Secure Electronic Transaction and dual signature

-By Sahil Choudhary
-161090065

Secure Electronic Transaction (SET)

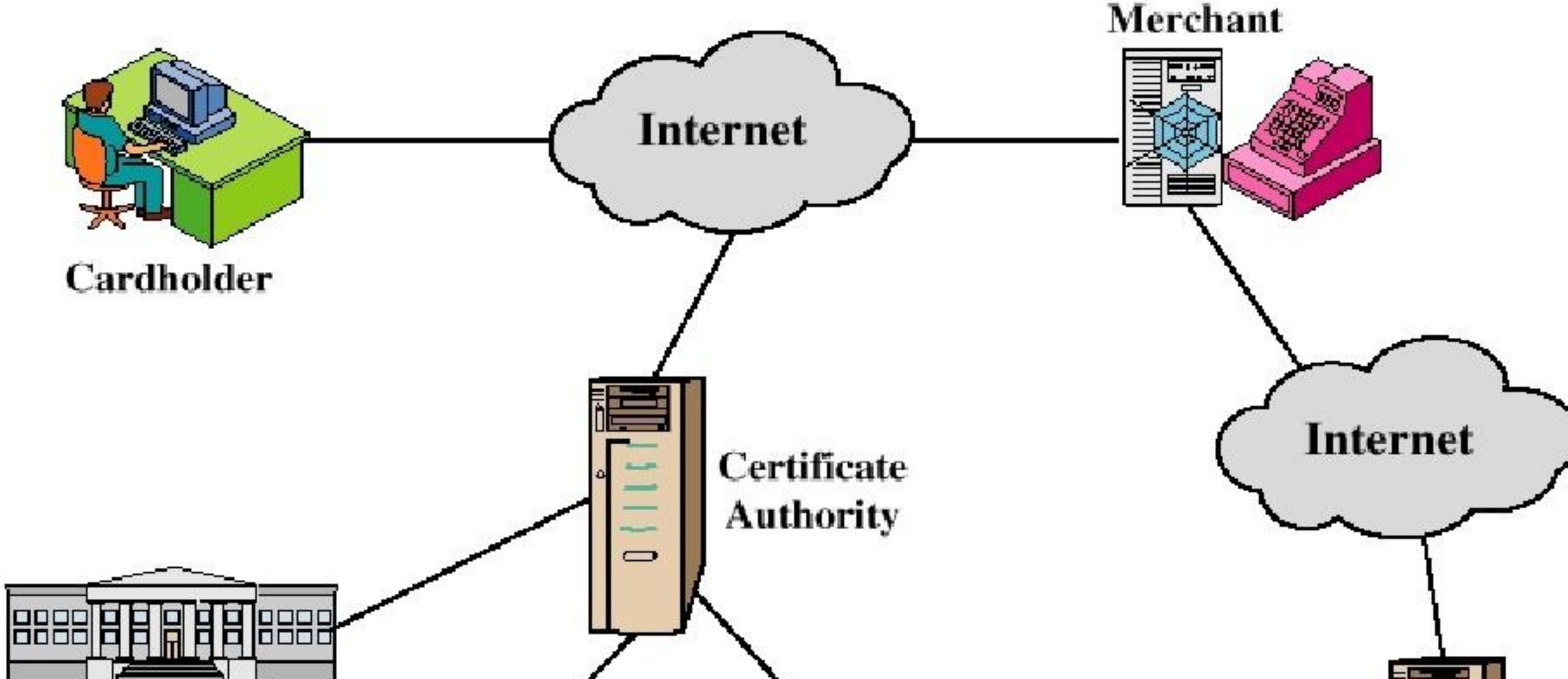
Credit and Debit Cards on the Intern

- Problem: communicate credit and debit card and purchasing data securely to gain consume trust
  - Authentication of buyer and merchant
  - Confidential transmissions
- Systems vary by
  - Type of public-key encryption

