Secure Electronic Transaction (SET) Protocol

As more and more companies are opting Internet as a medium for electronic commerce, trust and security requirements are increasing. The important security requirements for a successful e-commerce transaction are presented in table 1.

TABLE 1: IMPORTANT SECURITY REQUIREMENTS

REQUIREMENT	DESCRIPTION
Privacy	Information shared among the communicating parties must be known only to them. All others must be kept out of the loop.
Authentication	Both the communicating parties must be in a position to establish and prove their identities.
Integrity	The message that is transmitted by the sender should not be tampered. If tampered, the receiver must be in a position to identify the same and discard the message.
Non-Repudiation	Both the communicating parties must have the facility to legally prove that messages have been sent and received.

HOW ARE THESE SECURITY REQUIREMENTS ACHIEVED?

These four prime security requirements are achieved using cryptographic techniques. Cryptographic techniques are broadly classified into symmetric key cryptographic technique and asymmetric key cryptographic technique.

In symmetric key cryptographic technique, the same key is used for both encryption and decryption. The sender must have a copy of the key for encryption and the receiver must have a copy of the key for decryption. Figure 1 shows how a symmetric key encryption works.

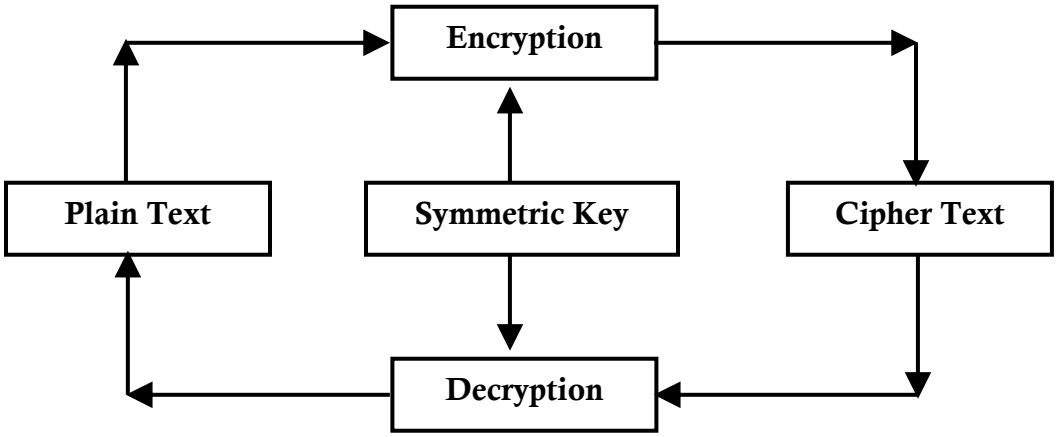

Figure 1: Working of a symmetric encryption

Symmetric key encryption techniques are efficient, fast and consume less computer resources of processor and memory. However, their main drawbacks are:

1. **The sender must send a copy of the key to the receiver for decryption**
2. **The sender must use different keys for different user and**
3. **It is not possible to digitally sign the message.**
4. **It is difficult to enforce non-repudiation for both the communicating parties share the same key.**

Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES) are good examples of symmetric encryption algorithms.

The drawbacks of symmetric encryption method were overcome using asymmetric key encryption techniques. Here, every user has a pair of keys, a public key and a private key. The public key of a user is known to all while the private key is kept secret. Every message that is sent is encrypted using the public key of the receiver and decrypted using the private key of the receiver. Figure 2 shows how a asymmetric key encryption system works.

