdroppers but not from the merchant. Some merchants are dishonest: pornographers have charged more than advertised price, expecting their customers to be too embarrassed to complain. Some others are just hackers who put up a snazzy illegal Web site and profess to be the XYZ Corp., or impersonate the XYZ Corp. and collecting credit card numbers for personal use.

- The merchant has not protected from dishonest customers who supply an invalid credit card number or who claim a refund from their bank without cause. Contrary to popular belief, it is not the cardholder but the merchant who has the most to lose from fraud. Legislation in most countries protects the consumer.

2.2 SET protocol Overview

What we want here is a protocol very similar to credit card transactions at a local store, something SSL doesn't mimic in functionality. SET is the one.

2.2.1 Purpose and Entities

Purpose
The purpose of the SET protocol is to establish payment transactions that

- provide confidentiality of information;
- ensure the integrity of payment instructions for goods and services order data;
- authenticate both the cardholder and the merchant .

Main Entities
There are four main entities in SET:

- Cardholder (customer)
- Merchant (web server)
- Merchant's Bank (payment gateway, acquirer): payment gateway is a device operated by an acquirer. Sometime, separate these two entities.
- Issuer (cardholder's bank)

2.2.2 How it Works

Both cardholders and merchants must register with CA (certificate authority) first, before they can buy or sell on the Internet, which we will talk about later. Once registration is done, cardholder and merchant can start to do transactions, which involve 9 basic steps in this protocol, which is simplified.

1. Customer browses website and decides on what to purchase
2. Customer sends order and payment information, which includes 2 parts in one message:
    a. Purchase Order – this part is for merchant
    b. Card Information – this pat is for merchant's bank only.
3. Merchant forwards card information (part b) to their bank
4. Merchant's bank checks with Issuer for payment authorization
5. Issuer send authorization to Merchant's bank
6. Merchant's bank send authorization to merchant

7. Merchant completes the order and sends confirmation to the customer
8. Merchant captures the transaction from their bank
9. Issuer prints credit card bill (invoice) to customer

2.2.3 Protocol Overview

SET (Secure Electronic Transaction) is a very comprehensive security protocol, which utilizes cryptography to provide confidentiality of information, ensure payment integrity, and enable identity authentication. For authentication purposes, cardholders, merchants, and acquirers will be issued digital certificates by their sponsoring organizations.

It relies on cryptography and digital certificate to ensure message confidentiality and security. Digital envelop is widely used in this protocol. Message data is encrypted using a randomly generated key that is further encrypted using the recipient's public key. This is referred to as the "digital envelope" of the message and is sent to the recipient with the encrypted message. The recipient decrypts the digital envelope using a private key and then uses the symmetric key to unlock the original message.

Digital certificates, which are also called electronic credentials or digital IDs, are digital documents attesting to the binding of a public key to an individual or entity. Both cardholders and merchants must register with a *certificate authority* (CA) before they can engage in transactions. The cardholder thereby obtains electronic credentials to prove that he is trustworthy. The merchant similarly registers and obtains credentials. These credentials do not contain sensitive details such as credit card numbers. Later, when the customer wants to make purchases, he and the merchant exchange their credentials. If both parties are satisfied then they can proceed with the transaction. Credentials must be renewed every few years, and presumably are not available to known fraudsters.

3. SET Cryptography

3.1. Overview

Secure Electronic Transactions (SET) relies on the science of cryptography – the encoding and decoding messages. There are two primary encryption methods in use today: secret-key cryptography and public-key cryptography. Secret-key cryptography is impractical for exchanging messages with a large group of previously unknown correspondents over a public network. For a merchant to conduct transactions securely with millions of subscribers, each consumer would need a distinct key assigned by that merchant and transmitted over a separate secure channel. However, by using public-key cryptography, that same merchant could create a public/private key pair and publish the public key, allowing any consumer to send a secure message to that merchant. This is why SET uses both methods in its encryption process. The secret-key cryptography used in SET is the well-known Data Encryption Standard (DES), which is used by financial institutions to encrypt PINs (personal identification numbers). And the public-key cryptography used in SET is RSA. In the following section, the usage of symmetric (secret-key) and asymmetric (public-key) key encryption in SET will be discussed.

