SET
for
E-commerce Transactions

Secure Electronic Transaction (SET)

- Protocol
- Protecting credit card transactions over the Internet
- It is an industry-backed standard
- Formed by MasterCard and Visa
- February 1996
- Advice and assistance provided by
  - IBM, GTE, Microsoft, Netscape, RSA, SAIC, Terisa and Verisign

SET

- Only Internet transaction protocol to provide **security through authentication**
- Ensure message **confidentiality and security**
- Relies on **cryptography and X.509** v3 digital certificates
- It **protects the transaction information** being altered in transit
  - by keeping information securely encrypted at all times
  - by using digital certificates to verify the identity of those accessing payment details

Secure Electronic Transaction (SET)

Business Requirements for SET

1. *Confidentiality of information*
2. *Integrity of data*
3. *Cardholder account authentication*
4. *Merchant authentication*
5. *Security techniques*
6. *Creation of brand-new protocol*
7. *Interoperability*

Secure Electronic Transaction (SET)

Business Requirements for SET

1. Confidentiality of information
   - Information
     - Payment
     - Order
   - Encryption provides confidentiality
   - Reduces the risk of fraud to the transaction
     - by either party
     - by malicious third parties
   - Cardholder account and payment information
     - should be secured as it travels across the network
     - should also prevent the merchant from learning the cardholder's credit card number
     - It is provided only to the issuing bank
   - Conventional encryption - DES is used

Secure Electronic Transaction (SET)

Business Requirements for SET

2. Integrity of data
   - Keep information securely encrypted at all times
     - Protect transaction information from being altered in transit
   - Digital signatures are used to ensure integrity
     - RSA digital signatures, using SHA-1 hash codes
     - HMAC using SHA-1

Secure Electronic Transaction (SET)

Business Requirements for SET

3.Cardholder account authentication

- Provide authentication that a **cardholder is a legitimate customer** of a branded payment card account
- **Merchants need** a way to verify that a cardholder is a legitimate user of a valid account number
  - Reduces the incidence of fraud and the overall cost of payment processing
- Digital signatures and certificates are used to ensure authentication of the cardholder account
  - X.509 v3 digital certificates with RSA signatures for this purpose

Secure Electronic Transaction (SET)

Business Requirements for SET

4. Merchant authentication
   - Provide authentication that a merchant can accept credit card transactions through its relationship with an acquiring financial institution
   - Merchants need to verifying
     - Cardholder is in possession of a valid payment card
     - Has the authority to be using that card
   - Cardholder to confirm
     - Authenticity of merchant
     - Merchant has a relationship with a financial institution (acquirer) allowing it to accept the payment card
   - Digital signatures and merchant certificates - ensure authentication of the merchant.
     - X.509 v3 digital certificates with RSA signatures

Secure Electronic Transaction (SET)

Business Requirements for SET

5. Security techniques
   - Best security practices and system design techniques - to protect all legitimate parties
   - Two asymmetric key pairs for
     - Encryption/decryption - Confidentiality
     - Creation and verification of digital signatures - Integrity and authentication
   - Utilises cryptography to provide
     - confidentiality of message information
     - ensure payment integrity
     - insure identity authentication
       - For authentication purposes, cardholders, merchants and acquirers will be issued with digital certificates by their sponsoring CAs
   - Highly secure cryptographic algorithms and protocols are used

Secure Electronic Transaction (SET)

Business Requirements for SET

6. Creation of brand-new protocol
   - Create a protocol that neither depends on transport security mechanisms nor prevents their use
   - SET is an end-to-end protocol
   - SET does not interfere with the use of other security mechanisms such as IPsec and SSL/TLS

Secure Electronic Transaction (SET)

Business Requirements for SET

7. Interoperability
   - Facilitate and encourage interoperability among software and network providers
   - SET uses specific protocols and message formats to provide interoperability
   - The specification must be applicable on a variety of hardware and software platforms and must not include a preference for one over another
   - Any cardholder with compliant software must be able to communicate with any merchant software that also meets the defined standard

SET

SET System Participants

- *Cardholder*
- *Issuer*
- *Merchant*
- *Acquirer*
- *Payment gateway*
- *Certification Authority*

SET

SET System Participants

1. Cardholder:
   - Authorised holder of a payment card that has been issued by an issuer
   - SET ensures that the payment card account information remains confidential
2. Issuer:
   - A bank
   - Financial institution that establishes an account for an cardholder and issues the payment card
   - The issuer guarantees payment for authorised transactions using the payment card

SET

- **SET System Participants**

3. Merchant:
   - A person or organisation that offers goods or services for sale to the cardholder
   - Goods or services are offered via a Website or by e-mail
   - With SET, the merchant can offer its cardholders secure electronic interactions
   - A merchant that accepts payment cards must have a relationship with an acquirer (a financial institution)

SET

- **SET System Participants**

4. Acquirer:
   - Financial institution that establishes an account with a merchant and processes payment card authorisation and payments
   - The acquirer provides authentication to the merchant that a given card account is active and that the proposed purchase does not exceed the credit limit
   - The acquirer also provides electronic transfer of payments to the merchant's account
   - Subsequently, the acquirer is reimbursed by the issuer over some sort of payment network for electronic funds transfer (EFT)

SET

- **SET System Participants**

5. Payment gateway:
   - Acts as the interface between a merchant and the acquirer
   - It carries out **payment authorisation services** for many card brands
   - A payment gateway is a device operated by the acquirer or a designated third party that processes merchant payment messages, including payment instructions from cardholders
   - The payment gateway functions as follows: it decrypts the encoded message, authenticates all participants in a transaction, and reformats the SET message into a format compliant with the merchant's point of sale system

SET

- **SET System Participants**

6. Certification Authority:
   - Entity that is trusted to issue X.509 v3 publickey certificates for cardholders, merchants and payment gateways
   - Receive registration requests, process and approve/decline requests
   - A financial institution may receive, process and approve certificate requests for its cardholders or merchants, and forward the information to the appropriate payment card brand(s) to issue the certificates

SET

- **SET System Participants**
- In the SET environment, there exists a hierarchy of Cas
- The SET protocol specifies a method of *trust chaining for entity authentication*
- *This trust chain method entails the exchange of digital* certificates and verification of the public keys by validating the digital signatures of the issuing CA