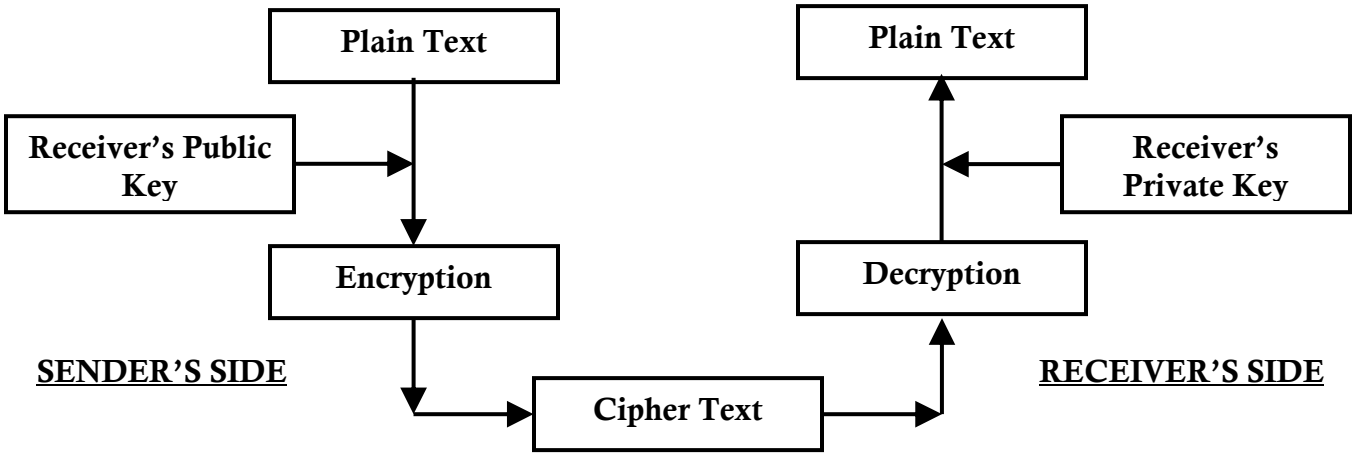

Figure 2: Working of a Asymmetric Key Encryption System

While the disadvantages of symmetric key encryption system are taken care off, asymmetric key encryption systems are slow, inefficient and consume considerable computer resources. RSA algorithm is a typical example of asymmetric key encryption technique.

TRANSACTION SECURITY PROTOCOLS

To successfully implement an e-commerce transaction, two acceptable protocols that are deployed are:

a) Secure-Socket Layer (SSL) protocol
b) Secure Electronic Transaction (SET) protocol

SSL PROTOCOL

Netscape Inc originally created the Secure Sockets Layer (SSL) protocol. On account of its popularity and acceptance, it is now implemented in all web browsers.

SSL has two main objectives:

1. **To ensure confidentiality, by encrypting the data that moves between the communicating parties (client and the server).**
2. **To provide authentication of the session partners, using RSA algorithm.**

The SSL protocol consists of two protocols:

1. **The SSL Handshake protocol, in which the communicating parties (client and the server) authenticate themselves and negotiate an encryption key. One point to note here is that the SSL there is significant additional overhead in starting up an SSL session.**
2. **The SSL Record protocol, in which the session data is exchanged between the communicating parties (client and the server) in an encrypted fashion.**

The ten steps in a SSL transaction are:

1. **The client first sends a request by introducing itself.**
2. **The server acknowledges.**
3. **The server sends its certificate to the client.**
4. **The client checks if the certificate was issued by a Certificate Authority (CA) it trusts.**
5. **The client then compares the information in the certificate with the information it just received concerning the site.**
6. **The client then tells the server what encryption algorithms are to be used.**
7. **The client then generates a session key using the agreed cipher.**
8. **The client then encrypts the session key using the server's public key and sends it to the server.**
9. **The server receives the encrypted session key and decrypts it with its private key.**
10. **The client and the server then use the session key for the rest of the transaction.**

Although SSL protocol has been implemented in all browsers, there are two main risks associated with SSL.

a) **The cardholder is NOT protected from the merchant. If the merchant is dishonest and charge more, users stand to lose.**
b) **Similarly, the merchant is also NOT protected from dishonest customers who supply an invalid credit card number.**

In a nutshell,

- **SSL is a secure message protocol, not a payment protocol**
- **SSL requires the vendor to have a certificate**
- **SSL protocol does not provide facilities for non-repudiation.**

SSL was followed by Transport Layer Security (TLS), which is an Internet Engineering Task Force (IETF) version of SSL. TLS functions very similar to SSL but they do not interoperate.

IBM later developed a standard called Internet Keyed Payment Protocol (iKP), which led to the development of Secure Electronic Transaction Protocol (SET).

SECURE ELECTRONIC TRANSACTION (SET) PROTOCOL

To carry out transactions successfully and without compromising security and trust, business communities, financial institutions and companies offering technological solutions wanted a protocol that works very similar to the way how a credit card transactions work.

Visa and MasterCard, leading credit card companies in the world formed a consortium with computer vendors such as IBM and developed an open protocol which emerged as a standard in ensuring security, authenticity, privacy and trust in electronic transactions.

