SET
for
E-commerce Transactions

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*

SET

SET System Participants

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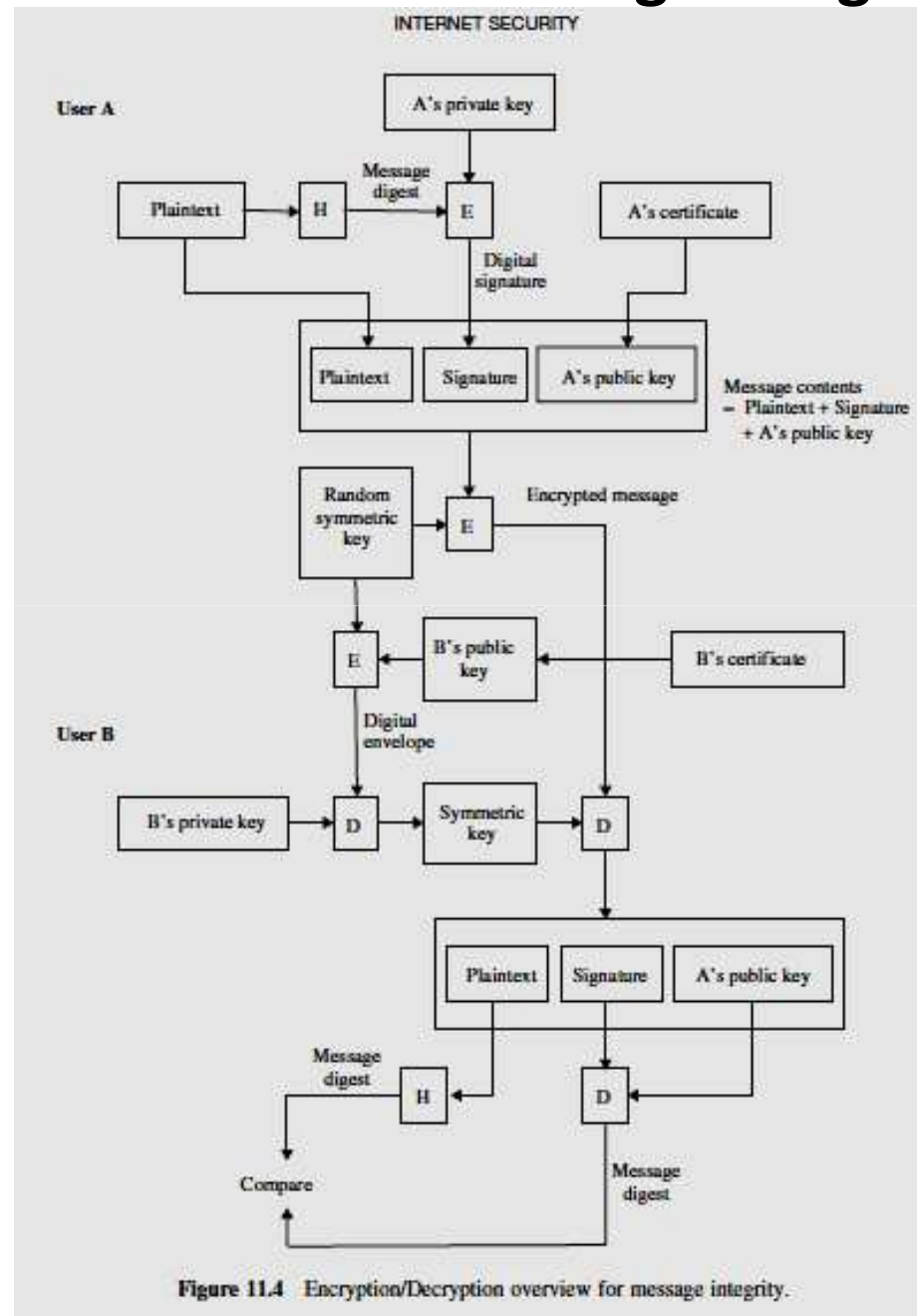- *Certification Authority*