3.2. Use of Symmetric Key

In SET, message data is encrypted using a randomly generated symmetric key (a DES 56-bit key). This key, in turn, is encrypted using the message recipient's public key (RSA). The result is the so called "digital envelope" of the message. This combines the encryption speed of DES with the key management advantages of RSA public-key encryption. After encryption, the envelope and the encrypted message itself are sent to the recipient. After receiving the encrypted data, the recipient decrypts the digital envelope first using his or her private key to obtain the randomly generated symmetric key and then uses the symmetric key to unlock the original message.

This level of encryption, using DES, can be easily cracked using modern hardware. In 1993, a brute-force DES cracking machine was designed by Michael Wiener – one which was massively parallel. For less than a million dollars, a 56-bit DES key could be cracked in average time of 3.5 hours. For a billion dollars, a parallel machine can be constructed that cracks 56-bit DES in a second (Schneier, 1996). Obviously, this is of great concern since DES encrypts the majority of a SET transaction.

3.3. Use of Asymmetric Key – Digital Signature (Message Digests)

In SET, the public key cryptography is only used to encrypt DES keys and for authentication (digital signature) but not for the main body of the transaction. In SET, the RSA modulus is 1024 bits in length (Using the latest factoring results it appears that factoring a 1024-bit modulus would require over 100,000,000,000 MY of computational effort). To generate the digital signature, SET uses a distinct public/private key. Each SET participant possesses two asymmetric key pairs: a "key exchange" pair, which is used in the process of section key encryption and decryption, and a "signature" pair for the creation and verification of digital signatures (160-bit message digests).

The algorithm is such that changing a single bit in the message will change, on average, half of the bits in the message digest. Approximately, the possibility of two messages having the same message digest is one in 1,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000, which means it is computationally unfeasible to generate two different messages that have the same message digest.