SET BUSINESS REQUIREMENTS

The main business requirements for SET are:

1. **Provide security, authenticity, privacy, integrity and trust with regard to payment and ordering information**
2. **Provide authentication that a cardholder is a legitimate user of a credit card account**
3. **Provide authentication that a merchant can accept credit card transactions.**
4. **To formulate a protocol that facilitates and encourages interoperability among software and network providers and which does not depend on the transport security mechanism.**

PARTICIPANTS OF THE SET SYSTEM

The main participants of the SET system and their details are presented in table 2.

TABLE 2: MAIN PARTICIPANTS OF THE SET SYSTEM

PARTICIPANT	DETAILS
Cardholder	Refers to the person who holds the card and who makes the purchases on the Internet.
Merchant	A person or organization that has goods or services to sell to the cardholder.
Issuer	Refers to the financial institutions that provide the cardholder with the credit card and are responsible for the payment.
Acquirer	Refers to organizations that provide verbal or telephonic card authorization for merchants. Merchants pay a small fee to the acquirer for their services.
Acquirer Payment Gateway	Acts as an interface between SET and the computer networks of banks. To put it simpler terms, the acquirer payment gateway acts as a proxy for the bank's network functions.
Certifying Authority (CA)	Refers to the organization that provides public key certification. One of the best-known Certifying Authority (CA) is Verisign which offers several classes of certificates. Class 1 certificate is of the lowest level which binds e-mail address and associated public keys. Class 4 certificates are the highest level certificates that apply to servers and their organizations.

HOW SET WORKS?

The following is a simplified version of how SET works.

Before SET can work, there is a preliminary step which has to completed.

Preliminary Step: Both cardholders and merchants must register with the CA (certifying authority).

Actual Steps in SET

Step 1: Customer browses website of the merchant, decides what to purchase and adds them to the shopping cart.

Step 2: Customer then communicates with the merchant and payment gateway in a single message. The message has two parts:
Part a: Purchase Order for use by the merchant
Part b: Card Information for use by the merchant's bank

Step 3: Merchant forwards the card information (part b) to their bank
Step 4: Merchant's bank contacts the issuer and checks with the issuer for payment authorization
Step 5: Issuer authorizes the purchase and sends authorization to Merchant's bank
Step 6: Merchant's bank sends a copy of the authorization to merchant
Step 7: Merchant completes the order and sends confirmation to the customer
Step 8: Merchant captures the transaction from their bank
Step 9: Issuer prints the credit card invoice to customer

Encryption Process in SET

Algorithm used:
1024 bit RSA algorithm for asymmetric encryption process
56 bit DES algorithm for symmetric encryption process
SHA-1 for computing the message digest.

The sequence of steps the sender S adopts in encryption process is as follows:

Step 1: The sender S subjects the message through a hash algorithm. SET uses Secure Hash Algorithm (SHA-1) for this. The output of the hash algorithm is the message digest.

Step 2: Sender S then encrypts the message digest using his RSA private key. The output of this step is the Digital Signature.

Step 3: Sender S then creates a key for the symmetric encryption.

Step 4: **Sender S takes the message, digital signature obtained in step 2 and his digital certificate and encrypts all of them using the symmetric key encryption method of Data Encryption Standard (DES). The result of step 4 is the encrypted message.**

Step 4: **Sender S then picks the public key of the recipient R. Encrypts the symmetric key of step 3. The output is called as digital envelope.**

The encrypted message obtained from step 4 and the digital envelope obtained from step 5 is sent to the receiver R.

Decryption Process in SET

Algorithm used: **1024 bit RSA algorithm for asymmetric encryption process**
56 bit DES algorithm for symmetric encryption process
SHA-1 for computing the message digest.

The sequence of steps the receiver R adopts in decryption process is as follows:

Step 1: **Receiver R decrypts the digital envelope using his RSA private key to obtain the DES symmetric key.**

Step 2: **Using the DES symmetric key obtained from step 1, the receiver decrypts the encrypted message to obtain the plain text message, digital signature and the digital certificate of the sender S.**

Step 3: **Receiver R then extracts the RSA public key of the sender S from the digital certificate.**

Step 4: **Using the RSA public key of the sender S, the encrypted message digest obtained from step 3 is decrypted to get the message digest.**

Step 5: **Receiver R then subjects the message again through the hash function SHA-1. A message digest is thus obtained. This computed message digest is then compared with the message digest obtained from step 4. If both of them are the same, the authenticity of the sender S is guaranteed.**

Figure 3 shows the encryption and decryption process.