SET

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

SET • Dual Signature and Signature Verification

Figure 11.2 Dual signature and order/payment message authentication.
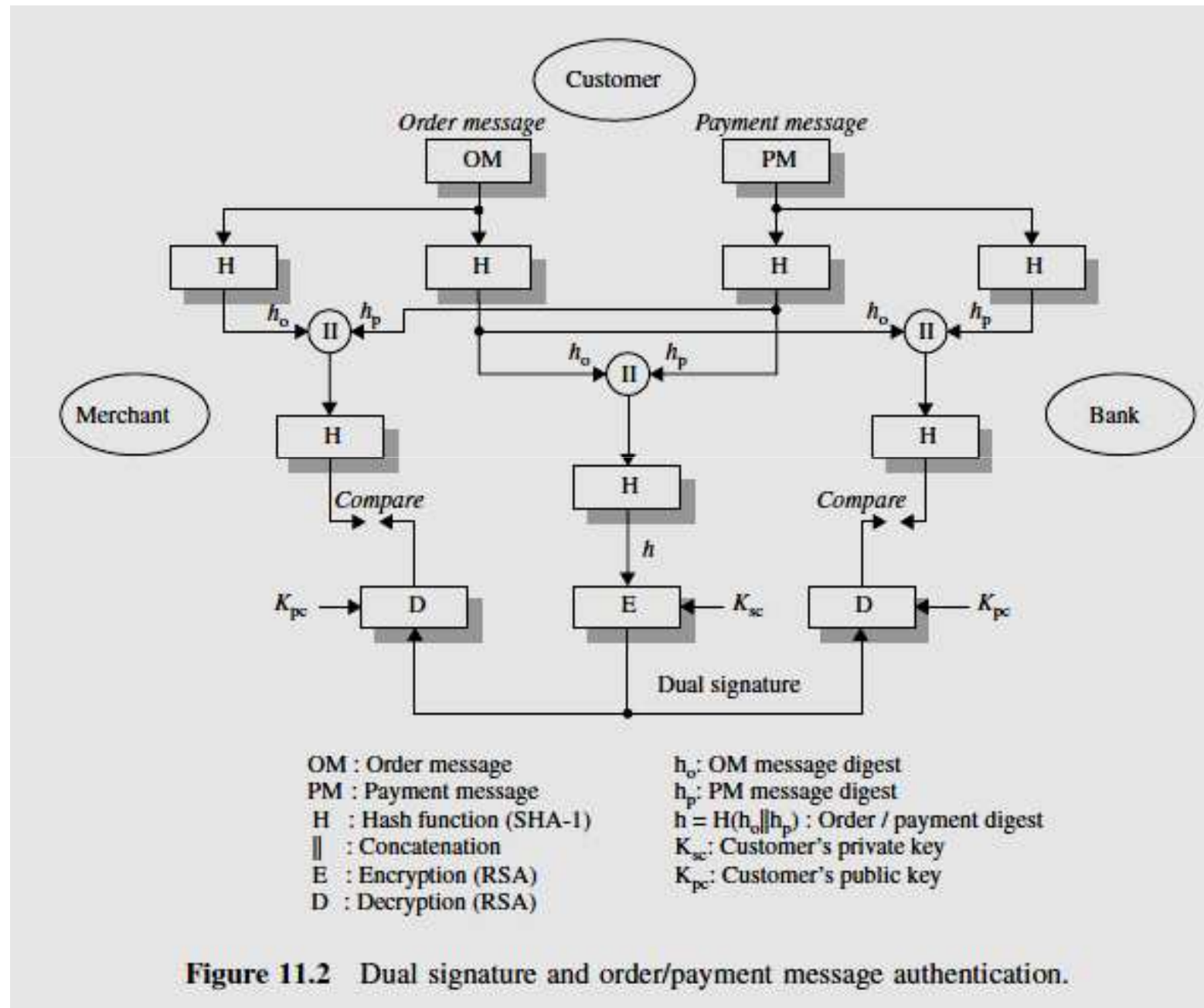
SET

