Abstract—Internet is widely used for many purposes such as entertainment, information, communication, Electronic commerce etc. In the emerging global economy, e-commerce and e-business have increasingly become a necessary component of business strategy and a strong catalyst for economic development. Electronic commerce or e-commerce refers to a wide range of online business activities for products and services. It also, pertains to “any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact.” Online transactions are an important part of the electronic commerce. Due to the frequently use of electronic transactions in the internet the security is the main concern of it how can we provide security to the online transaction so that any intruder in the middle can’t affect the transaction so that integrity of the transaction remains constant. SET (Secure Electronic Transaction) protocol is designed for this purpose. SET was developed by SETco, led by VISA and MasterCard (and involving other companies such as GTE, IBM, Microsoft, Netscape, RSA and VeriSign) starting in 1996 Credit card, smart card etc. Secure electronic transaction protocol is responsible for the financial exchange of money securely between buyers and sellers in the online environment. It provides the authentication, integrity, and confidentiality of the electronic transactions.

Keywords—Electronic Commerce, SET, Authentication, Intruder, Integrity, Confidentiality.

I. INTRODUCTION

Electronic commerce or e-commerce refers to a wide range of online business activities for products and services. It also pertains to “any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact. Online transactions are an important part of the e-commerce. When we sell or buy any product or service online then we have to pay for this. Online payment is done with the help of online transactions. For the successful online transaction there should be a protocol and that protocol should contain some properties related to the security and other aspects. SET (Secure Electronic Transaction) protocol is designed for this purpose. Credit card, smart card etc. transactions comes under the category of Secure Electronic Transactions.

Secure Electronic Transaction Protocol:

SET Secure Electronic Transaction is considered the major player of the payment process in the electronic commerce business. It is a very comprehensive security protocol which utilizes cryptography to provide confidentiality of information. It insures the payment integrity and identity authentication. The main and basic essential requirement of the SET protocol is to perform the Electronic transactions in a secure manner.

SET protocol:

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

- Provides confidentiality of information.
- Ensure the integrity of payment instructions for goods and services order Data.
- Authenticate both the cardholder and merchant.

Properties of Secure Electronic Transaction Protocol:

There are mainly the following properties of the Secure Electronic Transactions:-

Confidentiality: Confidentiality is the protection of transmitted data from passive attack. SET provides the confidentiality in the proper way. It ensures the cardholder and other participants that their instructions (payment information, order information etc.) are safe and accessible by only by the deliberate recipient. The information messages are secured as they travel across the network preventing interference by the unauthorized individuals.

Authentication: The authentication service is concerned with assuring that a communication is authentic. SET provides the authentication in the following two ways.

Card holder Account authentication: Merchant needs to verify that the particular customer is an alleged user of the particular branded payment card account no.

Merchant Authentication: The SET specification provides a way for cardholder to confirm that a merchant has a relationship with a financial institution allowing it to accept payment cards. Certification Authority plays an important role in the authentication.

Integrity: Data Integrity means that data send by the sender side is received by the receiver side as it was send by the sender. There is no modification or change in the data. The SET specifies that the content of the message should not alter during the transmission between the participants. If it will be altered then the transaction will not processed. It provides a way that the information send is matched with the information received.

II. SCOPE OF THE SET

SET uses the cryptography technique such as encryption and decryption, and two main methods Secret key cryptography and public-key cryptography. The public key cryptography allows a merchant to create a public or private key pair and publish the public key, allowing any customer to send a secure message to the merchant. The secret key cryptography used in SET is the DES (Data Encryption Standard), it is used by the financial institutions to encrypt PIN sans public key cryptography used in a SET is RSA.

Use of symmetric Key:

It uses the same key to encrypt and decrypt the messages. The sender and the receiver of the message must share the same key. This requires trust between the parties who share
the messages and share the key. Example of this kind of cryptography is the Data Encryption Standard (DES), used by financial institutions to share the personal identification numbers (PINs). This type of cryptography is also known as Secret-key Cryptography.

**Use of Public Key Cryptography:**
In this approach, each participant creates two unique keys. One is called the “public key” which is published to all and the other is called the “private key” which the participant keeps it secret from others. Also, one key is used for encrypting the data while the other key is used for decrypting the data. An example of the public-key cryptography is the well-known RSA algorithm. This kind of cryptography is well suited in situations where the user has to share his key to many unknown participants.