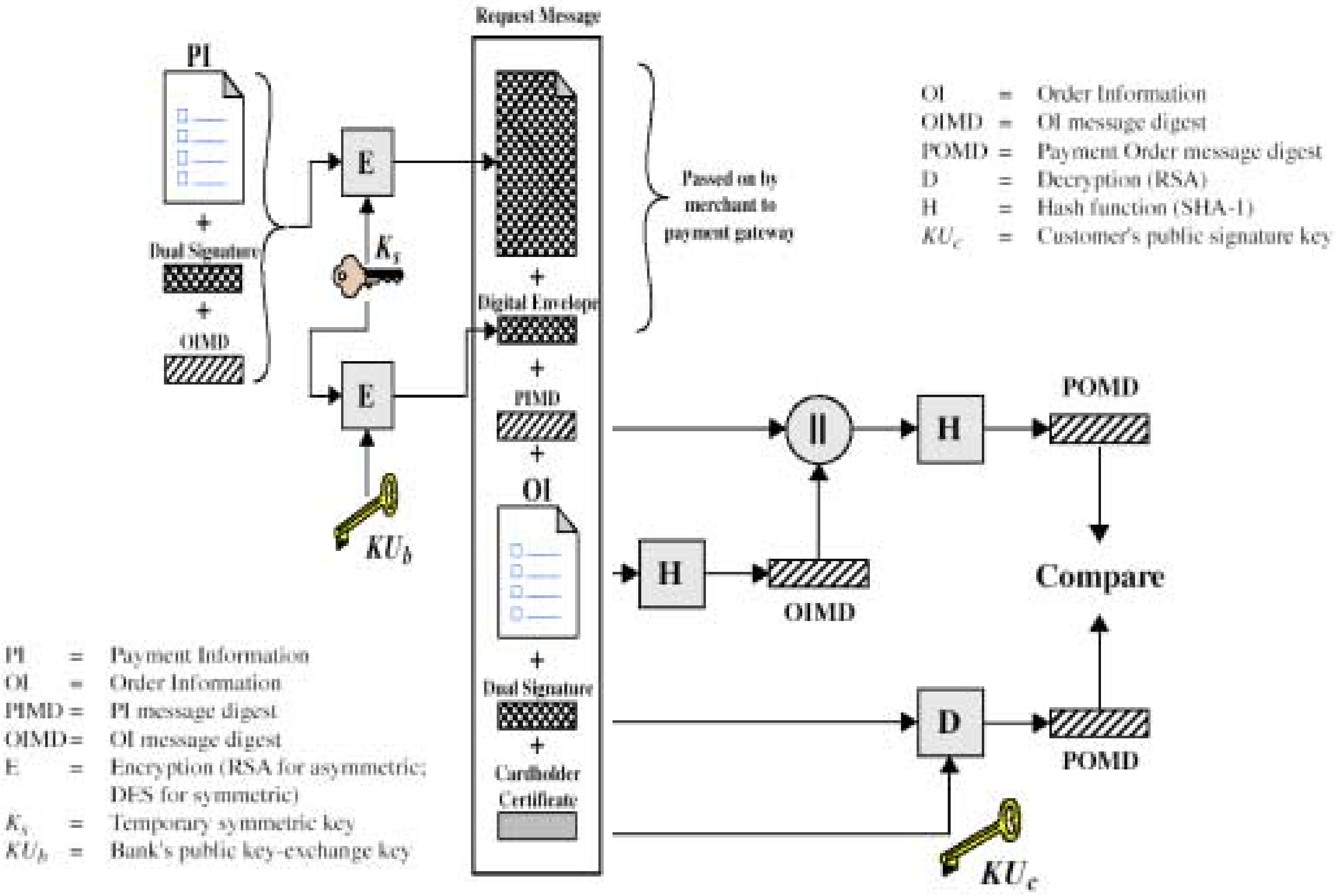

Figure 1- Cardholder Sends Purchase Request / Merchant Verifies Customer Purchase Request

3.4. RSA-OAEP

RSA-OAEP (RSA Encryption Scheme - Optimal Asymmetric Encryption Padding) was proposed by Bel-lare and Rogaway in 1994 which is one of the innovations of SET. RSA-OAEP public-key encryption scheme combines the encoding method of OAEP with the encryption primitive RSA. RSA-OAEP takes a plaintext as input, transforms it into an encoded message via OAEP and apply RSAEP (RSA encryption primitive) to the result (interpreted as an integer) using an RSA public key. RSA-OAEP is intended to be both efficient and secure and is designed to encrypt only short messages--typically secret keys for symmetric encryption or MAC algorithms. OAEP ties the security of RSA encryption closely to that of the basic RSA operation. The version of OAEP used in SET is a more advanced version of the original scheme. While existing message formatting methods for RSA encryption have no known flaw, the provable security aspects of OAEP are very appealing. OAEP is very new but already it is a part of the IEEE P1363 standards effort.

RSA-OAEP encryption scheme has been proven to be semantically secure against adaptive chosen-ciphertext attacks in the random oracle model under the RSA assumption. However, the reduction is not tight, and thus it is not clear what security assurances the proof provides. It is recommended that RSA-OAEP be modified to RSA-OAEP+ that has a tighter security reduction, and furthermore can be easily modified to allow encryption of arbitrarily-long messages. Furthermore, the RSA-KEM encryption scheme of which has a tight reduction should be considered as a replacement for RSA-OAEP.

3.5. Dual Signatures

A new application of digital signatures is introduced in SET, namely the concept of dual signatures. Dual signatures is needed when two messages are need to be linked securely but only one party is allowed to read each. The following picture shows the process of generating dual signatures.