- **Authentication and Message Integrity**

Figure 11.4 Encryption/Decryption overview for message integrity.
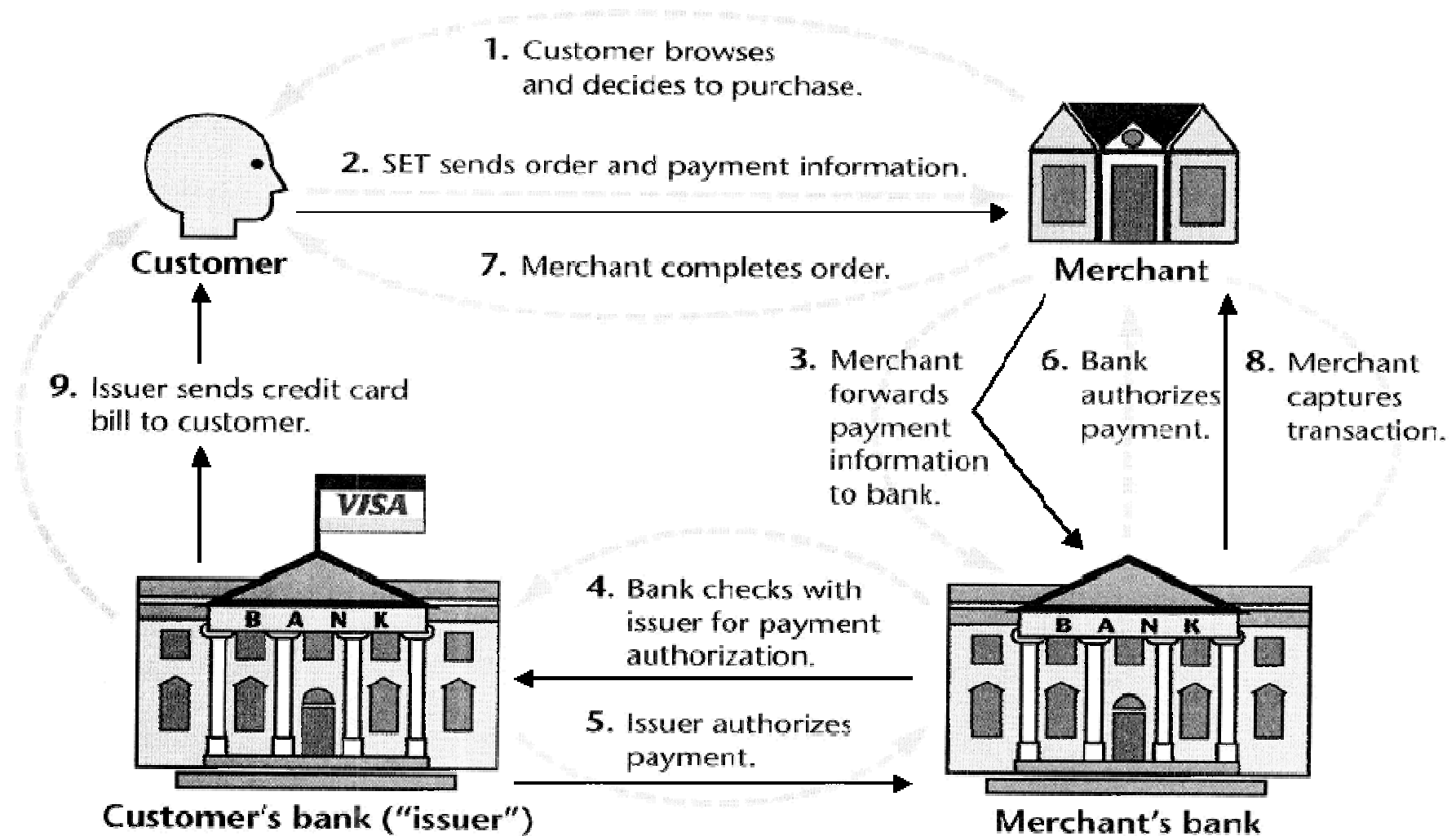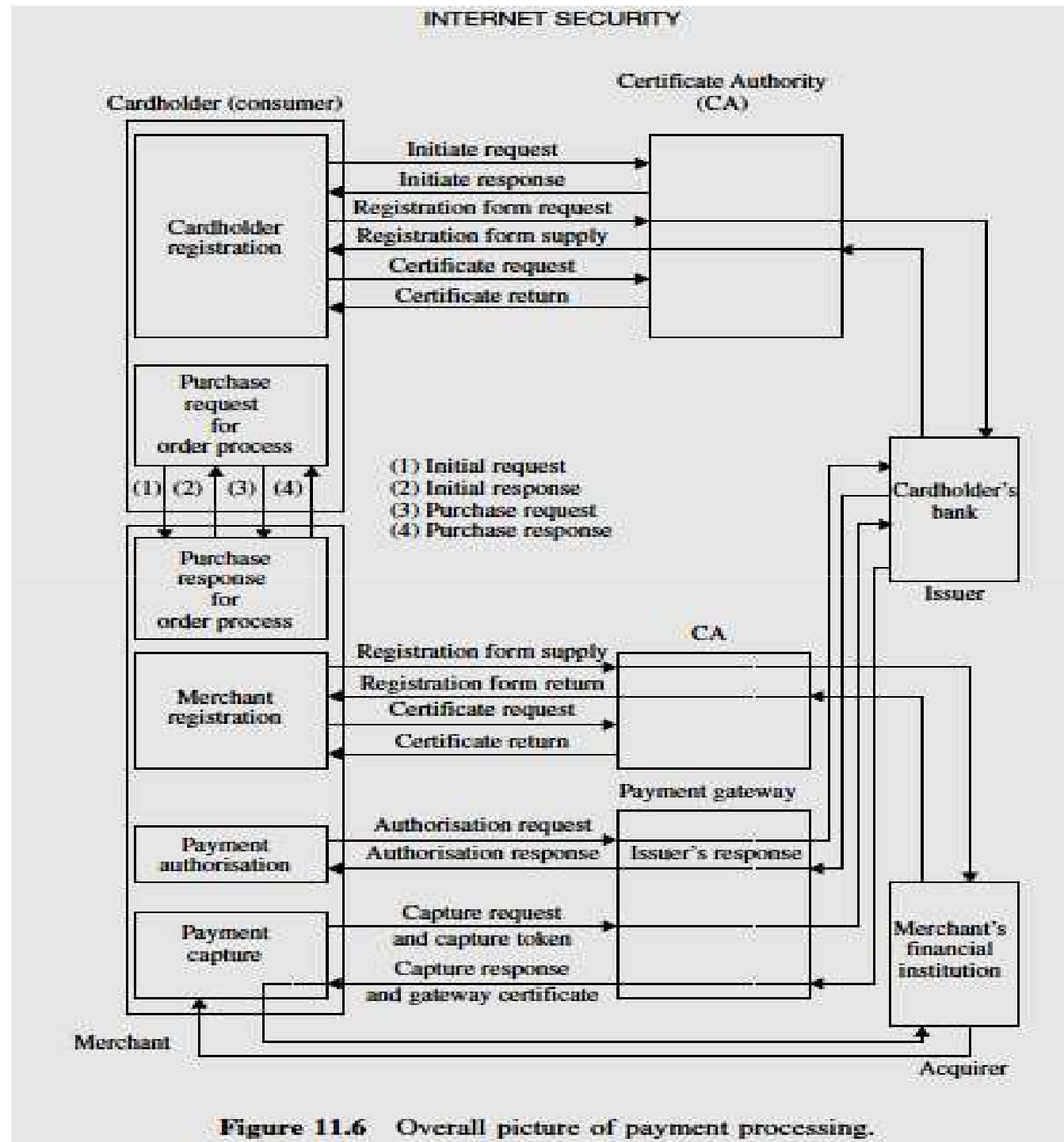
SET