SET

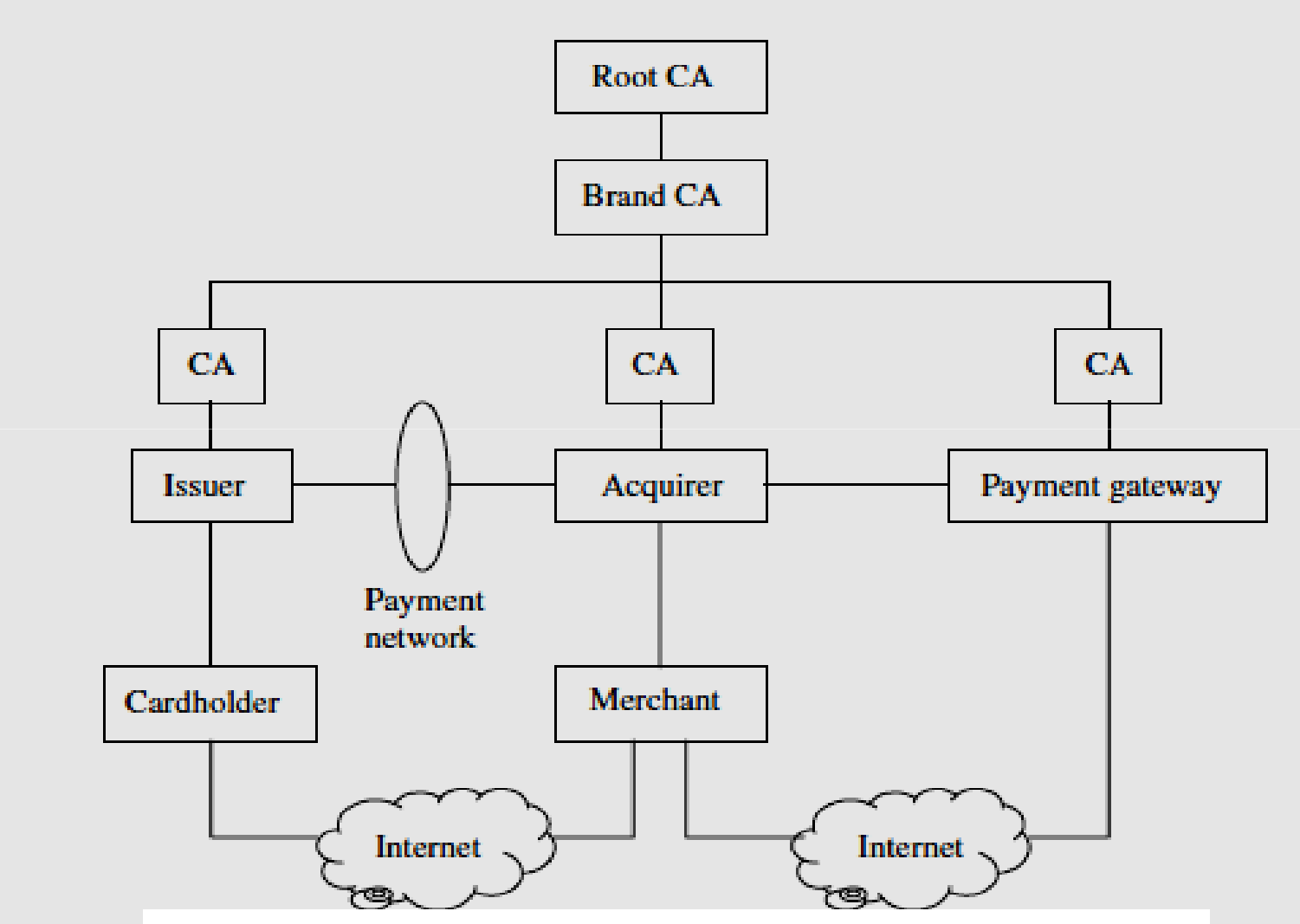
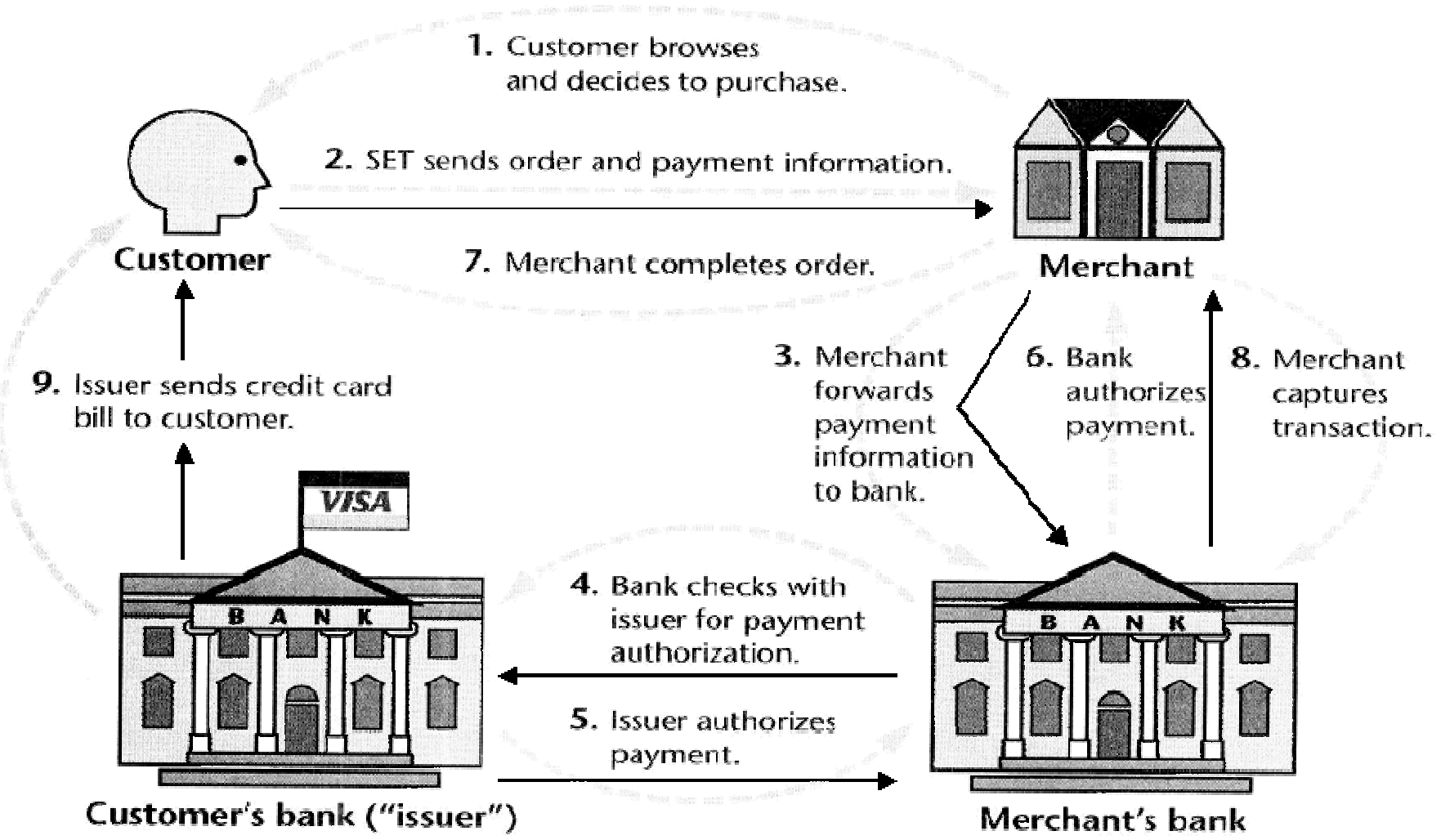


Figure 11.1 The SET hierarchy indicating the relationships between the participants.

