

Secure Electronic Transaction (SET)

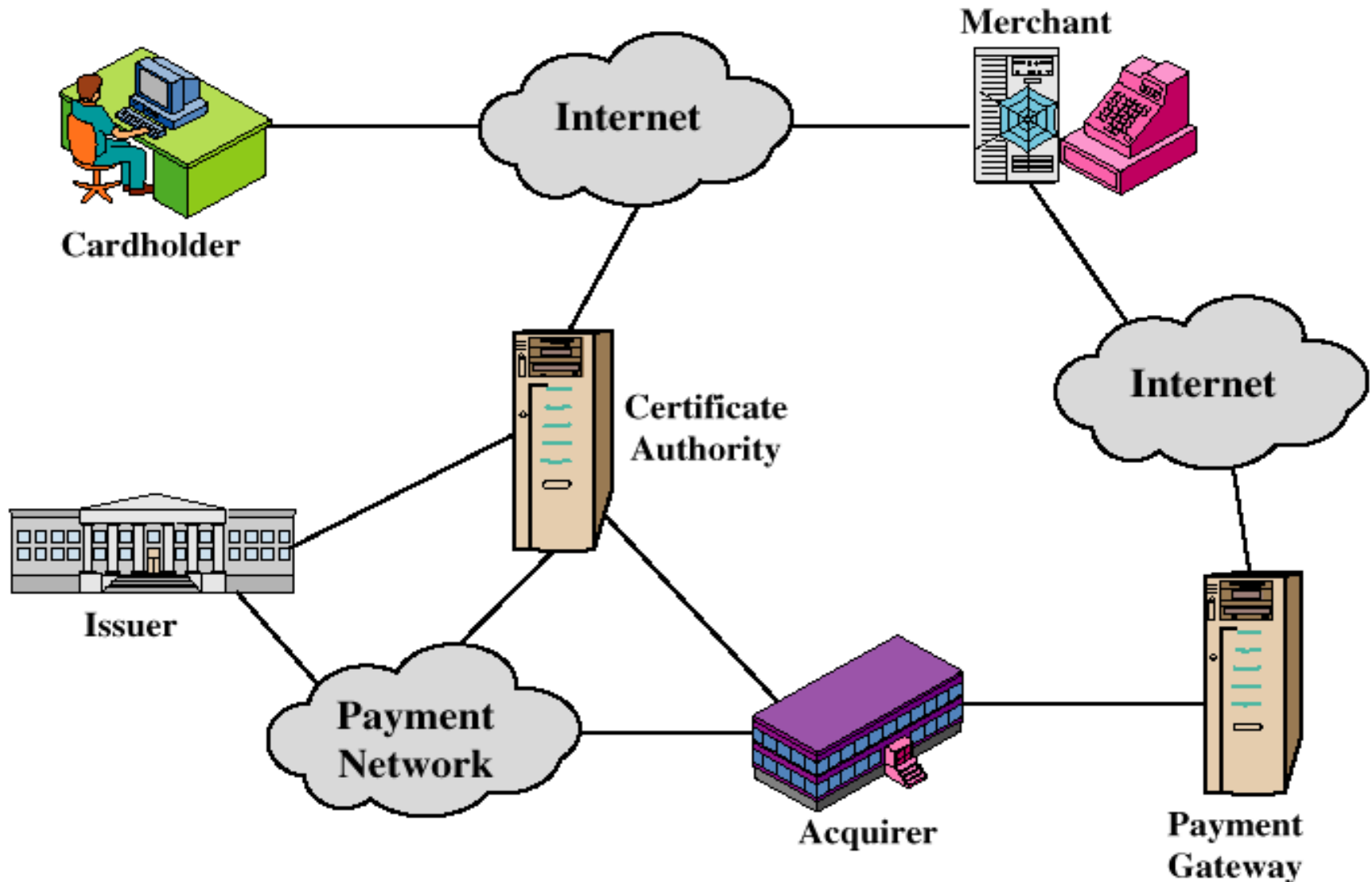
Credit and Debit Cards on the Internet

- Problem: communicate credit and debit card and purchasing data securely to gain consumer trust
 - Authentication of buyer and merchant
 - Confidential transmissions
- Systems vary by
 - Type of public-key encryption
 - Type of symmetric encryption
 - Message digest algorithm
 - Number of parties having private keys
 - Number of parties having certificates

Secure Electronic Transaction (SET)

- Developed by Visa and MasterCard
- Designed to protect credit and debit card transactions
- Confidentiality: all messages encrypted
- Trust: all parties must have digital certificates
- Privacy: information made available only when and where necessary