**Use of Digital Signature:**
A digital signature provides a way to associate the message with the sender. It helps in ensuring the authenticity and integrity of the message. When combined with message digests, encrypting messages using private keys allows users to digitally sign the messages. A message digest is a unique value generated for that particular message. Passing the message through a one-way cryptographic function generates a message digest. This message digest is then encrypted using the sender’s private key and is appended to the original message resulting in the digital signature of the message. The recipient of the digital signature can be sure that the message really came from the sender because changing even one character in the message changes the message digest in an unpredictable way. It is computationally unfeasible to generate two different messages that have the same message digest.

**SET Participants:**
There are the following participants in the SET protocol.

**Cardholder:** The cardholder is an authorized person holding the payment card such as credit card or smart card etc. Cardholder can perform online transactions with the help of the payment cards.

**Merchant:** The merchant is an authorized person or an organization that provides goods or services to the cardholder (customer). A merchant must have a relationship with an Acquirer for accepting payments on the Internet.

**Acquirer:** This is a financial institution that has a relationship with merchants for processing payment card authorizations, cardholder’s account credit limits and payments. The reason for having acquirers is that merchants accept credit cards of more than one brand, but are not interested in dealing with so many bankcard organizations or issuers.

**Issuer:** The issuer is a financial institution (such as bank) that provides a payment card to cardholder.

**Payment Gateway:** The payment gateway processes the payment messages. Specifically in SET, the payment gateway acts as an interface between SET and the existing card payment networks for payment authorizations. The merchant exchanges SET messages with the payment gateway over the Internet.

**Certification Authority:** This is an authority that is trusted to provide public key certificates to cardholders, merchants and payment gateways. It will provide the X.509 V3 certificates.

**III. WORKING OF SET PROTOCOL**

**Working Steps of SET Protocol:**
Visa and MasterCard designed the SET protocol to solve the problems occurred in the Electronic transactions. It keeps the information confidential and provides the integrity and authenticity. To achieve there are the following main Steps:-

1. The first step deals with the cardholder registration. It allows a cardholder to register his/her credit card with a certification authority. The request includes the cardholder’s public signature key and a secret nonce. The outcome of the registration is a public key certificate that includes the hash of the credit card number (Called the PAN) and a secret nonce, with the same role of the PIN for physical cards.

2. The merchant who supports the online transactions must have two keys. One key is for signing the messages and another is required for the key-exchange. These keys are obtained by the two certificates. The merchant must have a copy of the payment gateway public key certificate for the processing of the payment.

3. The customer place order to the merchant through the website. For this he/she will send the list of items to be purchased, to the merchant. Then the merchant returns an order from to the customer. This order form contains the Order No., list of items, individual price of items, quantity of the items, total price etc. A copy of merchant’s certificate is also send by the merchant that the customer can verify that the particular merchant is legal person for the transaction or not.

4. If the order form is according to the customer requirement then customer sends the purchase request message. That message includes the payment related information, information of the items to be purchased and certificates of the customer to the merchant. The merchant can verify the customer through the customer’s certificate. The payment information contains the information such as
credit card details (Card No., expiration date etc). This information is confidential and should not be viewed by the merchant for this purpose it is encrypted in such manner that merchant is unable to decrypt it.

The merchant can be assured that the financial institution responsible for issuing the card has validated the account number of the cardholder.

**Merchant Certificate:**
This certificate is an electronic representation that the merchant has a relationship with a financial institution allowing it to accept the payment card brand. Since the financial institution digitally signs them a third party cannot alter them. These certificates are just an assurance that the merchants hold a valid agreement with an Acquirer. A merchant has at least one pair of certificates to participate in the SET environment. Basically, it has a pair of certificates for each payment card brand it accepts.

**Payment Gateway Certificate:**
Acquirers who process authorization and capture messages obtain payment gateway certificate. Payment gateway certificates are issued to the Acquirer by the payment brand.

**Acquirer Certificate:**
In order to accept and process certificate requests from merchants over public and private networks, an acquirer must have a certificate. Acquirers receive their certificates from their payment card brand.

**Issuer Certificate:**
Similar to the Acquirer, the Issuer possesses a certificate to accept and process certificate requests from cardholders over public and private networks. Also, they receive the certificate from the payment card brand. If the Acquirer or the Issuer chose to have the payment card brand process the certificate requests, they will not require certificates because they are not processing SET messages.

### IV. PAYMENT PROCESSING IN SET

The payment processing in SET involves the transfer of messages between the participating entities. The following messages are transferred in any SET payment transaction: Cardholder Registration, Merchant Registration, and Purchase Request, payment Authorization and Payment Capture. At any point during the SET payment flow the following enquiry messages can be transferred, although they are optional: Certificate status inquiry, Purchase inquiry, and Authorization reversal, Capture Reversal, Credit Reversal and Error Message.