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

SET Transactions

1. Customer browses and decides to purchase.

2. SET sends order and payment information.

7. Merchant completes order.

Customer

Merchant

9. Issuer sends credit card bill to customer.

3. Merchant forwards payment information to bank.

6. Bank authorizes payment.

8. Merchant captures transaction.

VISA

BANK

4. Bank checks with issuer for payment authorization.

5. Issuer authorizes payment.

Customer's bank ("issuer")

Merchant's bank

SET

- **Payment Processing**

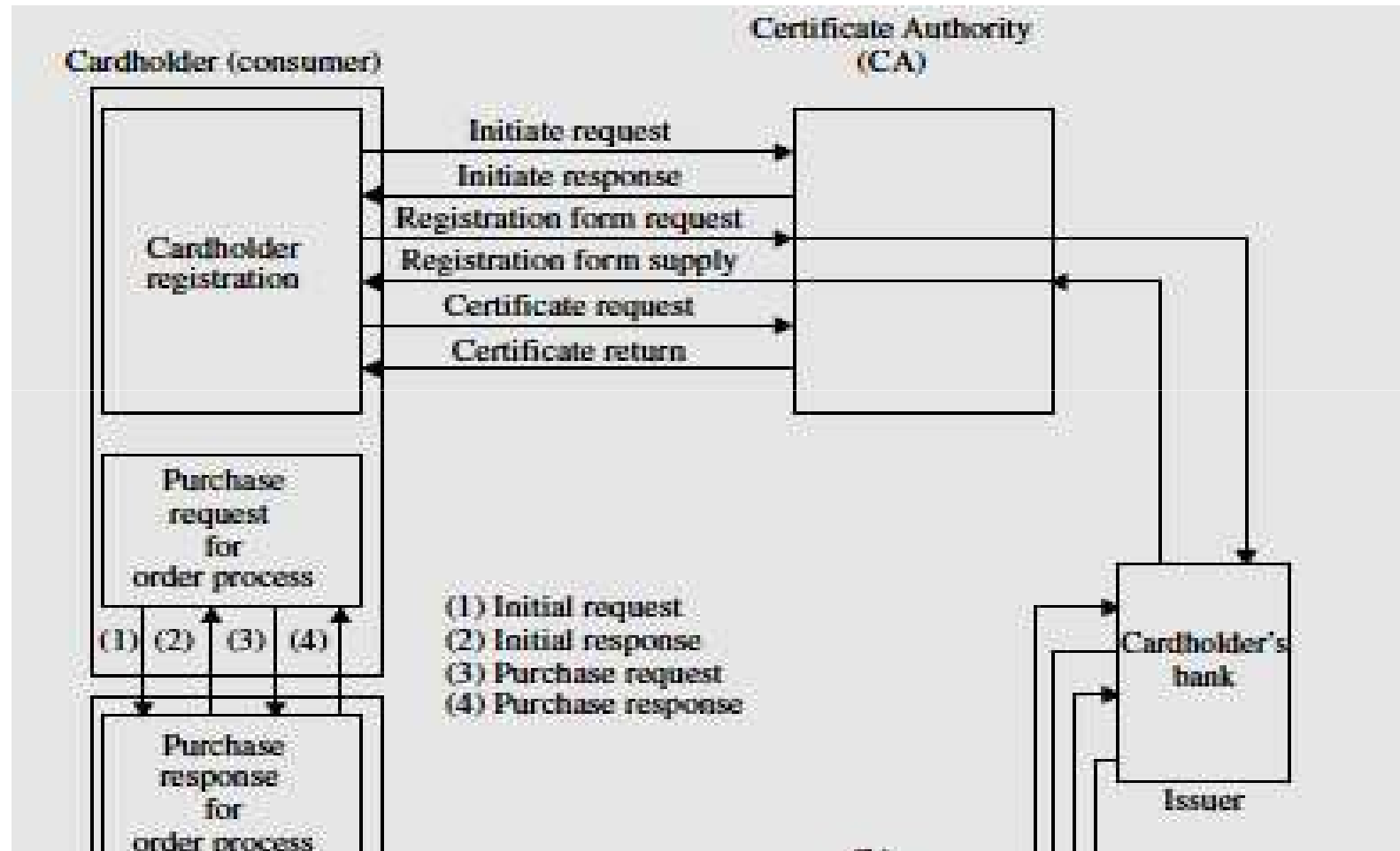**Figure 11.6** Overall picture of payment processing.

SET

- **Payment Processing**
  - Cardholder Registration
  - Merchant Registration
  - Purchase Request
  - Payment Authorisation
  - Payment Capture

