Secure Electronic Transactions (SET)

Jibi Abraham

COEP TECHNOLOGICAL UNIVERSITY

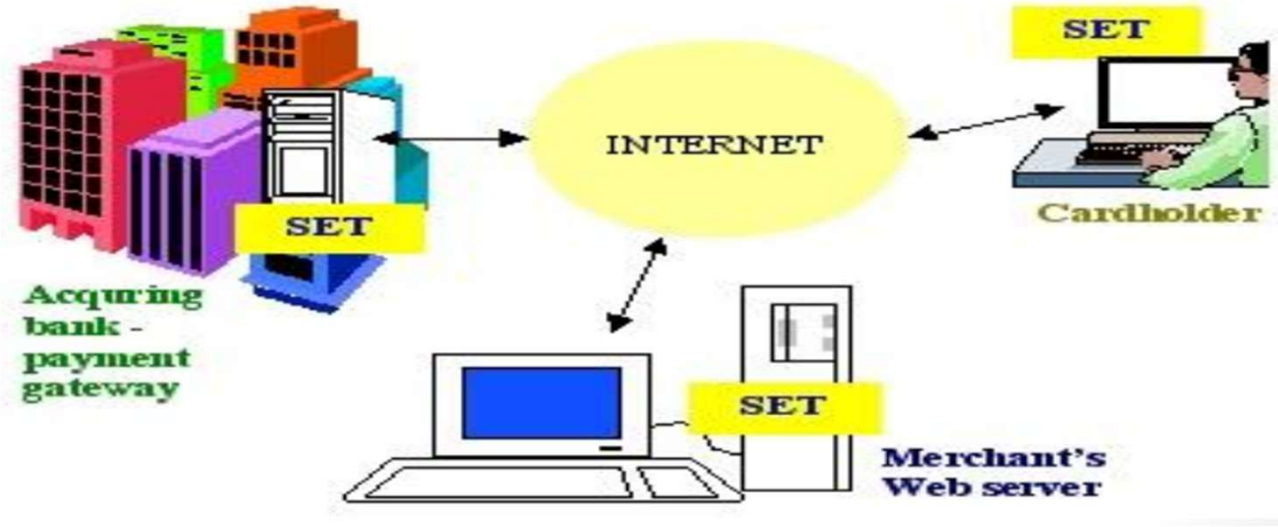
Shivajinagar, Pune-411 005

(A Unitary Technological University of Govt. of Maharashtra)

Secure Electronic Transactions (SET)

- Open encryption and security specification to protect Internet credit card transactions
- Developed in 1996 by Mastercard, Visa, IBM, Microsoft, Netscape, RSA, Terisa, and Verisign
- Not a payment system, rather a set of security protocols and formats
  - secure communications amongst parties
  - trust from use of X.509v3 certificates
  - privacy by restricted info to those who need it

WHY SET?



- Security concern of:
  - Consumers
  - Merchants
  - Issuer, Acquirer and Settlement Banks
- Growth in volume of credit card transactions over the internet
  - Need a protocol that protects consumers and merchants alike, allowing each to verify the identities of the other parties without necessarily revealing credit card information
  - This level of authentication does not exist in other cryptography-based protocols: SSL

SET: A Brief History

- Visa and Microsoft:
  - Secure Transaction Technology (STT): 1995
- MasterCard, Netscape, IBM, CyberCash:
  - Secure Electronic Payment Protocol (SEPP): 1996
- STT ans SEPP:
  - Change the bankers' treatment of internet-based credit card transactions
  - Require all parties to have digital certificates
  - Required having public key certificate authorities
  - Use industry standard public key cryptography techniques: Rivest, Shamir, Adelman (RSA)
  - Encrypt only credit card numbers and transactional data rather than the entire browser and shopping sessions
  - Enable using any type of credit card regardless of its issuer

SET: July 1997

- Objectives:
  - Provide confidentiality of payment information
  - Ensure the integrity of all transmitted data
  - Provide authentication that a Cardholder is a legitimate user of a branded payment card account
  - Provide authentication that a Merchant can accept payment card transactions through its bank
  - Ensure the use of best security practices and system design techniques to protect all legitimate parties
  - Facilitate and encourage interoperability among software and network providers