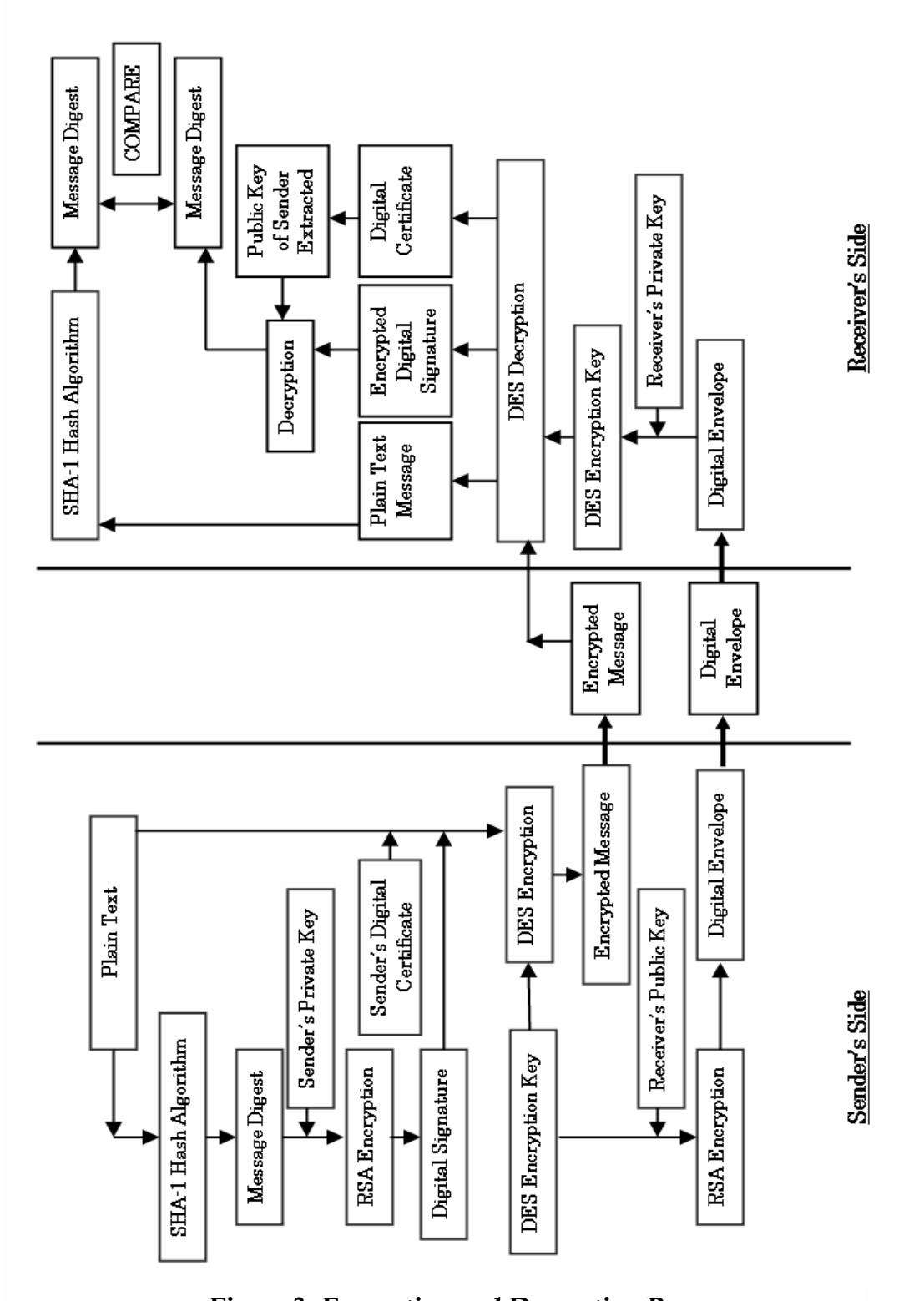

Figure 3: Encryption and Decryption Process

DUAL SIGNATURES

As mentioned earlier, in SET, the customer communicates with the merchant and the payment gateway through a single message. The message has two parts, a purchase order part for use by the merchant and a card information part for use by the merchant's bank

The customer has to ensure that

1. the merchant shall not view see the payment instruction
2. the acquirer shall not view the order instruction

It is also necessary to link the order and payment so that the customer can prove that the payment is for the particular order and not for other orders.