SET

- **Payment Processing**
  - **Cardholder Registration**
    - Scenario of cardholder registration
      - Registration request/response processes
      - Registration form process
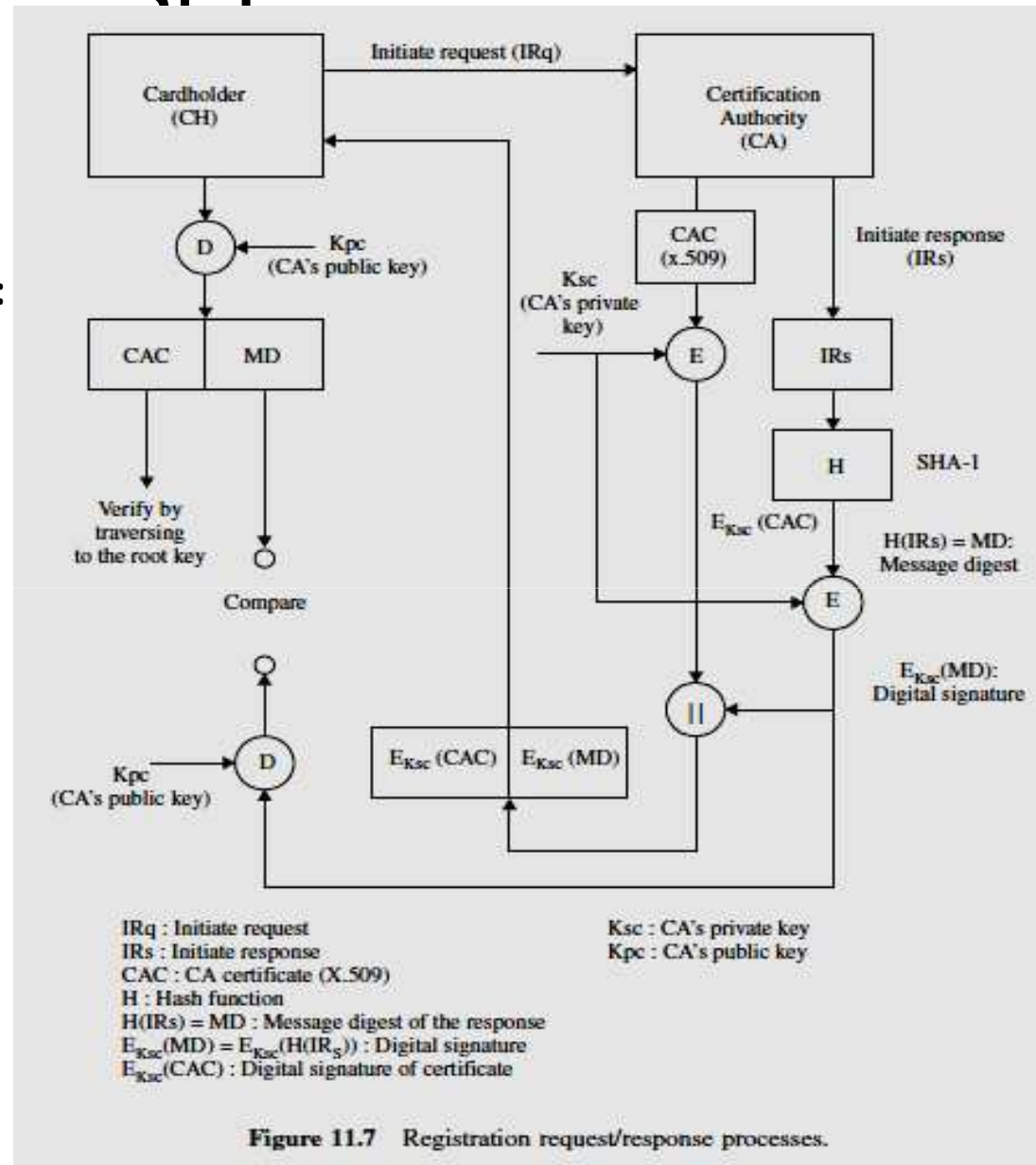   - Certificate request/response processes

SET

- **Payment Processing**
  - **Cardholder Registration**

Cardholder (consumer)

Certificate Authority (CA)

Cardholder registration

Initiate request
Initiate response
Registration form request
Registration form supply
Certificate request
Certificate return

Purchase request for order process

(1) (2) (3) (4)

(1) Initial request
(2) Initial response
(3) Purchase request
(4) Purchase response

Purchase response for order process

Cardholder's bank

Issuer

SET

- **Payment Processing**
  - **Cardholder Registration**
- **Registration request/response processes:**

IRq : Initiate request
IRs : Initiate response
CAC : CA certificate (X.509)
H : Hash function
H(IRs) = MD : Message digest of the response
$E_{Ksc}(MD) = E_{Ksc}(H(IR_S))$: Digital signature
$E_{Ksc}(CAC)$: Digital signature of certificate

Ksc : CA's private key
Kpc : CA's public key

Figure 11.7 Registration request/response processes.