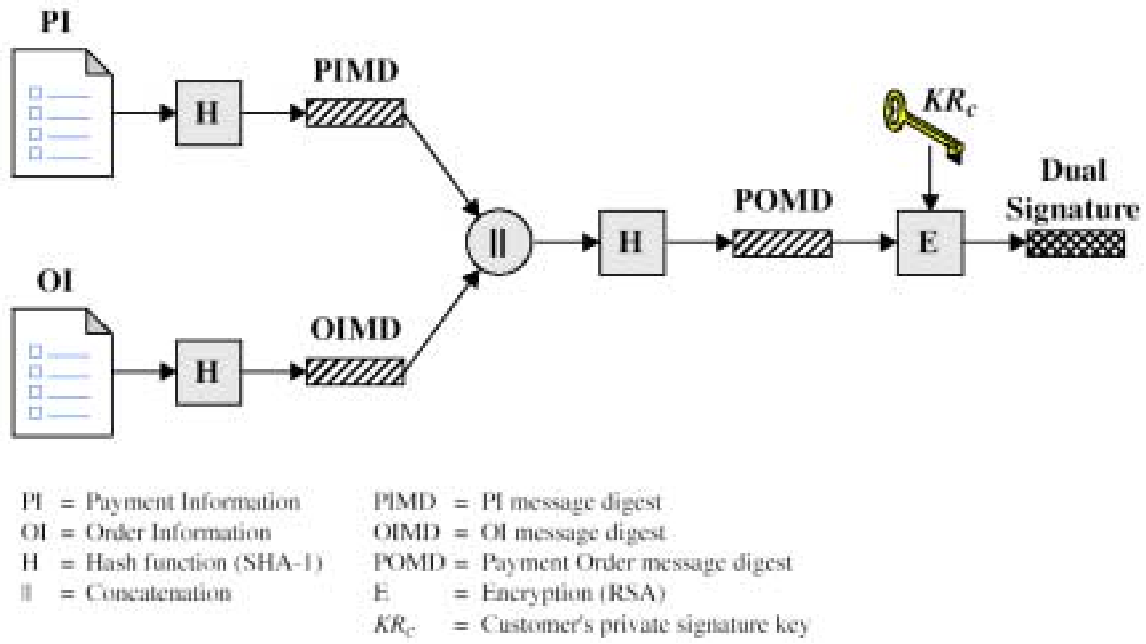

Figure 2- Construction of Dual Signatures in SET

In SET, dual signatures are used to link an order message sent to the merchant with the payment instructions containing account information sent to the acquirer (merchant bank). When the merchant sends an authorization request to the acquirer, it includes the payment instructions sent to it by the cardholder and the message digest of the order information. The acquirer uses the message digest from the merchant and computes the message digest of the payment instructions to check the dual signatures.

4. SET Process

The SET protocol utilizes cryptography to provide confidentiality of information, ensure payment integrity, and enable identity authentication. For authentication purposes, cardholders, merchants, and acquirers will be issued digital certificates by their sponsoring organizations. It also use *dual signature*, which hides the customer's credit card information from merchants, and also hides the order information to banks, to protect privacy.

4.1. Process Steps

1). Merchant sends invoice and unique transaction ID (XID)
2). Merchant sends merchant certificate and bank certificate (encrypted
with CA's private key)
3). Customer decrypts certificates, obtains public keys
4). Customer generates order information (OI) and payment info (PI)
encrypted with different session keys and dual-signed
5). Merchant sends payment request to bank encrypted with bank-merchant session key, PI, digest of OI and merchant's certificate
6). Bank verifies that the XID matches the one in the PI
7). Bank sends authorization request to issuing bank via card network
8). Bank sends approval to merchant
9). Merchant sends acknowledgement to customer

4.2. Payment Initialization

The Purpose of the payment initialization is to allow customer to get certificate from the merchant. The initialization request is represented as PinitReq which carries eight fields of information (Table 1). The security field in SET order information is listed in Table 2.

PInitReq: { RRPID, Language, LID_C, [LID_M], Chall_C, BrandID, BIN, [Thumbs]}

Table 1- Fields in Payment Initialization

Field	Information
RRPID	Request/Response Pair ID
Language	Customer's Language
LID_C	Customer's Local ID
[LID_M]	Merchant's Local ID
Chall_C	Customer's challenge salt to Merchant's signature freshness
BrandID	Card Brand (VISA, Master etc.)
BIN	Bank ID Number
Thumbs	Thumbnails (hashes) of of certificates known to Customer

Table 2- Security Field in Order Information

Field	Information	Security
OIData	{TransIDs, RRPID, Chall-C, HOD, ODSalt, [Chall-M], BrandID, BIN, [ODExtOIDs], [OIExtensions]}	
TransIDs	TRANSACTION Ids copied from PinitREs	Globally unique
RRPID	Request/response pair ID	
Chall-C	Copied from corresponding PInitReq	
HOD	DD(HODInput) Links OIData to PurchAmt without compying PurchAmt into OIData, which would create confidentiality problems.	Hash of order data
ODSalt	Copied from HODInput	Order data hash (to guard against dictionary attack on order data hash)
Chall-M	Merchant's challenge to Cardholder's signature freshness	Merchant's challenge to cardholder signature freshness
BrandID	Cardholder's chosen payment card brand	
BIN	Bank identification number from the cardholder's account number	
ODExtOIDs	List of object identifiers from ODExtensions in the same order as the extensions appeared in ODExtensions	
OIExtensions	The data in an extension to the OI should relate to the merchant's processing of the order	

5. Certificates Insurance

Before two parties use public-key cryptography to conduct business, each wants to be sure that the other party is authenticated. One way to be sure that the public key belongs to the right party is to receive it over a secure channel directly from the same place. However, in most circumstances this solution is not practical.