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

Participants in the SET System



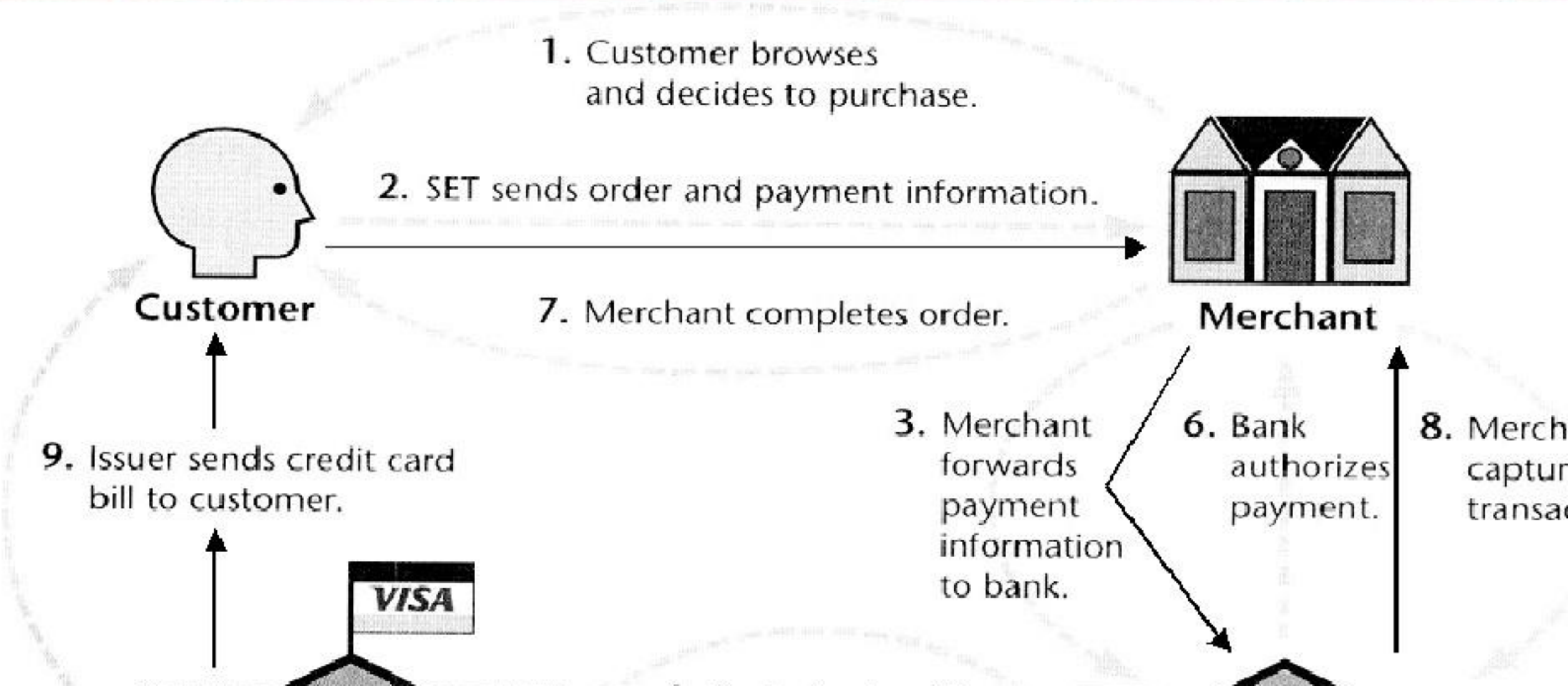
SET Business Requirements (1

- 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

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

SET Transactions (1)



1. Customer browses and decides to purchase.

2. SET sends order and payment information.

7. Merchant completes order.

9. Issuer sends credit card bill to customer.

3. Merchant forwards payment information to bank.

6. Bank authorizes payment.

8. Merch captur transac

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

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

SET Supported Transactions

- card holder registration
- merchant registration
- purchase request
- payment authorization
- payment capture
- certificate query
- purchase inquiry
- purchase notification

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

WHAT IS DUAL SIGNATURE?

+DUAL SIGNATURE link 2 messages that are intended for two different recipients .

+It is a process that guarantees that the contents of a message have not been altered in transit.

+The design of signature is not the binding principle.

PURCHASE REQUEST

Purchase request exchange consists of four messages:

1. **Initiate Request**
2. **Initiate Response**
3. **Purchase Request**
4. **Purchase Response**

INITIATE REQUEST

Basic Requirements:

+ Cardholder Must Have Copy of Certificates for Merchant and Payment Gateway
+ Customer Requests the Certificates in the Initiate Request Message to Merchant
+ Brand of Credit Card
+ ID Assigned to this Request/response pair by customer.
+ Nonce(timestamp) used to ensure timeliness.

INITIATE RESPONSE

+Merchant Generates a Response
+Signs with Private Signature Key.
+Transaction ID for Purchase Transaction
+Merchant's Signature Certificate
+Payment Gateway's Key Exchange Certificate
+The nonce from the customer
+Another nonce for the customer to return in the next message

PURCHASE REQUEST

+Cardholder Verifies Two Certificates(merchant and gateway)
Using their CAs and
+Creates the OI and PI.

First SET Message Includes:
+ Purchase-related Information
+ Order-related Information
+ Cardholder Certificate

THANK YOU!