SET

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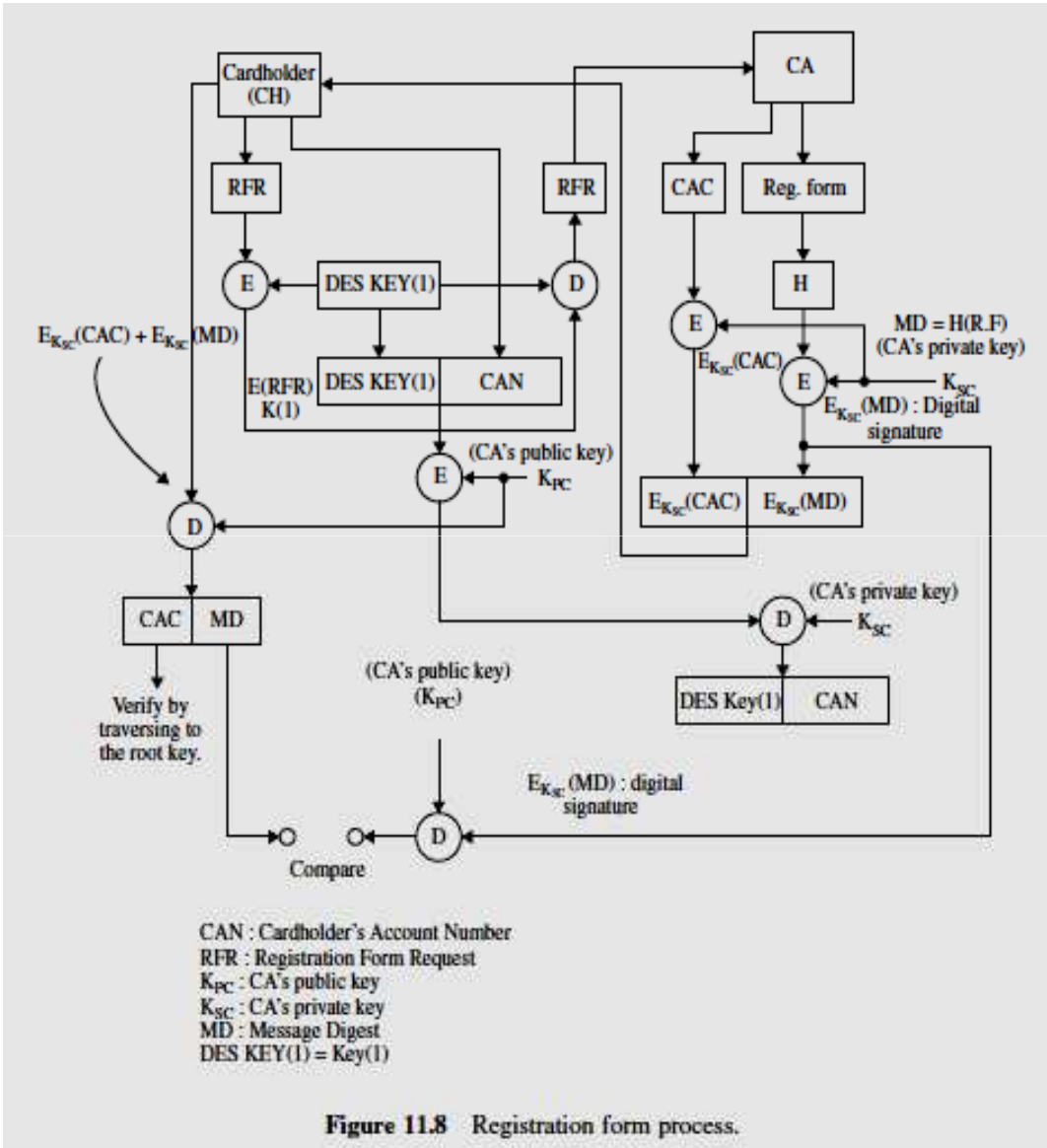- **2. Registration form process:**

Figure 11.8 Registration form process.

SET

- **Payment Processing**
  - **Merchant Registration**
    - Registration form process
    - Certificate request/create process

    The merchant registration process consists of five steps as follows:

    (1) The merchant requests the registration form

    (2) the CA processes this request and sends the registration form;

    (3) the merchant requests certificates after receiving the registration certificates;

    (4) the CA creates certificates;

    (5) the merchant receives certificates.