An alternative to secure transmission of the key is to use a trusted third party to authenticate that the public key belongs to Alice. Such a party is known as a *Certificate Authority* (CA). Because SET participants have two key pairs, they also have two certificates. Both certificates are created and signed at the same time by the Certificate Authority.

5.1. Certificate of Participants

5.1.1. Cardholder certificates

Cardholder certificates function as an electronic representation of the payment card. Because they are digitally signed by a financial institution, they cannot be altered by a third party and and can only be generated by a financial institution. A cardholder certificate does not contain the account number and expiration date. Instead the account information and a secret value known only to the ardholder's software are encoded using a one-way hashing algorithm. If the account number, expiration date, and the secret value are known, the link to the certificate can be proven, but the information cannot be derived by looking at the certificate. Within the SET protocol, the cardholder supplies the account information and the secret value to the payment gateway where the link is verified.

A certificate is only issued to the cardholder when the cardholder's issuing financial institution approves it. By requesting a certificate, a cardholder has indicated the intent to perform commerce via electronic means. This certificate is transmitted to merchants with purchase requests and encrypted payment instructions. Upon receipt of the cardholder's certificate, a merchant can be assured, at a minimum, that the account number has been validated by the card-issuing financial institution or its agent. In this specification, cardholder certificates are optional at the payment card brand's discretion.

5.1.2. Merchant certificates

Merchant certificates function as an electronic substitute for the payment brand decal that appears in the store window—the decal itself is a representation that the merchant has a relationship with a financial institution allowing it to accept the payment card brand. Because they are digitally signed by the merchant's financial institution, merchant certificates cannot be altered by a third party and can only be generated by a financial institution. These certificates are approved by the acquiring financial institution and provide assurance that the merchant holds a valid agreement with an Acquirer. A merchant must have at least one pair of certificates to participate in the SET environment, but there may be multiple certificate pairs per merchant. A merchant will have a pair of certificates for each payment card brand that it accepts.

5.1.3. Payment Gateway Certificates

Payment gateway certificates are obtained by Acquirers or their processors for the systems that process authorization and capture messages. The gateway's encryption key, which the cardholder gets from this certificate, is used to protect the cardholder's account information. Payment gateway certificates are issued to the Acquirer by the payment brand.

5.1.4. Acquirer Certificates

An Acquirer must have certificates in order to operate a Certificate Authority that can accept and process certificate requests directly from merchants over public and private networks. Those Acquirers that choose to have the payment card brand process certificate requests on their behalf will not require certificates because they are not processing SET messages. Acquirers receive their certificates from the payment card brand.

5.1.5. Issuer Certificates

An Issuer must have certificates in order to operate a Certificate Authority that can accept and process certificate requests directly from cardholders over public and private networks. Those Issuers that choose to have the payment card brand process certificate requests on their behalf will not require certificates because they are not processing SET messages. Issuers receive their certificates from the payment card brand.