**Cardholder Registration:**
Cardholders must register with a Certificate Authority (CA) before they can send SET messages to merchants. The entire registration process goes through the following steps.

1. The cardholder computer initiates the registration process by sending the INITIATE REQUEST message to CA. The CA sends a response to the request by sending the INITIATE RESPONSE to the cardholder.
2. The cardholder receives the response from the CA and requests the registration form by sending the REGISTRATION FORM REQUEST to the CA. The CA processes the request and sends the registration form through the REGISTRATION FORM message.
3. The cardholder then sends the CARDHOLDER CERTIFICATE REQUEST message to the CA. The CA upon receiving the request message will process that and eventually respond by sending the cardholder’s certificate by sending the CARDHOLDER CERTIFICATE.

4. The above sequence of sending and receiving of messages ends when the cardholder receives his certificate. At any point during the transfer of messages if something is amiss, either one of the participating entities will send the ERROR message and the transaction will be aborted. The transfer of many messages characterizes SET protocol.

**Merchant registration:**

Like cardholders, the merchants must register with a Certificate Authority (CA) before they can receive SET payment messages from cardholders or process SET transactions through a payment gateway. The registration process starts when the merchant software requests a copy of the CA’s key exchange certificate and the appropriate registration form. The entire merchant registration flow of messages is summarized below.

1. Initially, the merchant computer requests the registration form from the CA by sending the INITIATE REQUEST. The CA on receiving the request from the merchant processes the request and sends the registration form through the REGISTRATION FORM message.

2. On receiving the registration form from the merchant requests the certificate by sending the MERCHANT CERTIFICATE REQUEST message to the CA. The CA processes the request and generates the certificates and passes to the merchant through the MERCHANT CERTIFICATE messages.

**Purchase Request:**

1. Cardholder software creates a purchase initiate request, containing the name of the credit card brand that the cardholder has elected to use. This request is effectively asking for a copy of the merchant certificate containing its public signature key and payment gateway certificate containing its public key-exchange key. The cardholder sends the initiate request to the merchant.

2. The merchant receives the initiate request. The merchant generates the response message and digitally signs it by passing the response through a hash function. The message digest created by this is encrypted with the merchant private signature key, resulting in a digital signature. The merchant sends the initiate response, the digital signature, the merchant certificate containing the public signature key and the payment gateway certificate containing the public key-exchange key to the cardholder.

3. The cardholder receives the initiate response message from the merchant and verifies the merchant and payment gateway certificates by traversing the trust chain to the root. These certificates will be used later during the ordering process. The merchant signature is verified by running the initiate response through a hash function and creating a message digest. The digital signature is decrypted using the merchant public signature key and the result is compared with the message digest obtained from the received message. If they are equal, the integrity of the message is assured. The cardholder software creates the order instruction (OI) portion of the purchase request message using information from the shopping phase. The OI does not contain the description of the goods purchased. This information was exchanged between the cardholder and the merchant during the shopping process and before the first SET message.

3.1 The cardholder creates the second portion of the purchase request, the payment instruction (PI). This contains details of the credit card that the cardholder has chosen to use.

3.2 A transaction identifier, received from the merchant in the initiate response, is placed in the OI and PI. This identifier will be used by the payment gateway to link the OI and PI when the merchant requests payment authorization. The cardholder generates a dual signature by passing the order instruction and payment instruction through a hash function. The two message digests created (OI message digest and PI message digest) are concatenated. The resulting message is run through a hash function and is encrypted with the cardholder private signature key. This is the dual signature.

3.3 The PI, dual signature and OI message digest are encrypted using a randomly generated symmetric key. This is the encrypted payment message, which will be passed on to the payment gateway.

3.4 The symmetric key used to construct the payment message and the cardholders account number are encrypted with the payment gateway public key-exchange key, generating the payment digital envelope.

3.5 The encrypted payment message, PI message digest, order instruction (OI) message, payment digital envelope, dual signature and the cardholder certificate containing its public signature key are sent to the merchant.

4. The merchant receives the request message and verifies the cardholder certificate by traversing the trust chain to the root. The public key in this certificate will be needed to check the dual signature.

4.1 The dual signature is verified by running the order instruction (OI) through a hash function and creating the OI message digest. This message digest is concatenated with the PI message digest that was received within the request message. The dual signature is decrypted using the cardholder public signature key and the result is compared with the OPI message digest obtained locally. If they are equal, the merchant can be assured of the integrity of the request.