SET Transactions



SET

- **Cryptographic Operation Principles**
  - Validate each participant's identity
  - Ensure
    1. Confidentiality
    2. Data integrity
    3. Authentication
  - Utilises cryptography

SET

- **Cryptographic Operation Principles**

  1.Confidentiality

  - Ensured by message encryption
  - Message data is encrypted with a random symmetric key which is further encrypted using the recipient's public key **$EM = E_{KPu}(E_{ks}(M))$**
  - The encrypted message along with this digital envelope is sent to the recipient
  - The recipient decrypts the digital envelope with a private key and then uses the symmetric key in order to recover the original message
  - **$M = D_{KPr}(D_{ks}(EM))$**

SET

- **Cryptographic Operation Principles**

  2.Integrity:

  - *Ensured by the use of a digital signature*
  - *Using the public/private key* pair
    - Sender encrypt a message using the sender's private key
    - Any recipient can determine that the message came from the sender by decrypting the message using the sender's public key
  - The merchant can be assured that
    - The 'order' it received is what the cardholder entered
    - Guarantees that the order information is not altered in transit

SET

- **Cryptographic Operation Principles**

  3.Authentication:

  - This is also ensured by means of a **digital signature**
  - It is further strengthened by the **use of a CA**
  - In business transactions each party wants to be sure that the other is authenticated
    - Before a user B accepts a message with a digital signature from a user A, B wants to be sure that the public key belongs to A

SET

- **Cryptographic Operation Principles**

  3. Authentication:

  - One way to **secure delivery of the key** is to utilise a CA to authenticate that the public key belongs to A
    - A CA is a trusted third party that issues digital certificates
    - CA **authenticates A** as well as offers a high **assurance of personal identity**
      - » This CA may require **A to confirm his or her identity** prior to issuing a certificate
      - » Once A has provided proof of his or her identity, the **CA creates a certificate containing** A's name and public key
      - » This certificate **is digitally signed** by the CA
      - » It contains the **CA's** identification **information**, as well as a copy of the CA's public key

SET

- **Cryptographic Operation Principles**

  3. Authentication:

  - For authentication purposes, cardholders, merchants and acquirers (financial institutions) will be issued with digital certificates by their sponsoring CAs
  - The certificates are digital documents attesting to the binding of a public key to an individual user
  - They allow verification of the claim that a given public key belong to a given individual user

SET

- **Dual Signature and Signature Verification**
  - SET introduced a new concept of digital signature called ***dual signatures***
  - *A dual signature is* generated by creating the message digest of two messages:
    - order digest
    - payment digest

SET

- **Dual Signature and Signature Verification**
  - The customer takes the hash codes (message digests) of both the order message (OM) and payment message (PM) by using the SHA-1 algorithm
  - These two hashes, ho and hp, are then concatenated and the hash code h of the result is taken
  - Finally, the customer encrypts (via RSA) the final hash code with his or her private key, Ksc, creating the dual signature

$$
\begin{aligned}
DS &= E_{K_{sc}}(h) \\
\text{where } h &= H(H(OM) \| H(PM)) \\
&= H(h_o \| h_p)
\end{aligned}
$$

$E_{K_{sc}} (= d_c)$ is the customer's private signature key.

SET • Dual Signature and Signature Verification

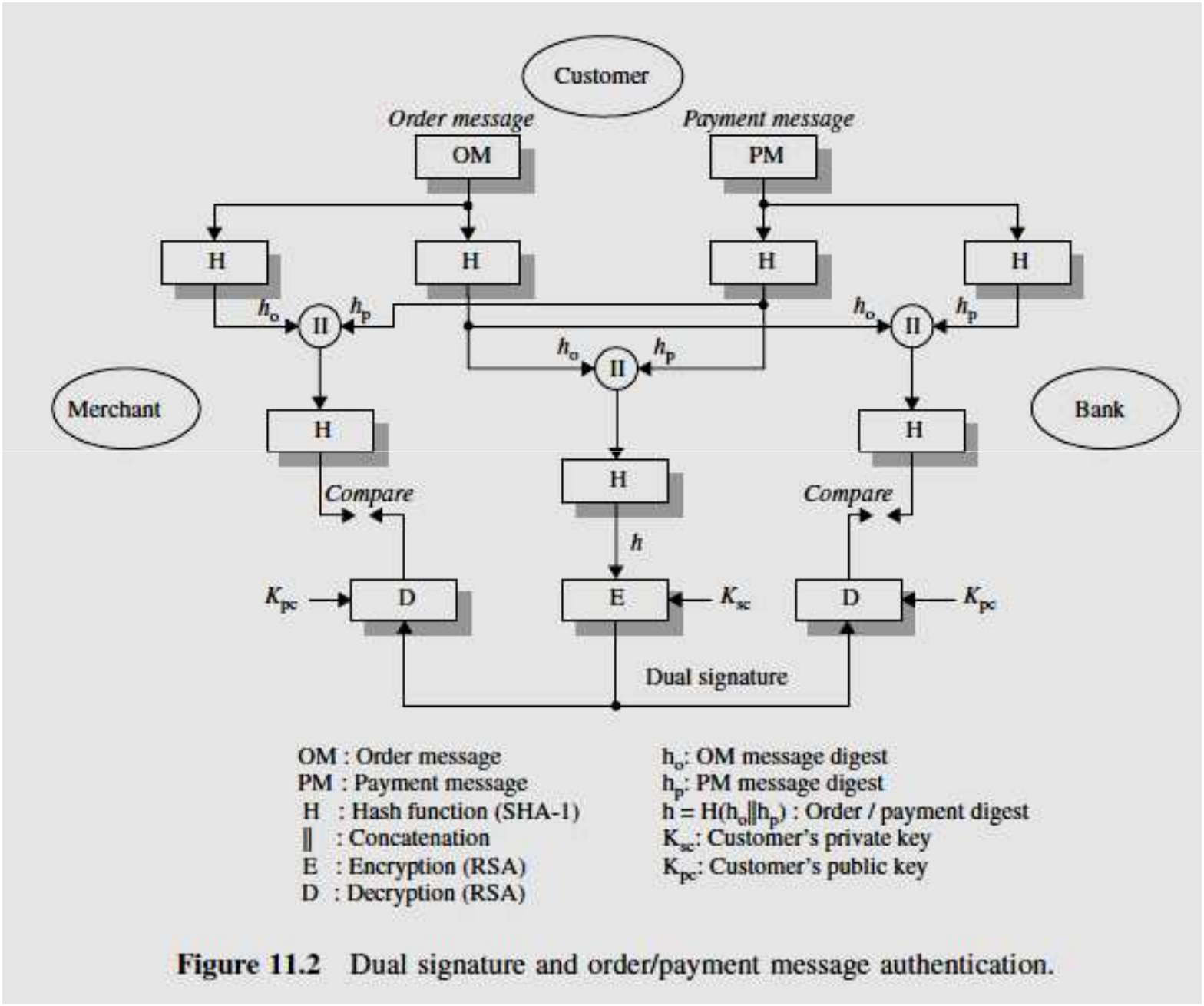


Figure 11.2 Dual signature and order/payment message authentication.