5.1.6. SET Certificate Hierarchy

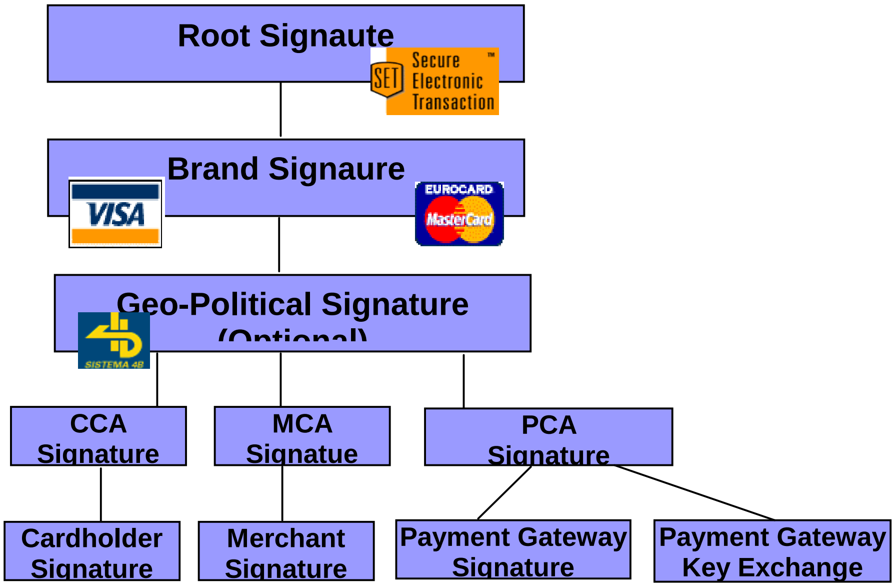

Figure 3- Hierarchy of Trust

5.2. Registration

5.2.1. Participants Registration

As described in section 1, both the cardholder and the merchant have to register with a CA before they can do transactions. And the registration processes have to be secure enough, since these two processes involve sensitive details.

Cardholder Registration

This process comprised 6 messages between two parties: cardholder and Issuer (CA).

1. The cardholder initiates request to the CA.
2. After the CA receives message 1 from the cardholder, the CA replies. The message includes the CA's public key-exchange key certification signed by root CA, CA's signature certificate and the initial request encrypted using CA's private key.
3. The cardholder request a registration form in this message. He randomly generates a symmetric key K1, which is used to encrypt the request, and sends this along with a digital envelop including key K1 and his credit card number.
4. The CA determines the cardholder's issuing bank by the credit card number and returns the appropriate the form, which is signed by the CA and along with CA's signature certificate.
5. The cardholder generates a public/private signature key pair, two symmetric keys K2, K3 and a random number S1. He creates a message with his filled registration form, public key, and K2, and its digital signature. This message is encrypted using K3 and sent with a digital envelop including K3 and card number.
6. The CA verifies the information, then issue a digital ID to CA. The CA generates a secret value using the random number S2 generated by the CA and S1. This secret value, the account number and the expiration date further feed into a one-way hashing to generate a secret number. The CA signs the certificate includes this secret number and the cardholder's public signature key. Then, CA sends this certificate encrypted using K2 along with and its signature certificate.

This registration process includes 3 steps. The first two messages are about to get CA's public key. Once the cardholder has CA's key-exchange key, he can request a registration form in message 3 and 4. The certificate is in the last 2 messages.

Merchant Registration

The Merchant' registration is simpler than cardholder's, which include 4 messages. The first two messages are almost same as cardholder's, except in the second message the registration form has been sent. The merchant has to generate two public/private key pairs – one is for signature, the other is for key-exchange—instead of one pair compared to the cardholder.

5.2.2. Two problems with registration protocol

The registration protocol has been proved to be secure [3]. But there are two risks to cause insecure. The first is that the cardholder is not required to generate a fresh signature key pair, but may register an old one. There is a risk that the old one could be compromised. And another problem is that the secret value generation mentioned above which is the exclusive-OR of numbers (S1, S2) chosen by two parties. Since exclusive-OR is invertible, a criminal working for a CA can give every cardholder the same secret value. This combination introduces some risk that a criminal can impersonate the cardholder.

These two problems are fixable. The first insecurity can be repaired in the cardholder's implementation. The second one can be fixed by replacing exclusive-OR by one-way hashing.

6. Security of SET

Cryptography Algorithm in SET

- Symmetric encryption
  – DES (Data Encryption Standard) : 56bit key, protect financial data
  – CDMF (Commercial Data Masking Facility) : 40 bit key, protect acquire-to cardholder message
- Asymmetric encryption and digital signature : RSA
- Hash function : SHA-1
- Message Authentication Code : HMAC (based on SHA-1)

Security Technology in SET

- Digital envelopes, nonces, salt and Dual signatures

- Two public-private key pairs for each party
  –One for digital signatures; one for key exchange messages

- 160-bit message digests

- Statistically globally unique IDs (XIDs)

- Certificates (5 kinds)
  –Cardholder, Merchant, Acquirer, Issuer, Payment Gateway