4.2 The merchant processes the order request and forwards the encrypted payment message and payment digital envelope to the payment gateway for payment authorization. The merchant does not need to wait for a response to its authorization request before it sends a response to the cardholder’s request.

4.3 The merchant creates the response message and digitally signs it by passing it through a hash function. The message
digest so created is encrypted with the merchant private signature key, resulting in a digital signature.

4.4 The CA sends the purchase response, the digital signature and the merchant certificate containing the public signature key to the cardholder. This message only indicates that the merchant received the order. The services or goods purchased by the cardholder will only be executed or shipped when the merchant receives a payment authorization response from the payment gateway. After the cardholder receives the confirmation that the merchant received the order information, he or she can send inquiries to the merchant to know if the authorization has been performed.

5. The cardholder receives the response from the merchant. This tells him or her that the purchase request has been accepted and that he or she can expect to receive the goods, as long as the card has enough credit remaining.

5.1 The cardholder receives the purchase response message from the merchant and verifies the certificates by traversing the trust chain to the root.

5.2 The merchant signature received is verified by running the purchase response through a hash function and creating a message digest. The digital signature from the response is decrypted using the merchant public signature key and the result is compared with the message digest obtained locally. If they are equal, the cardholder is assured of the integrity of the message.

5.3 The cardholder stores the purchase response. The cardholder can determine the status of the order (if the payment gateway approved the transaction) by sending an order inquiry message to the merchant. If it was approved, the goods purchased will be shipped or the services will be performed.

V. PAYMENT AUTHORIZATION

1. The merchant software creates an authorization request including the amount to be authorized, the transaction identifier from the order instruction (OI), a locally generated digest of the OI and other information related to the transaction.

2. The merchant digitally signs the authorization request by passing it through a hash function, creating a message digest. The message digest is encrypted with the merchant’s private signature key resulting in a digital signature.

3. The authorization request and the digital signature are encrypted using a randomly generated symmetric key (1). We refer to this as key (1) because a second key is also used in this process.

4. Symmetric key (1) is then encrypted with the payment gateway public key exchange key, generating the digital envelope.

5. The merchant sends the authorization request message, the payment message created during the cardholder’s purchase process, the cardholder certificate containing the public signature key, the merchant certificate containing the public signature key, and the other merchant certificate containing the public key-exchange key to the payment gateway.

![Fig 4. Payment Gateway Processes the Payment Authorization Request](image)

When the payment gateway receives the authorization Request, it first has to disassemble it and validate it.

1. The payment gateway receives the authorization message and verifies the merchant certificates by traversing the trust chain to the root. It also verifies that the certificate have not expired.

2. The payment gateway decrypts the digital envelope contained in the authorization request message using the payment gateway private key-exchange key thereby obtaining symmetric key (1).

3. Symmetric key (1) is used to decrypt the encrypted authorization request to obtain the authorization request message and the digital signature.

4. Digital signature is verified by running the authorization request through a hash function to create a message digest. The digital signature from the request is decrypted using the merchant public key and the result is compared with the message digest obtained locally. If they are equal, the integrity of the request is assured.

5. The payment gateway verifies the cardholder certificate by traversing the trust chain to the root. It also verifies that the certificate has not expired.

6. The payment gateway decrypts the payment digital envelope contained in the payment message using the payment gateway private key-exchange key to obtain the symmetric key (2) and the cardholder account information.

7. This symmetric key is used to decrypt the encrypted payment message to obtain the payment instruction (PI) and dual signature.

8. The dual signature is verified by running the PI through a hash function to create the PI message digest. The PI message digest is concatenated with the OI message digest received from the merchant as part of the authorization request. The two digests are then run through a hash function to generate the OPI message digest. The dual signature is decrypted using the cardholder public signature key and the result (which is the OPI digest originally calculated by the cardholder) is compared with the OPI message digest generated locally. If they are equal, the payment gateway can be assured that the two halves of the
message match each other and they have not been altered in any way.
The payment gateway also verifies the integrity of the transaction by checking that the transaction identifier received from the merchant matches the identifier sent with the cardholder payment instruction.