SET

- **Authentication and Message Integrity**

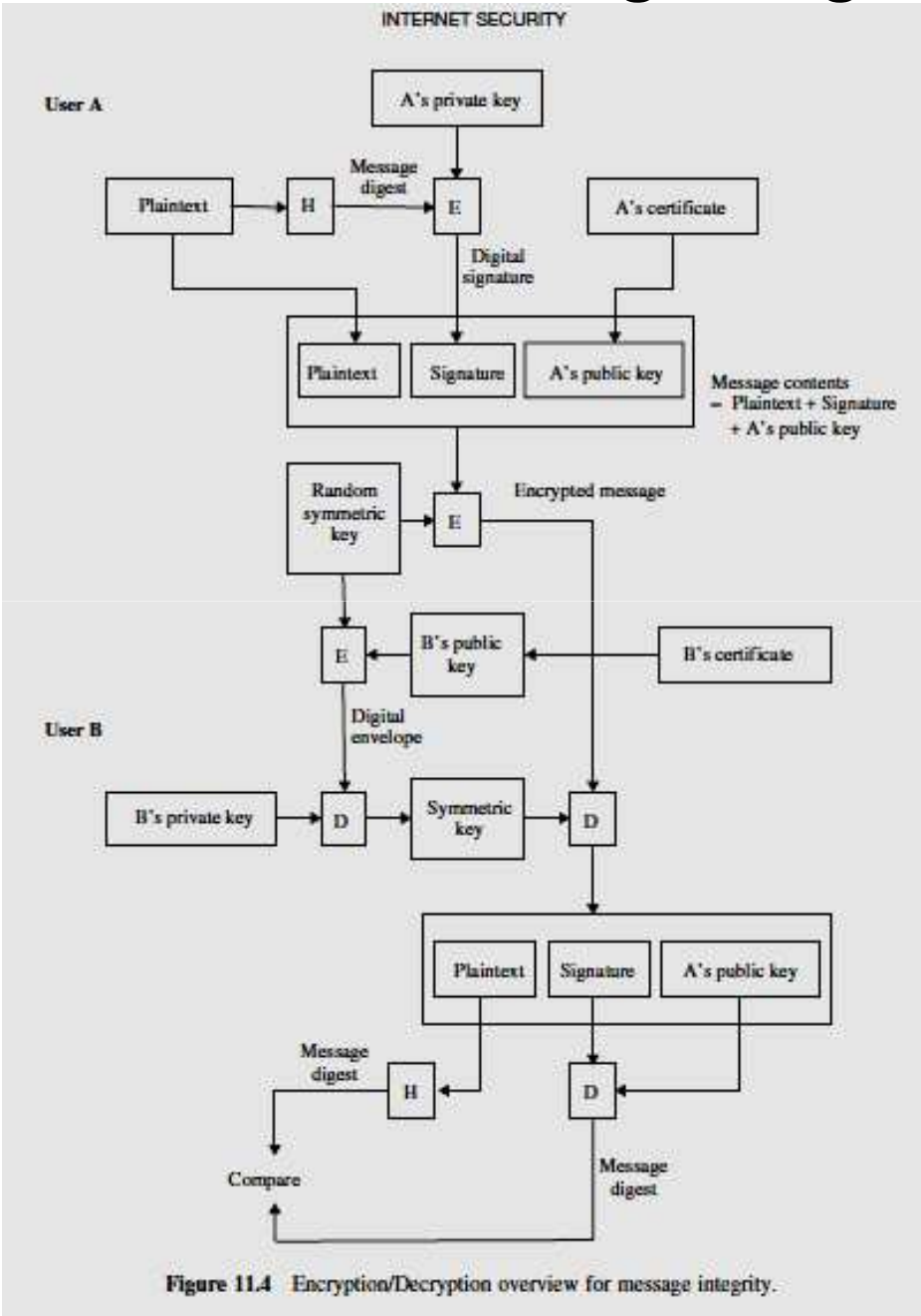


Figure 11.4 Encryption/Decryption overview for message integrity.

SET

- **Authentication and Message Integrity**

1. Encryption process:
   - User A sends the plaintext through a hash function to produce the message digest that is used later to test the message integrity.
   - A then encrypts the message digest with his or her private key to produce the digital signature.
   - Next, A generates a random symmetric key and uses it to encrypt the plaintext, A's signature and a copy of A's certificate, which contains A's public key. To decrypt the plaintext later, user B will require a secure copy of this temporary symmetric key.
   - B's certificate contains a copy of his or her public key. To ensure secure transmission of the symmetric key, A encrypts it using B's public key. The encrypted key, called the digital envelope, is sent to B along with the encrypted message itself.
   - A sends a message to B consisting of the DES-encrypted plaintext, signature and A's public key, and the RSA-encrypted digital envelope.

SET

- **Authentication and Message Integrity**

2. Decryption process:
   - B receives the encrypted message from A and decrypts the digital envelope with his or her private key to retrieve the symmetric key.
   - B uses the symmetric key to decrypt the encrypted message, consisting of the plaintext, A's signature and A's public key retrieved from A's certificate.
   - B decrypts A's digital signature with A's public key that is acquired from A's certificate. This recovers the original message digest of the plaintext.
   - B runs the plaintext through the same hash function used by A and produces a new message digest of the decrypted plaintext.
   - Finally, B compares his or her message digest to the one obtained from A's digital signature. If they are exactly the same, B confirms that the message content has not been altered during transmission and that it was signed using A's private key. If they are not the same, then the message either originated somewhere else or was altered after it was signed. In that case, B discards the message.

SET

- **Payment Processing**
  - Done Securely
    - Needs several transaction protocols
    - Utilize Cryptographic concepts