Participants in the SET System



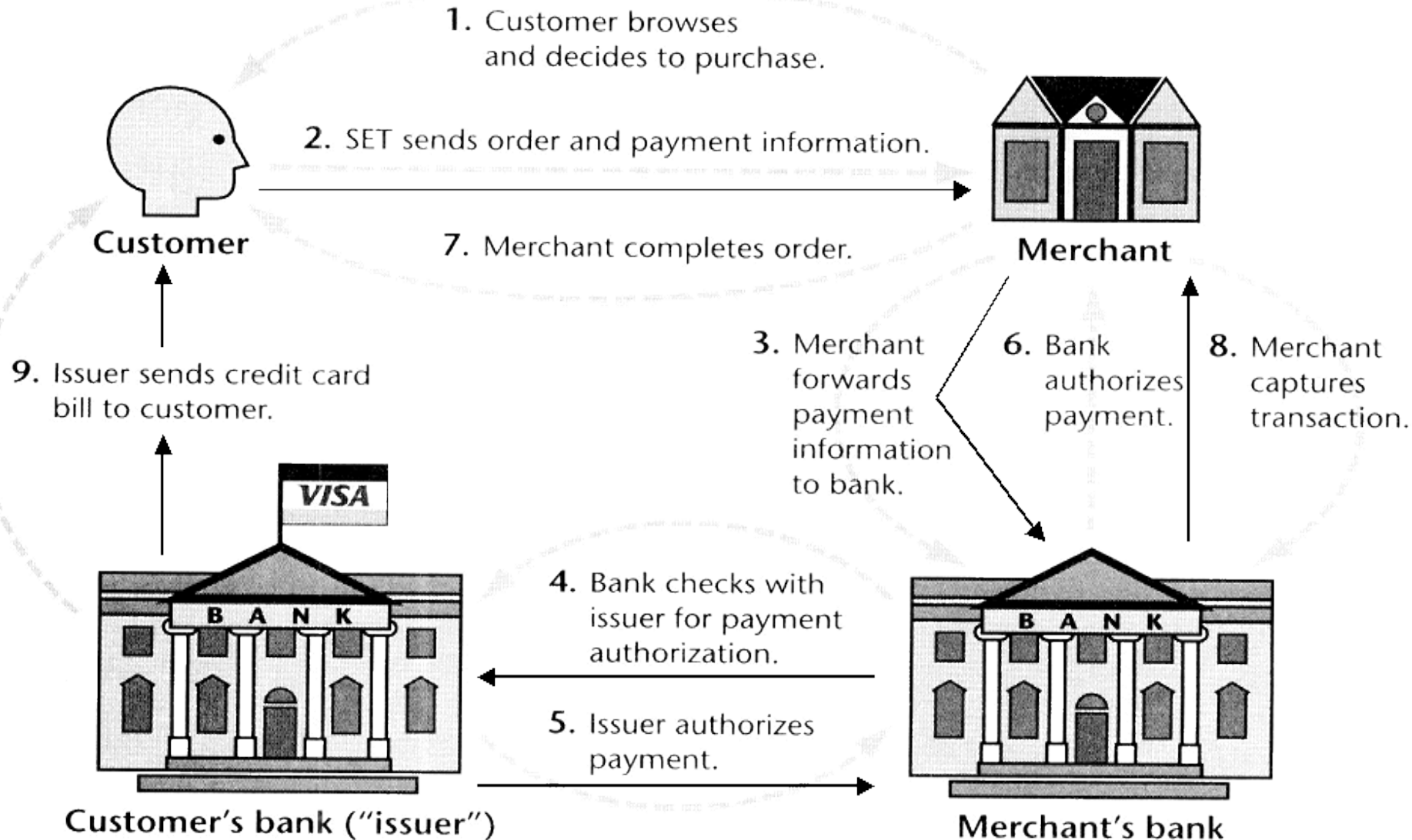
SET Business Requirements (1)

- Provide confidentiality of payment and ordering information
- Ensure the integrity of all transmitted data
- Provide authentication that a cardholder is a legitimate user of a credit or debit card account
- Provide authentication that a merchant can accept credit or debit card transactions through its relationship with a financial institution

SET Business Requirements (2)

- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction
- Create a protocol that neither depends on transport security mechanisms nor prevents their use
- Facilitate and encourage interoperability among software and network providers

SET Transactions (1)



SET Transactions (2)

- The customer opens an account with a card issuer.
 - MasterCard, Visa, etc.
- The customer receives a digital certificate signed by a bank.
- A merchant who accepts a certain brand of card must possess two digital certificates.
 - One for signing & one for key exchange
- The customer places an order for a product or service with a merchant.
- The merchant sends a copy of its certificate for verification.

SET Transactions (3)

- The customer sends order and payment information to the merchant.
- The merchant requests payment authorization from the payment gateway prior to shipment.
- The merchant confirms order to the customer.
- The merchant provides the goods or service to the customer.
- The merchant requests payment from the payment gateway.

SET Supported Transactions

- card holder registration
- merchant registration
- purchase request
- payment authorization
- payment capture
- certificate query
- purchase inquiry
- purchase notification
- sale transaction
- authorization reversal
- capture reversal
- credit / payment reversal

Key Technologies of SET

- Confidentiality of information: 3DES
- Integrity of data: RSA digital signatures with SHA-1 hash codes
- Cardholder account authentication: digital certificates with RSA signatures
- Merchant authentication: digital certificates with RSA signatures
- Privacy: separation of order and payment information using dual signatures