VI. MERCHANT PROCESSES RESPONSE
1. The merchant receives the response message and verifies the payment gateway certificate by traversing the trust chain to the root. The public key in this certificate will be used to check the digital signature included in the encrypted authorization message.
2. The merchant decrypts the authorization digital envelope using the merchant’s private key-exchange key to obtain the symmetric key (2).
3. Symmetric key(2) is used to decrypt the encrypted authorization message to obtain the authorization response and digital signature.
4. The digital signature is verified by running the authorization response through a hash function and creating a message digest. The digital signature is decrypted using the payment gateway public signature key and the result is compared with the message digest obtained locally. If they are equal, the integrity of the message has been proved.
5. The merchant stores the encrypted capture message and capture digital envelope for later capture processing.

Payment Capture Process:
At some point in time after the purchase transaction, the merchant will want to get paid. The process to request the payment begins when the merchant sends a capture request to the payment gateway including the amount of the transaction authorized. The payment gateway receives the request and sends it to the issuer (cardholder’s financial institution) via a financial network. The payment gateway sends a capture response to the merchant that will store it to be used for reconciliation with payment received from the acquirer.

VII. MERCHANT REQUESTS PAYMENT
1. The merchant software creates a capture request including the final amount to be authorized, the transaction identifier from the order instruction (OI) and other information related to the transaction.
2. The merchant digitally signs the capture request by passing it through a hash function. The message digest created is encrypted with the merchant’s private signature key to create a digital signature.
3. The capture request and the digital signature are encrypted using a randomly generated symmetric key (4), resulting in the encrypted capture request message.
4. Symmetric key(4) is encrypted with the payment gateway public key exchange key, generating the capture request digital envelope.
5. The capture token message, which was received from the payment gateway in the authorization response, will be sent to the payment gateway together with the encrypted capture request message, capture request digital envelope, the two merchant certificates containing the signature key and the key-exchange key.

Payment Gateway Processes Capture Request
When the payment gateway receives the capture request from the merchant, it must first unscramble the message, then initiate the funds transfer and inform the merchant of the result.
1. The payment gateway receives the capture message and verifies the merchant certificates by traversing the trust chain to the root.
2. The payment gateway decrypts the capture request digital envelope using the payment gateway private key-exchange key to obtain the symmetric key (4).
3. This symmetric key(4) is used to decrypt the encrypted capture request message to obtain the capture request and digital signature.
4. The digital signature is verified by running the capture request through a hash function and creating a message digest. The digital signature is decrypted using the merchant public signature key and the result is compared with the message digest obtained. If they are equal, the payment gateway is assured of the integrity of the message.
5. The payment gateway decrypts the capture token digital envelope using the payment gateway private key-exchange key to obtain the symmetric key (3).
6. This symmetric key (3) is used to decrypt the encrypted capture token message to obtain the capture token.

The payment gateway checks for consistency between the capture request and capture token. It then uses the information from the capture request and capture token to create a clearing request that is sent to the issuer using a private bank card network. This request causes funds to be transferred to the merchant’s account. Finally, the payment gateway has to send notification of the result of the capture operation back to the merchant.
1. The payment gateway creates a capture response and passes it through a hash function, creating a message digest. This message digest is encrypted with the payment gateway private signature key, creating a digital signature.
2. The capture response and the digital signature are encrypted using a randomly generated symmetric key (5). The result is the encrypted capture response message.
3. The symmetric key (5) is encrypted with the merchant public key exchange key, generating the capture response digital envelope.
4. The capture response message including the encrypted capture response message, capture response digital envelope and payment gateway certificate including the signature key are sent to
the merchant.

VIII. MERCHANT PROCESSES RESPONSE
The capture response is the merchant’s proof that payment has been made. It needs to log the information contained in it in case of discrepancy.

1. The merchant receives the capture response message and verifies the payment gateway certificate by traversing the trust chain to the root. This certificate will be used to check the digital signature included in the encrypted capture response message.

2. The merchant decrypts the capture request digital envelope using the merchant private key-exchange key to obtain the symmetric key (5).

3. This symmetric key (5) is used to decrypt the encrypted capture response message to obtain the capture response and digital signature.

4. The digital signature is verified by running the capture response through a hash function to create a message digest. The digital signature is decrypted using the payment gateway public signature key and the result is compared with the message digest obtained locally. If they are equal, the message integrity has been assured.

5. The merchant stores the capture response to be used for reconciliation with payment received from the acquirer.

IX. CONCLUSION
All through the years since it was first announced by Visa International and MasterCard in beginning of 1996, SET today has mature technical specifications and has a very wide market acceptance. Today all components of SET, have the ability to process SET secured transactions. There are already products for each component, Certificate Authorities, Payment Gateways, merchants and cardholders, which make the system successfully run. SET is safer than other payment methods.

REFERENCES