SET

- **Payment Processing**
  - **Purchase Request**
    - The purchase request exchange consists of four messages:
      - Initiate request
      - Initiate response
      - Purchase request
      - Purchase response
  - **Payment Authorisation**
      - Authorization request
      - Authorization response
  - **Payment Capture**
      - Capture request
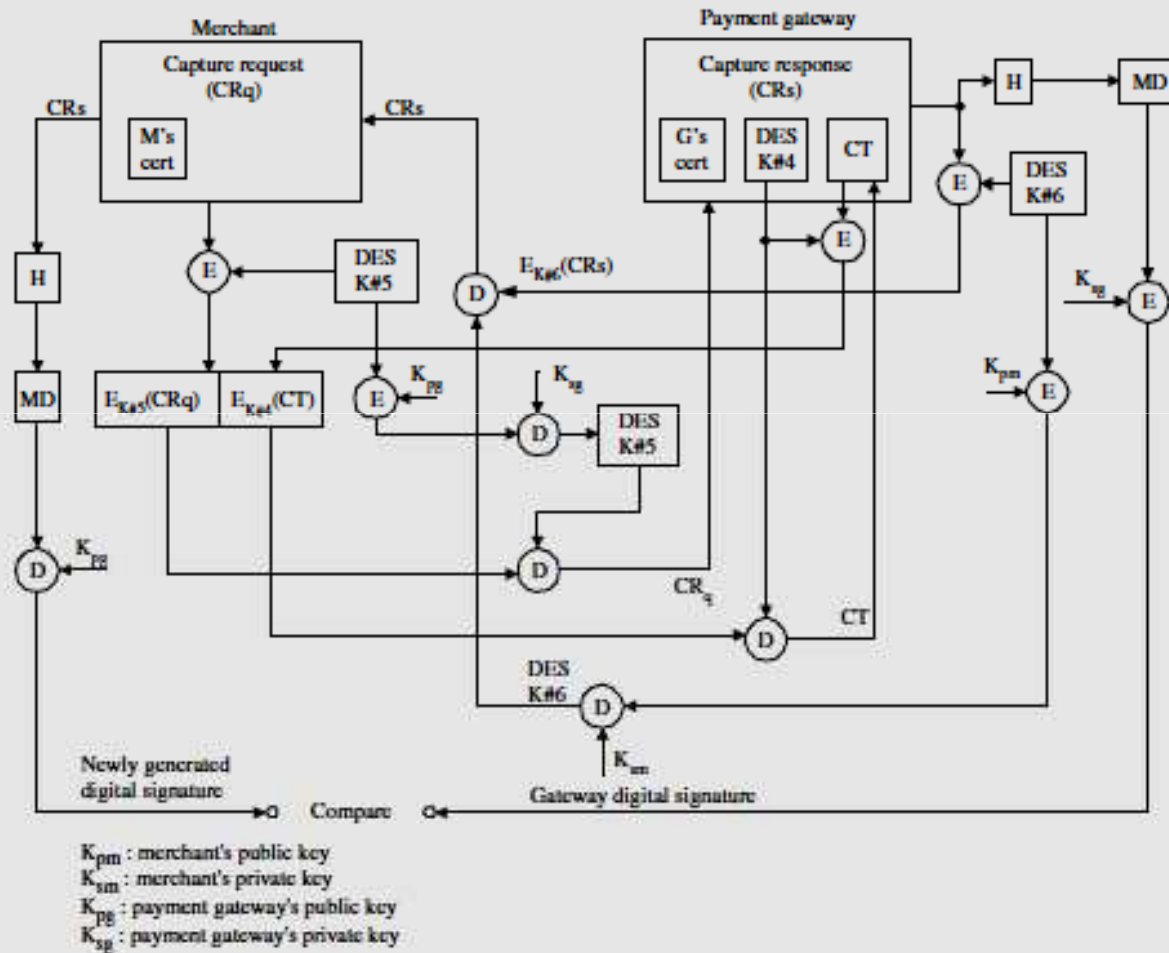   - Capture response

SET

Figure 11.9 Payment capture process.