SET

- **Payment Processing**

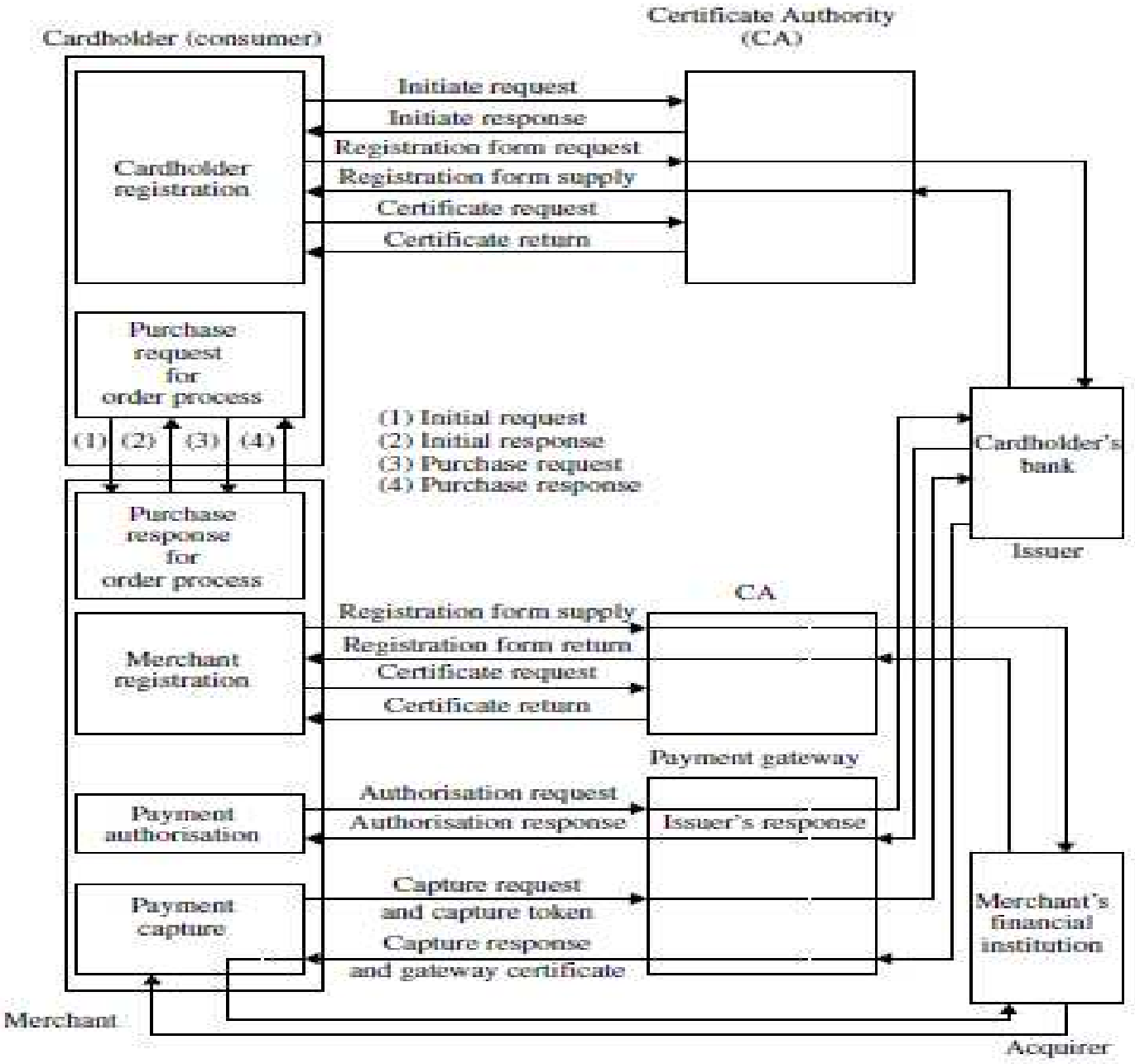


Figure 11.6 Overall picture of payment processing.

SET

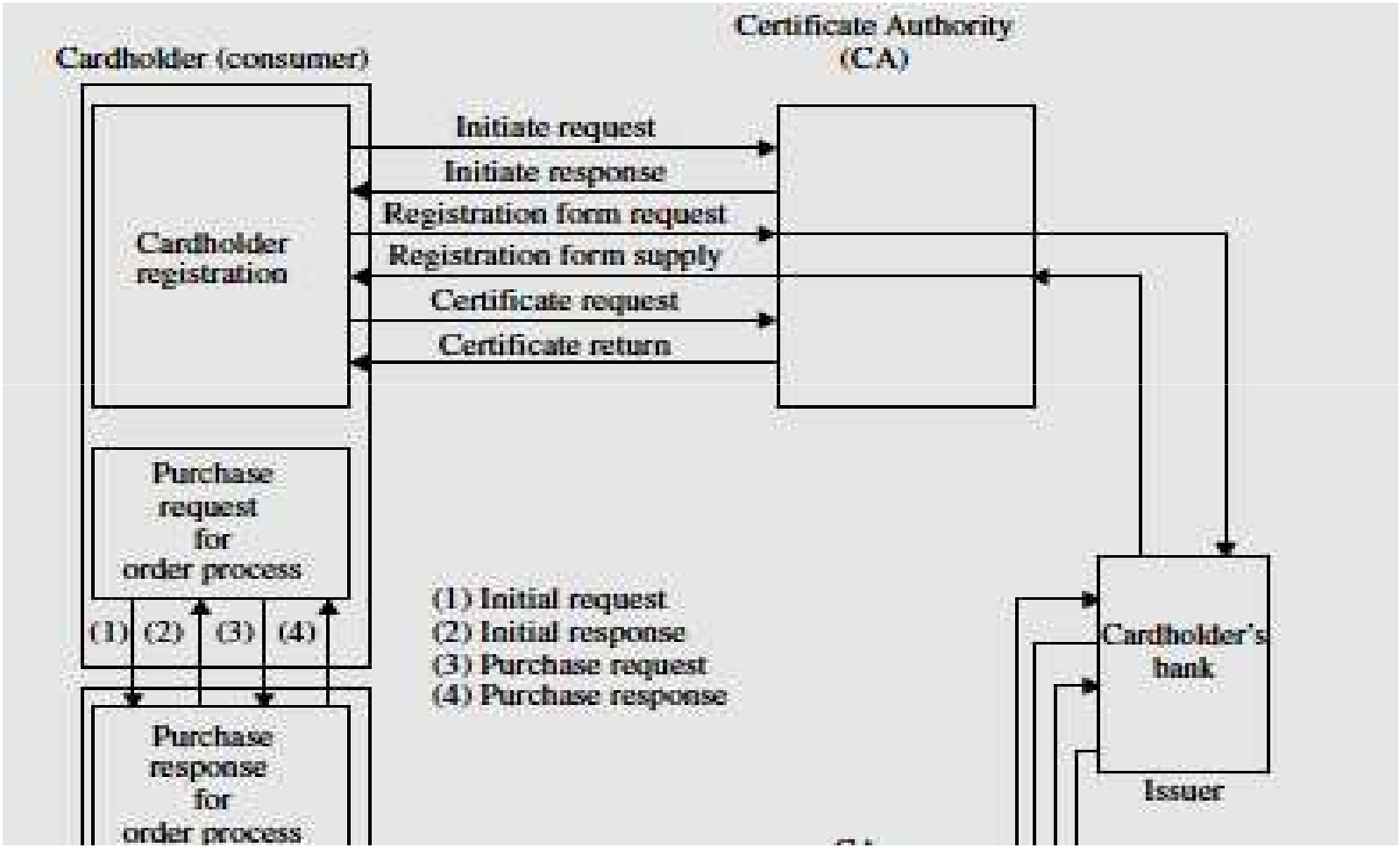
- **Payment Processing**
    1. Cardholder Registration
    2. Merchant Registration
    3. Purchase Request
    4. Payment Authorisation
    5. Payment Capture

SET

- **Payment Processing**
  1. Cardholder Registration
     - To send SET messages to the merchant
       - The cardholder **needs a public/private-key pair** for use with SET
       - The cardholder **must register** with a CA before
     - Scenario of cardholder registration
       a) Registration request/response processes
       b) Registration form process
       c) Certificate request/response processes

SET • **Payment Processing**

1. Cardholder Registration



SET

- **Payment Processing**
  1. Cardholder Registration
     a. Registration request/response processes:
        - Cardholder sends the *initiate request to the CA*
        - On receiving initiate request the CA generates the response and digitally signs it by generating a message digest of the response and encrypting it with the CA's private key
        - The CA sends the *initiate response along with the CA certificate to the cardholder*
        - The cardholder receives the initiate response and verifies the CA certificate by traversing the trust chain to the root key
        - The cardholder verifies the CA certificate by decrypting it with the CA's public key and comparing the result with a newly generated message digest of the initiate response

SET

- **Payment Processing**
  1.Cardholder
  a. RegistrationRegistration request/response processes:

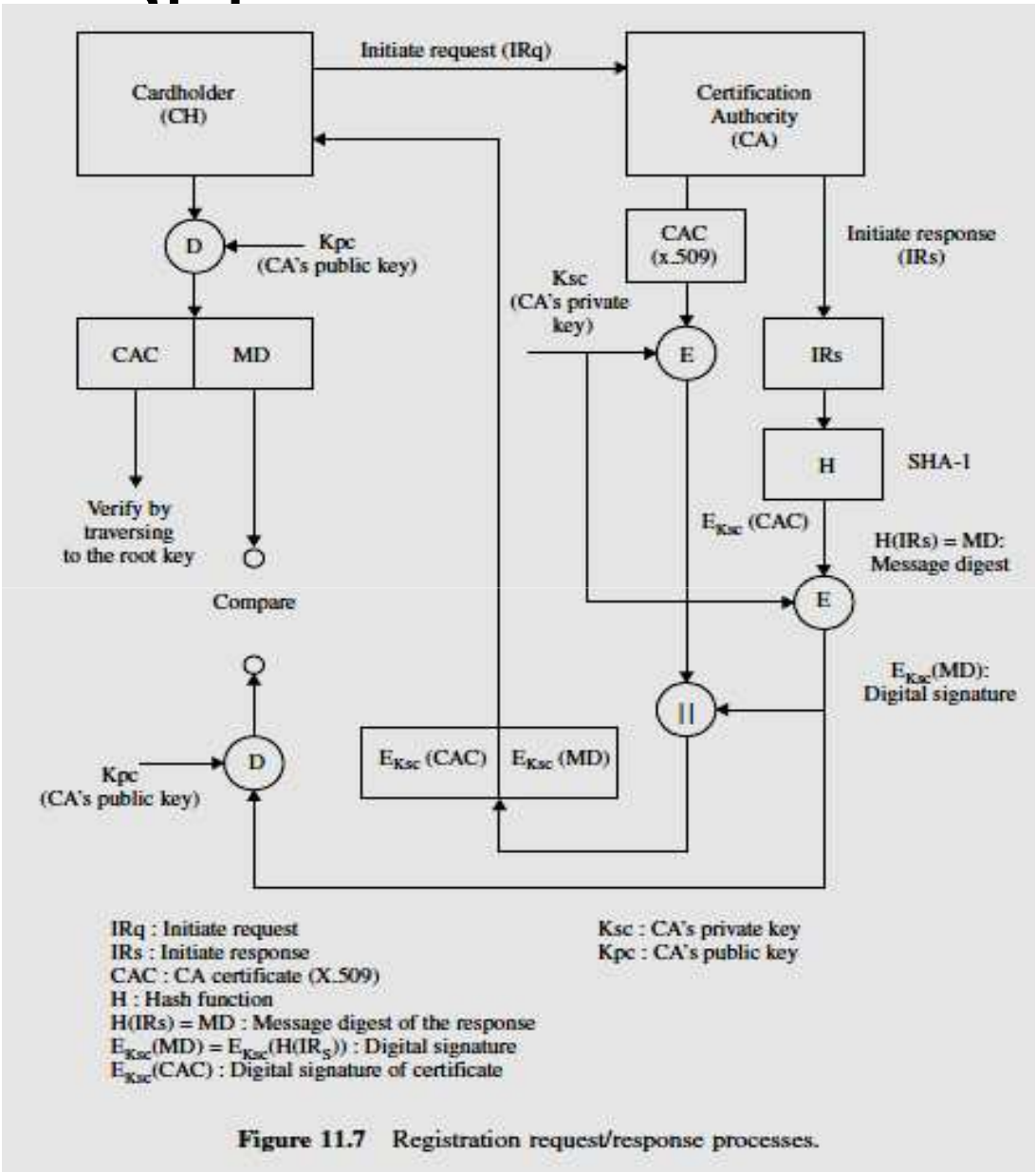


Figure 11.7 Registration request/response processes.

SET

- **Payment Processing**
  1. Cardholder Registration

     b. Registration form process:

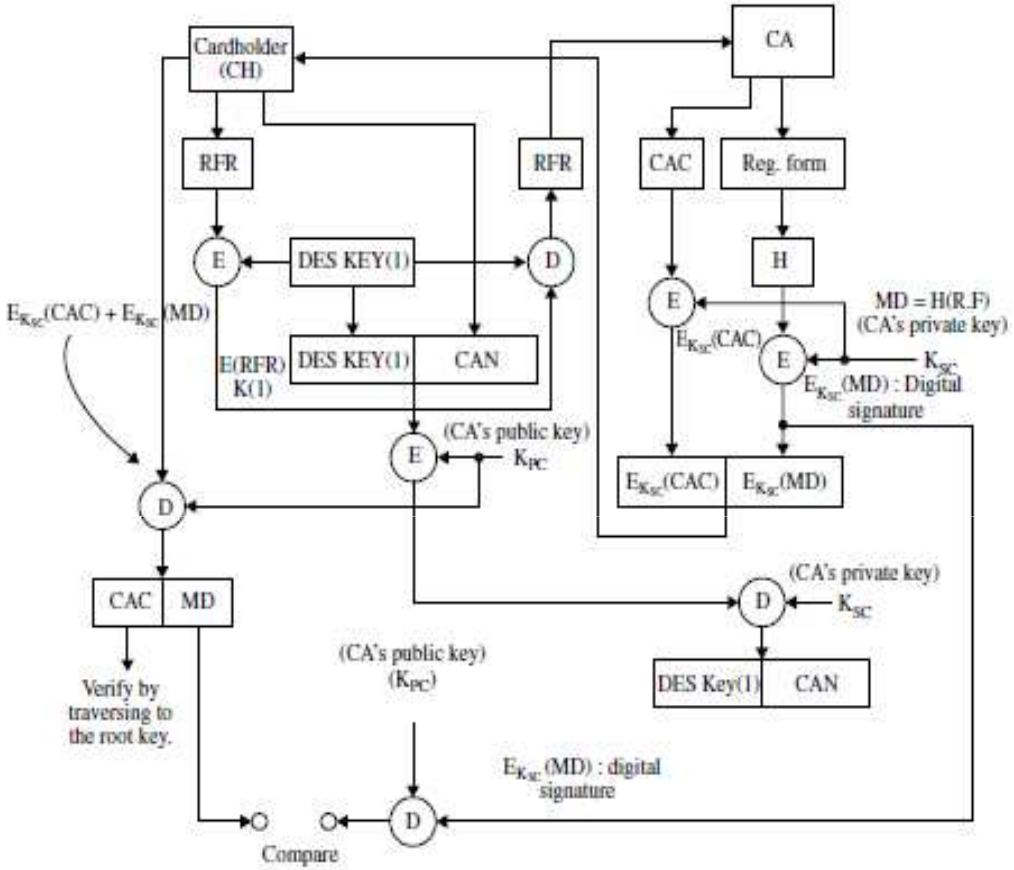
     - The cardholder generates the registration form request
     - The cardholder encrypts the SET message with a random symmetric key
     - This key, along with the cardholder's account number, is then encrypted with the CA's public key
     - The cardholder transmits the encrypted registration form request to the CA

SET

- **Payment Processing**
  1. Cardholder Registration
     b. Registration form process:

SET

- **Payment Processing**
  - Cardholder Registration
    b. Registration form process:



CAN : Cardholder's Account Number
RFR : Registration Form Request
K_{PC} : CA's public key
K_{SC} : CA's private key
MD : Message Digest
DES KEY(1) = Key(1)

Figure 11.8 Registration form process.

SET

- **Payment Processing**
  - Cardholder Registration

    c. Certificate request/response processes:

    - The cardholder generates the certificate request, including the information entered into the registration form.
    - The cardholder creates a message with request, the cardholder's public key and a newly generated symmetric key (No. 2), and digitally signs it by generating a message digest of the cardholder's private key.
    - The cardholder encrypts the message with a randomly generated symmetric key (No. 3). This symmetric key, along with the cardholder's account information, is then encrypted with the CA's public key.
    - The cardholder transmits the encrypted certificated request messages to the CA.
    - The CA decrypts the No. 3 symmetric key and cardholder's account information with the CA's private key, and then decrypts the certificate request using this symmetric key.
    - The CA verifies the cardholder's signature by decrypting it with the cardholder's public key and comparing the result with a newly generated message digest of the certificate requested.