This is achieved by a new concept introduced in SET named as dual signature.

HOW ARE DUAL SIGNATURES CREATED?

The following steps explain how dual signatures are created.

Step 1: **Customer takes the Payment Information (PI) data and subjects the same through the hash function SHA-1. He gets Payment Information Message Digest (PIMD).**

Step 2: **Customer takes the Order Information (OI) data and subjects the same through the hash function SHA-1. He gets Order Information Message Digest (OIMD).**

Step 3: **Both PIMD and OIMD are concatenated.**

Step 4: **The concatenated output is again subjected through the hash function SHA-1. The output is called Payment Order Message Digest (POMD).**

Step 5: **POMD is encrypted using the RSA private key of the customer. The result is the dual signature.**

Figure 4 shows how dual signatures are created.

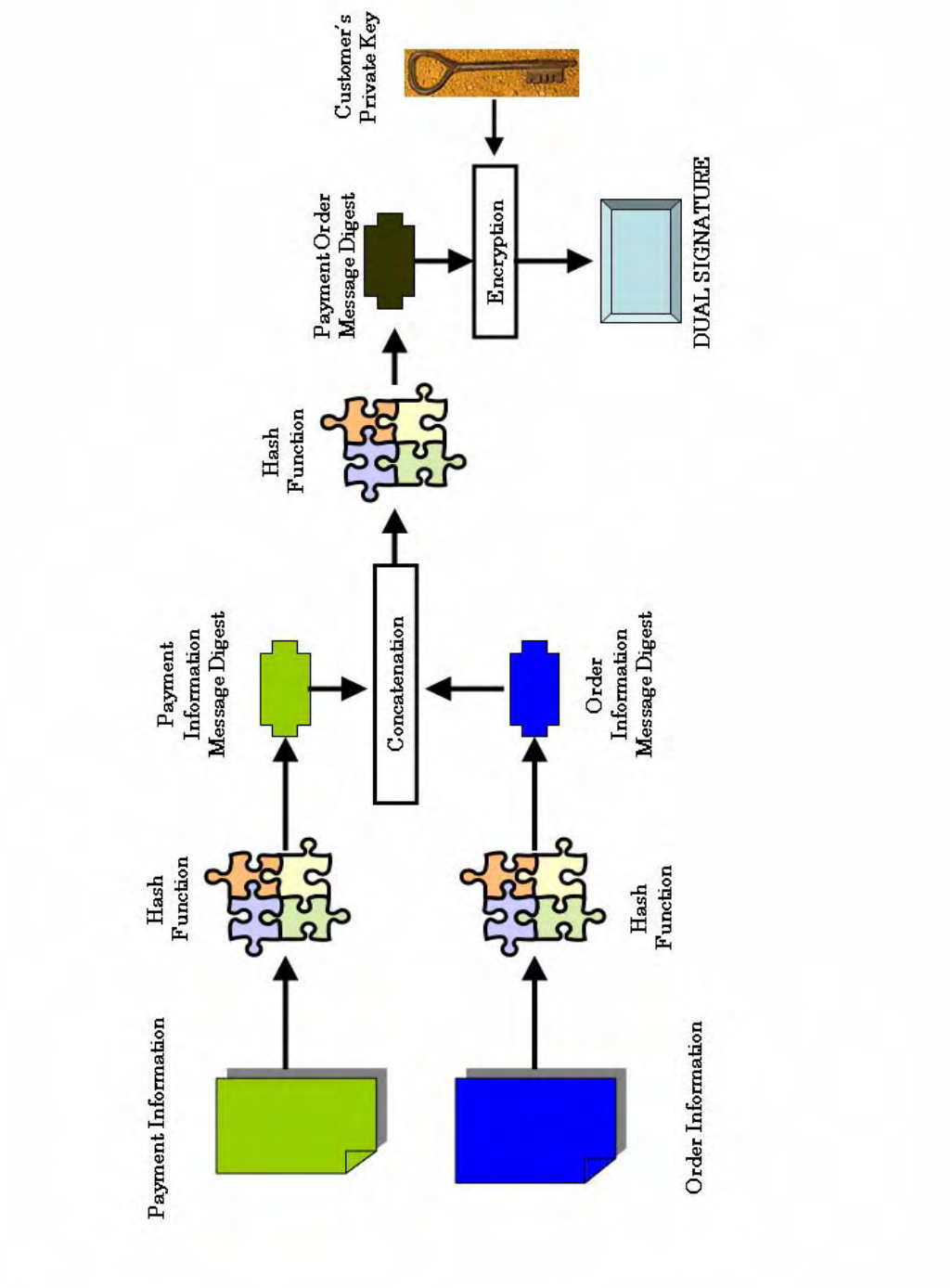

Figure 4: How Dual Signatures are created

HOW DUAL SIGNATURE HELPS THE BANK?

Here also, there are two steps, encryption process and decryption process.

Encryption process

Algorithms used: **1024 bit RSA algorithm for asymmetric encryption process**
56 bit DES algorithm for symmetric encryption process
SHA-1 for computing the message digest.

The sequence of steps the customer C adopts after the dual signature has been created:

Step 1: **The customer C creates a key for the DES symmetric encryption.**

Step 2: **The customer C then uses the DES encryption method to encrypt the Payment Instruction (PI) message, the dual signature, his certificate and the Order Information Message Digest (OIMD). The result is the encrypted message.**

Step 3: **The customer C then picks the RSA public key of the bank B. Encrypts the DES symmetric key of step 1. The output is called as digital envelope.**

The encrypted message obtained from step 2 and the digital envelope obtained from step 3 is sent to the bank B.

Decryption process

Algorithms used: **1024 bit RSA algorithm for asymmetric encryption process**
56 bit DES algorithm for symmetric encryption process
SHA-1 for computing the message digest.

The sequence of steps the bank B adopts after it has received the encrypted message and the digital envelope are:

Step 1: **The bank B uses its RSA private key to decrypt the digital envelope to obtain the DES symmetric key.**

