Unit 4

Secure Electronic Transaction

SET

Secure Electronic Transaction (SET)

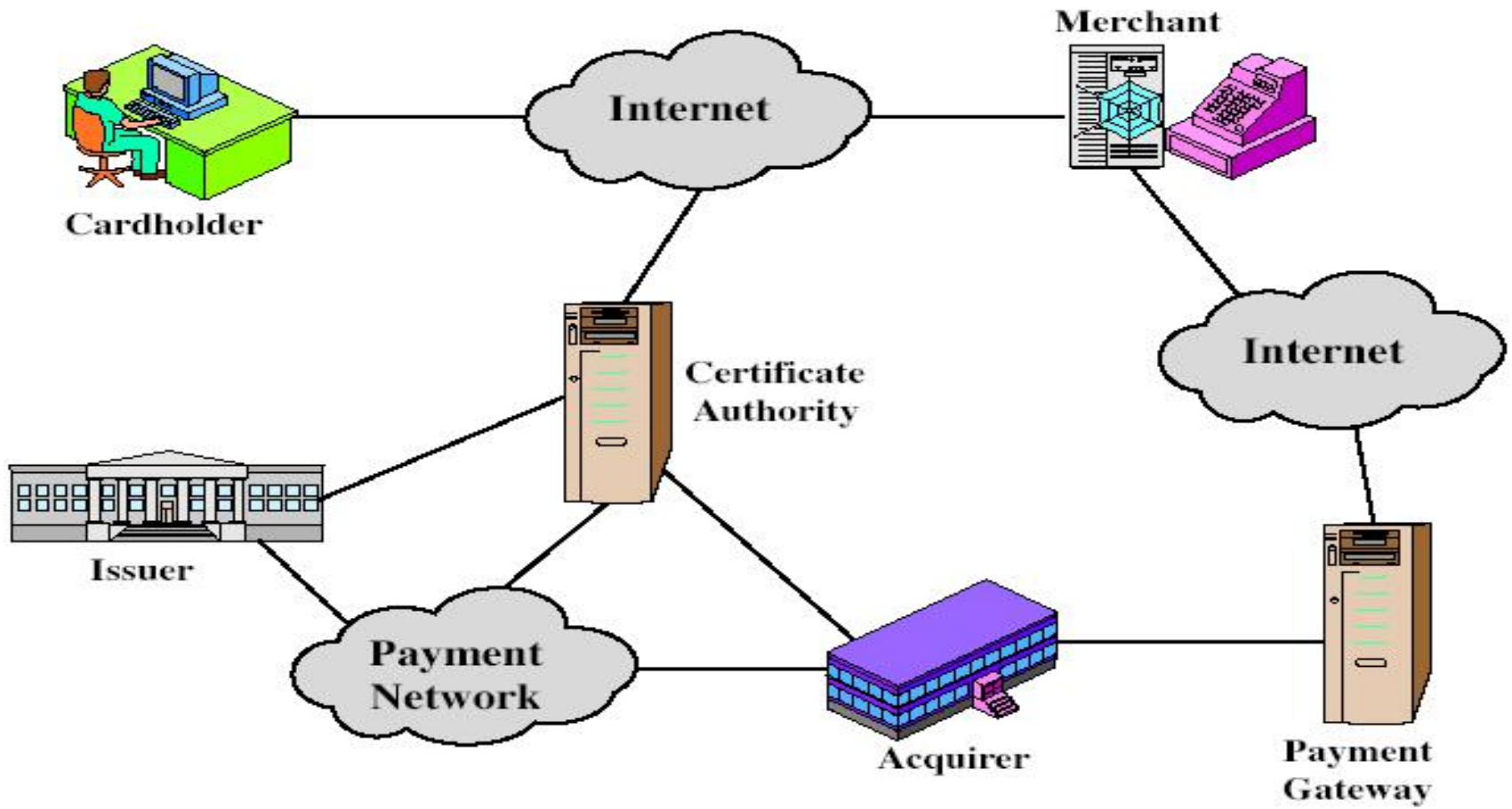
- open encryption & security specification
- to protect Internet credit card transactions
- developed in 1996 by Mastercard, Visa etc **Mastercard Visa 1996**
- not a payment system
- rather a set of security protocols & formats
  - secure communications amongst parties
  - trust from use of X.509v3 certificates**X.509v3**
  - privacy by restricted info to those who need it

Secure Electronic Transaction (SET)

- Merchant does not get to know the credit card details of the cardholder

- Requires software set up on the client as well as server

SET Participants
SET



SET Transaction Process
SET

1. customer opens account
2. customer receives a certificate
3. merchants have their own certificates
4. customer places an order
5. merchant is verified
6. order and payment are sent
7. merchant requests payment authorization
8. payment gateway authorizes payment
9. merchant confirms order
10. merchant provides goods or service
11. merchant requests payment