SET

- **Payment Processing**
  - Cardholder Registration

    c. Certificate request/response processes:

    - The CA verifies the certificate request using the cardholder's account information and information from the registration form.
    - Upon verification the CA creates the cardholder certificate, digitally signing it with the CA's private key.
    - The CA generates the certificate response and digitally signs it by generating a message digest of the response and encrypting it with the CA's private key.
    - The CA encrypts the certificate response with the No. 2 symmetric key from the cardholder request.
    - The CA transmits the certificate response to the cardholder.
    - The cardholder verifies the certificate by traversing the trust chain to the root key.
    - The cardholder decrypts the response using the symmetric key (No. 2) saved from the cardholder request process.
    - The cardholder verifies the CA's signature by decrypting it with the CA's public key and comparing the result with a newly generated message digest of the response.
    - The cardholder stores the certificate and information from the response for future e-commerce use.

SET

- **Payment Processing**

2. Merchant Registration

- Merchants must register with a CA before they can receive SET payment instructions from cardholders
- In order to send SET messages to the CA, the merchant must have a copy of the CA's public key which is provided in the CA certificate
- The merchant also needs the registration form from the acquirer
- The merchant must identify the acquirer to the CA

SET

- **Payment Processing**

  2. Merchant Registration

  – The merchant registration process consists of five steps as follows:
    - The merchant requests the registration form
    - The CA processes this request and sends the registration form
    - The merchant requests certificates after receiving the registration certificates
    - The CA creates certificates
    - The merchant receives certificates

SET

- **Payment Processing**

  2. Merchant Registration

  a. Registration form process:

  - The merchant sends the initiate request of the registration form to the CA. To register, the merchant fills out the registration form with information such as the merchant's name, address and ID.
  - The CA receives the initiate request.
  - The CA selects an appropriate registration form and digitally signs it by generating a message digest of the registration form and encrypting it with the CA's private key.
  - The CA sends the registration form along with the CA certificate to the merchant.
  - The merchant receives the registration form and verifies the CA certificate by traversing the trust chain to the root key.
  - The merchant verifies the CA's signature by decrypting it with the CA's public key and comparing the result with a newly computed message digest of the registration form.
  - The merchant creates two public/private-key pairs for use with SET: key encryption and signature.

SET

- **Payment Processing**

2. Merchant Registration

b. Certificate request/create process:

- The merchant generates the certificate request.
- The merchant creates the message with request and both merchant public keys and digitally signs it by generating a message digest of the certificate request and encrypting it with the merchant's private key.
- The merchant encrypts the message with a random symmetric key (No. 1). This symmetric key, along with the merchant's account data, is then encrypted with the CA's public key.
- The merchant transmits the encrypted certificate request message to the CA.
- The CA decrypts the symmetric key (No. 1) and the merchant's account data with the CA's private key, and then decrypts the message using the symmetric key (No. 1).
- The CA verifies the merchant's signature by decrypting it with the merchant's public key and comparing the result with a newly computed message digest of the certificate request.

SET

- **Payment Processing**

2. Merchant Registration

b. Certificate request/create process:

- The CA confirms the certificate request using the merchant information.
- Upon verification, the CA creates the merchant certificate digitally signing the certificate with the CA's private key.
- The CA generates the certificate response and digitally signs it by generating a message digest of the response and encrypting it with the CA's private key.
- The CA transmits the certificate response to the merchant.
- The merchant receives the certificate response from the CA. The merchant decrypts the digital envelope to obtain the symmetric key. This key is used to decrypt the registration response containing the certificates.
- The merchant verifies the certificates by traversing the trust chain to the root key.
- The merchant verifies the CA's signature by decrypting it with the CA's public key and comparing the result with a newly computed message digest of the certificate response.
- The merchant stores the certificates and information from the response for use in future e-commerce transactions.

SET

- **Payment Processing**

3. Purchase Request

- Made after the cardholder has completed browsing, selecting and ordering
- Cardholder indicates which payment card brand will be used for the transaction
- The purchase request exchange consists of four messages:
  - initiate request
  - initiate response
  - purchase request
  - purchase response

SET

- **Payment Processing**

3. Purchase Request

a. Initiate request

- The cardholder sends the initiate request to the merchant.
- The merchant receives the initiate request.
- The merchant generates the response and digitally signs it by generating a message digest of the response and encrypting it with the merchant's private key.
- The merchant sends the response along with the merchant and payment gateway certificates to the cardholder.

SET

- **Payment Processing**

3. Purchase Request

b. Initiate response

- The cardholder receives the initiate response and verifies the certificates by traversing the trust chain to the root key.
- The cardholder verifies the merchant's signature by decrypting it with the merchant's public key and comparing the result with a newly computed message digest of the response.

- The cardholder creates the order message (OM) using information from the shopping phase and payment message (PM). At this step the cardholder completes payment instructions.

SET

- **Payment Processing**

3. Purchase Request

c. purchase request

- The cardholder generates a dual signature for the OM and PM by computing the message digests of both, concatenating the two digests, computing the message digest of the result and encrypting it using the cardholder's private key.
- The cardholder generates a random symmetric key (No. 1) and uses it to encrypts the PM. The cardholder then encrypts his or her account number as well as the random symmetric key used to encrypt the PM in a digital envelope using the payment gateway's key.
- The cardholder transmits the OM and the encrypted PM to the merchant.
- The merchant verifies the cardholder certificate by traversing the trust chain to the root key.
- The merchant verifies the cardholder's dual signature on the OM by decrypting it with the cardholder's public key and comparing the result with a newly computed message digest of the concatenation of the message digests of the OM and PM.
- The merchant processes the request, including forwarding the PM to the payment gateway for authorisation.

SET

- **Payment Processing**

3. Purchase Request

d. Purchase response:

- The merchant creates the purchase response including the merchant signature certificate and digitally signs it by generating a message digest of the purchase response and encrypting it with the merchant's private key.
- The merchant transmits the purchase response to the cardholder.
- If the transaction was authorised, the merchant fulfils the order to the cardholder.
- The cardholder verifies the merchant signature certificate by traversing the trust chain to the root key.
- The cardholder verifies the merchant's digital signature by decrypting it with the merchant's public key and comparing the result with a newly computed message digest of the purchase response.
- The cardholder stores the purchase response.

SET

- **Payment Processing**
  - **4. Payment Authorisation**
    - **a.** Authorisation request:

- The merchant creates the authorisation request.
- The merchant digitally signs an authorisation request by generating a message digest of the authorisation request and encrypting it with the merchant's private key.
- The merchant encrypts the authorisation request using a random symmetric key (No. 2), which in turn is encrypted with the payment gateway public key.
- The merchant transmits the encrypted authorisation request and the encrypted PM from the cardholder purchase request to the payment gateway.
- The gateway verifies the merchant certificate by traversing the trust chain to the root key.

SET

- **Payment Processing**

4. Payment Authorisation

a. Authorisation request:

- The payment gateway decrypts the digital envelope of the authorisation request to obtain the symmetric encryption key (No. 2) with the gateway private key. The gateway then decrypts the authorisation request using the symmetric key (No. 2).
- The gateway verifies the merchant's digital signature by decrypting it with the merchant's public key and comparing the result with a newly computed message digest of the authorisation request.
- The gateway verifies the cardholder's certificate by traversing the trust chain to the root key.
- The gateway decrypts the symmetric key (No. 1) and the cardholder account information with the gateway private key. It uses the symmetric key to decrypt the PM.
- The gateway verifies the cardholder's dual signature on the PM by decrypting it with the cardholder's public key and comparing the result with a newly computed message digest of the concatenation of the message digest of the OM and the PM.
- The gateway ensures consistency between the merchant's authorisation request and the cardholder's PM.
- The gateway sends the authorisation request through a financial network to the cardholder's financial institution (issuer).