Step 2: **The bank B then uses the DES symmetric key to decrypts the first portion of the encrypted message to obtain the Payment Instruction (PI) message, the dual signature, certificate of the customer and the Order Information Message Digest (OIMD).**

Step 3: **The bank B then subjects the Payment Instruction (PI) to the hash function SHA-1 to get the Payment Information Message Digest (PIMD).**

Step 4: **The bank concatenates the PIMD value and the OIMD and subjects the result again through the hash function SHA-1. The result is the Payment Order Message Digest (POMD).**

Step 5: **The bank then decrypts the second portion of the encrypted message which is the dual signature using the customer's public key (obtained from the digital certificate of the customer) and obtains a copy of the Payment Order Message Digest (POMD).**

Step 6: **The value of POMD obtained from steps 4 and 5 are compared. If they are same, then it is confirmed that the message has come from the customer.**

CERTIFICATES OF VARIOUS PARTICIPANTS

Certificates play a critical role in SET for trust is always built on certificates.

Since there are various participants in SET, each of them has their own certificates. Table 3 gives details on these certificates.

TABLE 3: PARTICIPANTS AND THEIR CERTIFICATE DETAILS

PARTICIPANT	CERTIFICATE DETAILS
Cardholder certificate	Used to verify that the cardholder is a genuine person. These are digitally signed by a financial institution and the certificate does not contain the account number and expiration date of the card
Merchant certificate	These are digitally signed by the merchant's financial institution and provide assurance that the merchant has a valid agreement with an acquirer. In SET, the merchant needs two public key pairs, one for digital signatures and one for encrypting key exchanges. It will therefore need two certificates for each payment card brand that it accepts.
Payment Gateway Certificate	Payment gateway obtains its certificates from their acquirers for the systems that process authorization.

HIERARCHY OF TRUST IN SET CERTIFICATES

As you might have noticed, all the participants of SET needs to have a certificate for operating.

Certificates are created by Certifying Authorities (CA) and there is a hierarchy of trust among the SET certificate authorities.

Figure 5 shows the hierarchy of trust among SET CA.