SET – Dual Signature Concept

- **customer creates dual messages**
  order information (OI) for merchant
  - **payment information (PI) for bank**
- **neither party needs details of other**

- **but must know they are linked**

- **use a dual signature for this**
  - **signed concatenated hashes of OI & PI**

SET – Dual Signature Concept

1. Purchase-related information

（a) PI

DS[PI+OI]

OIMD

(b)All above are encrypted with K

(c)Digital envelope is created by encrypting K with the payment gateway’s public key

SET – Dual Signature Concept

2. Order-related information

    QI

    DS[PI+OI]

    PIMD

3. Cardholder certificate

SET – Dual Signature Concept

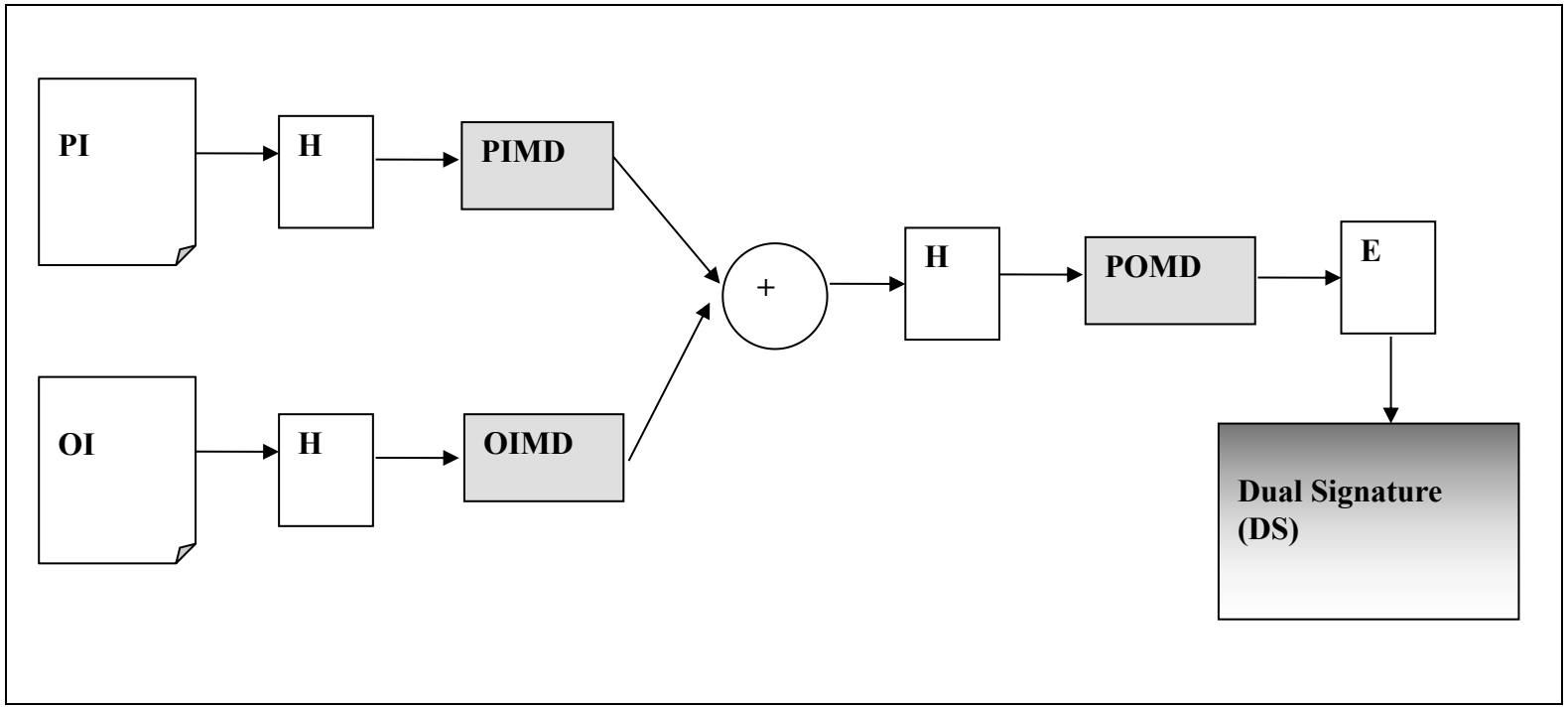
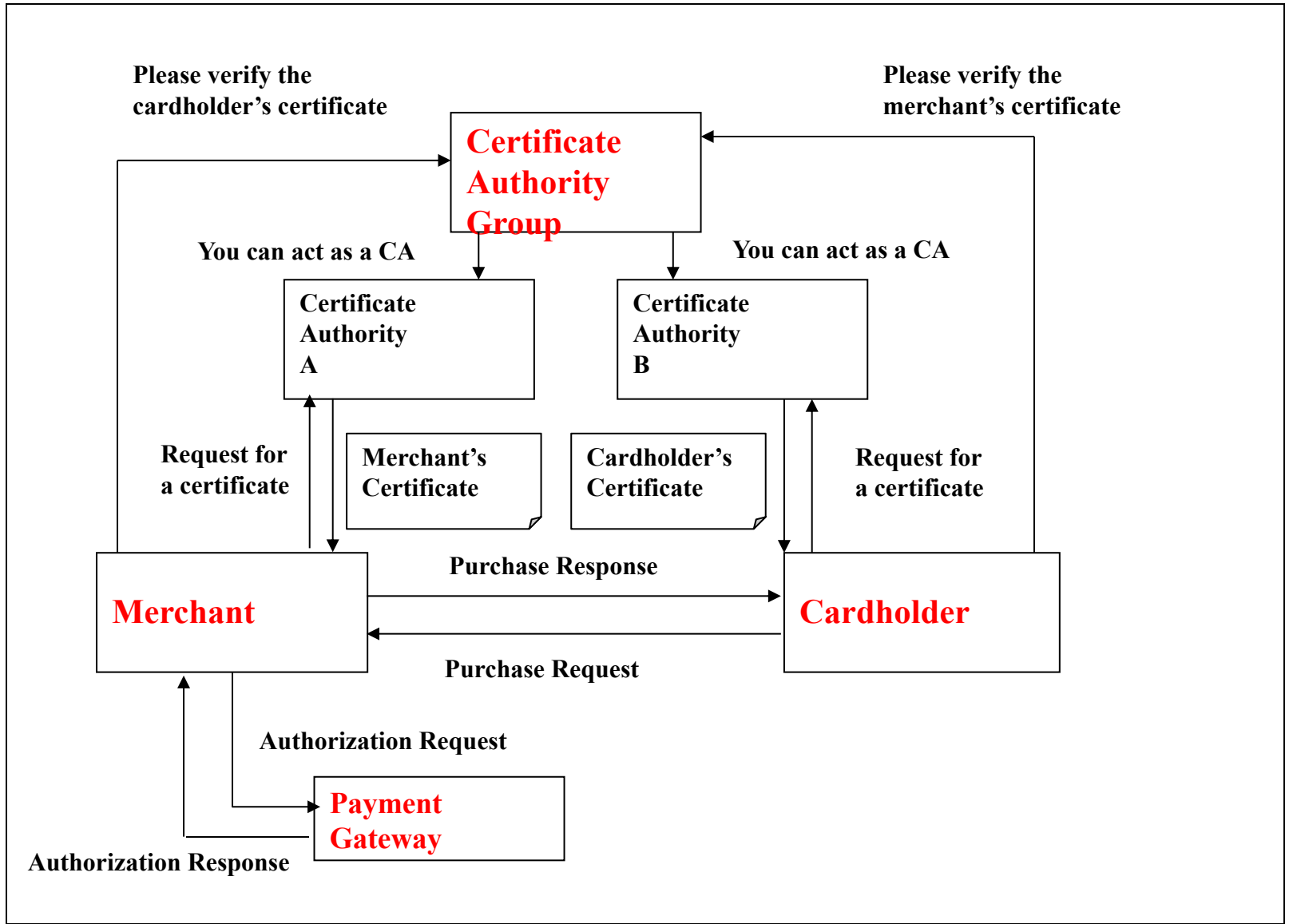


Fig 6.31

SET Model


Please verify the cardholder's certificate
Please verify the merchant's certificate
Certificate Authority Group
You can act as a CA
You can act as a CA
Certificate Authority A
Certificate Authority B
Request for a certificate
Merchant's Certificate
Cardholder's Certificate
Request for a certificate
Purchase Response
Merchant
Cardholder
Purchase Request
Authorization Request
Payment Gateway
Authorization Response

SSL versus SET

Issue	SSL	SET
Main aim	Exchange of data in an encrypted form	E-commerce related payment mechanism
Certification	Two parties exchange certificates	All the involved parties must be certified by a trusted third party
Authentication	Mechanisms in place, but not very strong	Strong mechanisms for authenticating all the parties involved
Risk of merchant fraud	Possible, since customer gives financial data to merchant	Unlikely, since customer gives financial data to payment gateway
Risk of customer fraud	Possible, no mechanisms exist if a customer refuses to pay later	Customer has to digitally sign payment instructions
Action in case of customer fraud	Merchant is liable	Payment gateway is liable
Practical usage	High	Low at the moment, expected to grow