- Hardware cryptographic modules (for high security)

- Idempotency (message can be received many times but is only processed once) *f* (*f* (*x*)) = *f* (*x*)
- Complex protocol. Over 600 pages of detail

6.1. SET Security Recommendations

SET is not secure if its servers are not secure:

• Dedicate a machine to the Merchant Server and POS software.
• Use a firewall to insulate it from the Internet and intranet. Do not allow FTP or telnet on other ports.
• Remove all unnecessary software from the Merchant Server.
• Only SET-defined protocol ports should be open to computers outside the firewall.
• Merchant Server software should interface with POS software only through APIs.
• Need to protect transaction databases against access/alteration.

7. Future of SET

SET can work in Real Time or be a store and forward transfer, and is industry backed by the major credit card companies and banks. Its transaction can be accomplished over the WEB or via email. It provides confidentiality, integrity, authentication, and, or non-repudiation.

Table 3- SET Future Technology

Algorithm	Now	Near-Future	Future
Symmetric(encrypts order instruction)	DES	Triple DES	(AES)
Hash (digests message)	SHA-1	?	?
Asymmetric (data integrity for authentication; key management)	RSA	ECC (ElGamal+Diffie Hellman+DSA)	?

Confidentiality

- payment info is secure
- but order info is not secure

Data Integrity

- Uses mathematical techniques to minimize corruption or detect malicious tamper

Client Authentication

- Digital ID (certificate) used to identify costumer
- Digital ID (certificate) checked via the card's Issuer

Merchant Authentication

- Digital certificate again used as a back check for confirming the merchant is valid
- The check generally against a dB held by the issuer of the card

Interoperability

- Has not been achieved
- IBM and VeriFone(Hewlett-Packard) are working together to make their individual products interoperable.
- Results in many different "interoperable" versions of SET, instead a single protocol

SET is safe since it addresses all the parties involved in typical credit card transactions: consumers, merchants, and the banks. Besides the interoperability problem, it has difficulties to spread since it needs all the participants to have some part of the software, even very expensive hardware. It may be clearly in the interests of the credit card companies and banks, but it looks quite different from the perspective of merchants and consumers. In order to process SET transactions, the merchants have to spend several million dollars in equipment and services when they already have what are arguably sufficient security provisions in SSL. To consumers, they have to install software, "Anything that requires consumers to take an extra step deters them from adopting it," Vernon Keenan, a senior analyst at Zona Research argues.

SET is a very comprehensive and very complicated security protocol. It has to be simplified to be adopted by every parties involved, otherwise, it might be abandoned.

References:

[1] Nikki Goth Itoi. PROMISES, PROMISES What ever happened to SET?
http://www.herring.com/mag/issue51/promises.html

[2] SetCo. SET *Secure Electronic Transaction Specification*: Business Description, May 1997.
http://www.setco.org/set_specifications.html

[3] Lawrence C. Paulson. SET Cardholder Registration: The Secrecy Proofs (Extended Abstract). *Lecture Notes in Computer Science*, Vol 2083, 2001.

[4] Enabling technologies: SET in action.
http://sellitontheweb.com/ezine/tech31.shtml

[5] Jeff Crume. Cryptography and SET.
http://www3.ibm.com/software/webservers/commerce/payment/cryptset.html

[6] What is SET.
http://www.ibm.com/software/webservers/commerce/payment/whatisset.html

[7] Payment Processing.
http://www.ibm.com/software/webservers/commerce/payment/support/overview.html

[8] Secure Electronic Transactions: An Overview
http://www.davidreilly.com/topics/electronic_commerce/essays/secure_electronic_transactions.html

[9] The SET Standard Book 1 Business Description
http://www.setco.org/download/set_bk1.pdf

[10] Electronic Payment Systems (20-763) Official Course Web
http://euro.ecom.cmu.edu/program/courses/tcr763/2002pgh/cards7.ppt

[11] Evaluation of Security Level of Cryptography: RSA-OAEP, RSA-PSS, RSA Signature
http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1049_ace.pdf

[12] RSA-OAEP algorithm specification and supporting documentation (.PDF)
ftp://ftp.rsasecurity.com/pub/rsalabs/rsa_algorithm/rsa-oaep_spec.pdf