SET

- **Payment Processing**

4. Payment Authorisation

b. Authorisation response:

- The gateway creates the authorisation response message and digitally signs it by generating a message digest of the authorisation response and encrypting it with the gateway's private key.
- The gateway encrypts the authorisation response with a new randomly generated symmetric key (No. 3). This key is then encrypted with the merchant's public key.
- The gateway creates the capture token and digitally signs it by generating a message digest of the capture token and encrypting it with the gateway's private key.
- The gateway encrypts the capture token with a new symmetric key (No. 4). This key and the cardholder account information are then encrypted with the gateway's public key.
- The gateway transmits the encrypted authorisation response to the merchant.
- The merchant verifies the gateway certificate by traversing the trust chain to the root key.
- The merchant decrypts the symmetric key (No. 3) with the merchant's private key and then decrypts the authorisation response using the symmetric key (No. 3).

SET

- **Payment Processing**

4. Payment Authorisation

b. Authorisation response:

- The merchant verifies the gateway's digital signature by decrypting it with the gateway's public key and comparing the result with a newly computed message digest of the authorisation response.
- The merchant stores the encrypted capture token and envelope for later capture processing.

- The merchant then completes processing of the purchase request and the cardholder's order by shipping the goods or performing the services indicated in the order.

SET

- **Payment Processing**

5. Payment Capture

a. Capture request:

- The merchant creates the capture request.
- The merchant embeds the merchant certificate in the capture request and digitally signs it by generating a message digest of the capture request and encrypting it with the merchant's private key.
- The merchant encrypts the capture request with a randomly generated symmetric key (No. 5). This key is then encrypted with the payment gateway's public key.
- The merchant transmits the encrypted capture request and encrypted capture token previously stored from the authorisation response to the payment gateway.
- The gateway verifies the merchant certificate by traversing the trust chain to the root key.
- The gateway decrypts the symmetric key (No. 5) with the gateway's private key and then decrypts the capture request using the symmetric key (No. 5).
- The gateway verifies the merchant's digital signature by decrypting it with the merchant's public key and comparing the result with a newly computed message digest of the capture request.
- The gateway decrypts the symmetric key (No. 4) with the gateway's private key and then decrypts the capture token using the symmetric key (No. 4).
- The gateway ensures consistency between the merchant's capture request and the capture token.
- The gateway sends the capture request through a financial network to the card-holder's issuer (financial institution).

SET

- **Payment Processing**

5. Payment Capture

b. Capture response:

- The gateway creates the capture response message, including the gateway signature certificate, and digitally signs it by generating a message digest of the capture response and encrypting it with the gateway's private key.
- The gateway encrypts the capture response with a newly generated symmetric key (No. 6). This key is then encrypted with the merchant's public key.
- The gateway transmits the encrypted capture response to the merchant.
- The merchant verifies the gateway certificate by traversing the trust chain to the root key.
- The merchant decrypts the symmetric key (No. 6) with the merchant's private key and then decrypts the capture response using the symmetric key (No. 6).
- The merchant verifies the gateway's digital signature by decrypting it with the gateway's public key and comparing the result with a newly generated message digest of the capture response.

SET

- **Payment Processing**

  5. Payment Capture

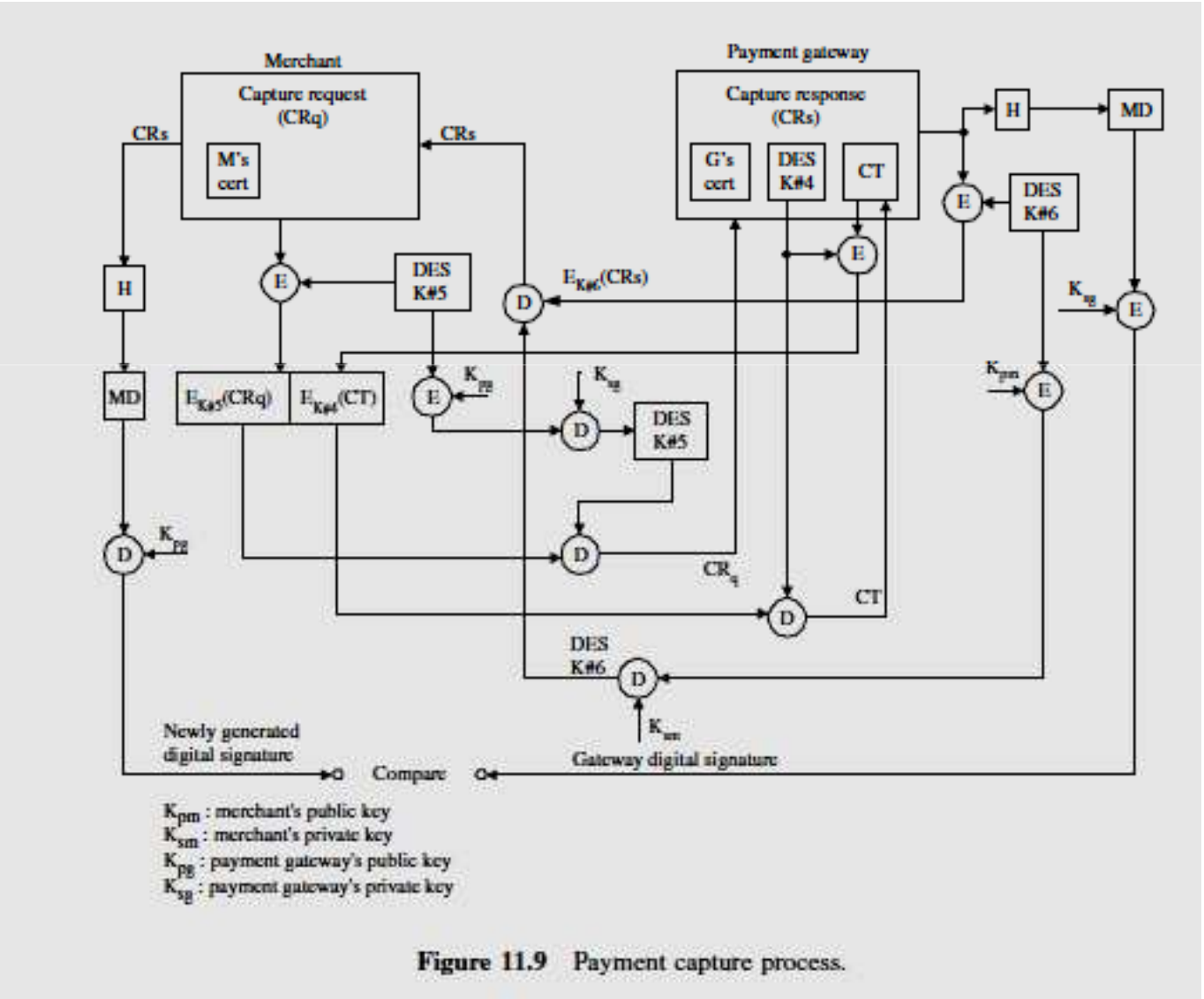


Figure 11.9 Payment capture process.