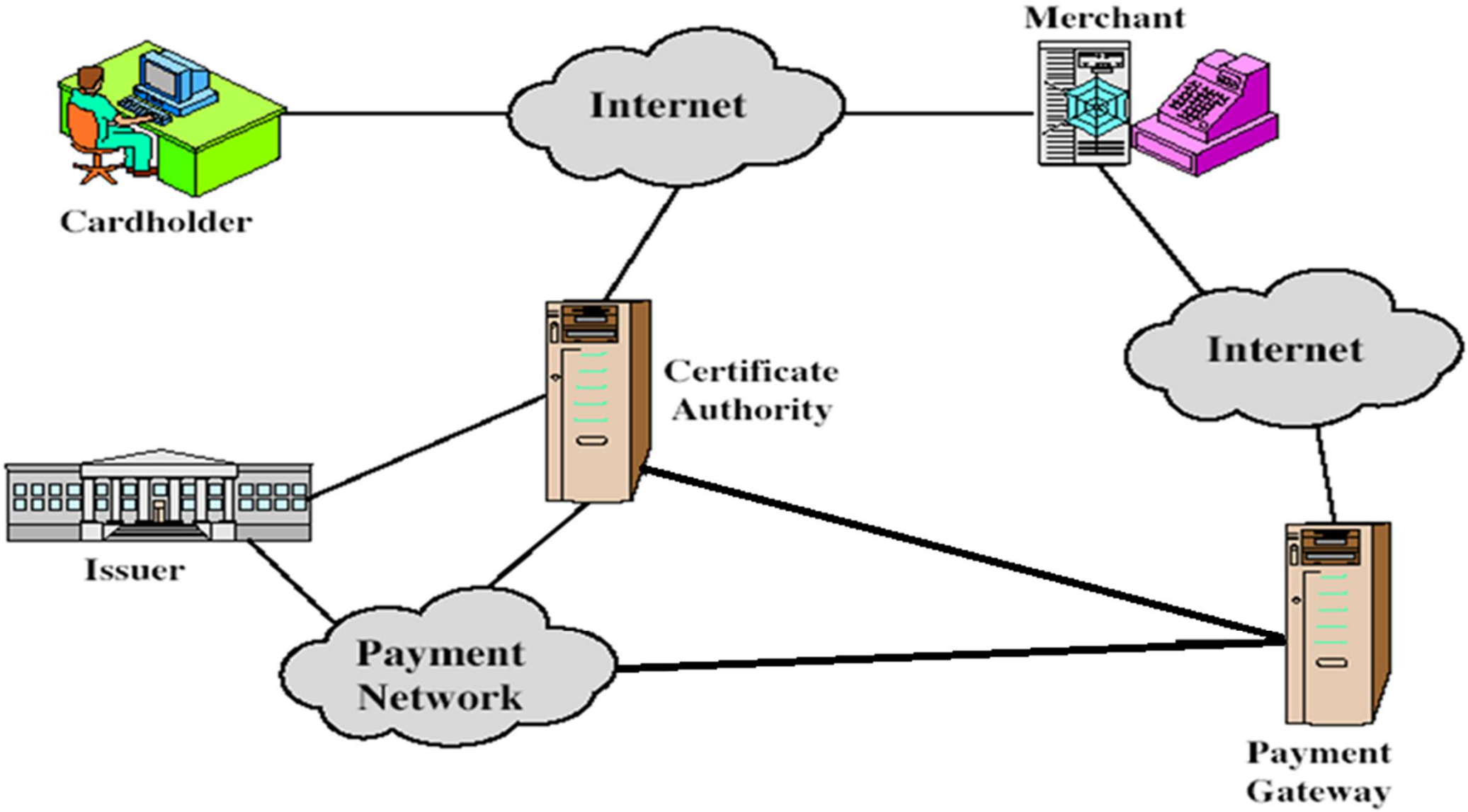
SET

- Out-of-band:
  - Phases that are not included under SET
  - Activities that their implementation is left up to the involved parties
  - Systems required for using SET
- Merchants and banks need to customise their own applications in order to plug into SET infrastructure