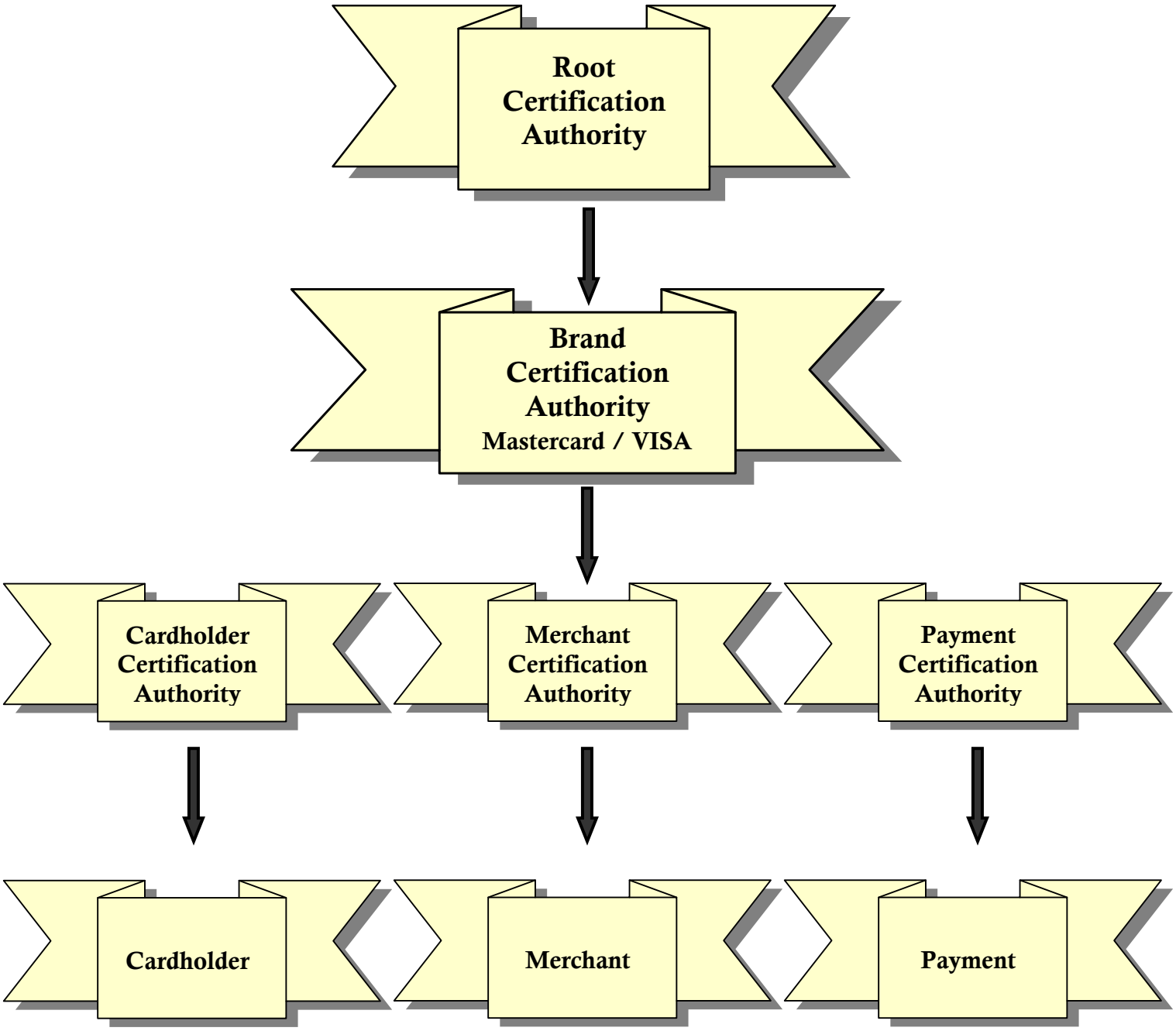

Figure 5: Hierarchy of trust among SET Certification Authorities.

LIMITATIONS OF SET

1. **Despite being very secure, SET has not been a success in e-commerce environments. The reasons attributed are:**

2. **The overheads associated with SET are heavy. For a simple purchase transaction:**
   a. **Four messages are exchanged between the merchant and customer,**
   b. **Two messages are exchanged between the merchant and payment gateway,**
   c. **6 digital signatures are computed,**
   d. **There are 9 RSA encryption/decryption cycles,**
   e. **There are 4 DES encryption/decryption cycles and**
   f. **Four certificate verifications**

3. **It has been argued by merchants that they have to expend lot of money in order to process SET transactions. From consumer's point of view, they have to install appropriate software.**

4. **Inter-operability problem has not been solved.**

5. **With SET, while the payment information is secure, order information is not secure.**