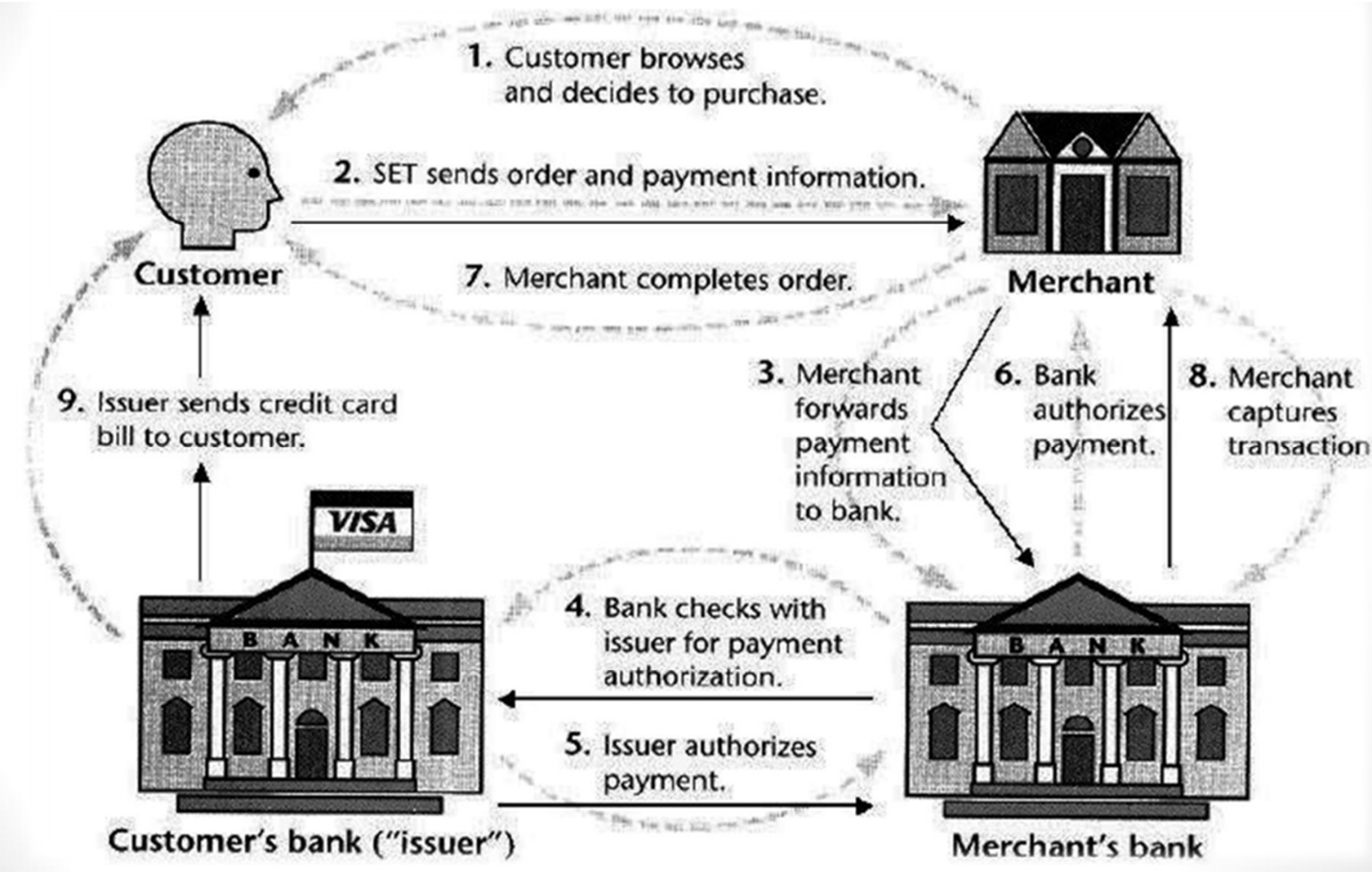
PAYMENT SYSTEMS

- Closed Loop Systems
  - Amex, Discover, Diners Club
  - The bank serves as a broker between the user of its cards and the Merchants
- Open Loop Systems
  - Cardholder and Merchant having different banks and the transaction is settled by a bank that is different than the either two
  - Visa and MasterCard

SET Components



SET Transactions



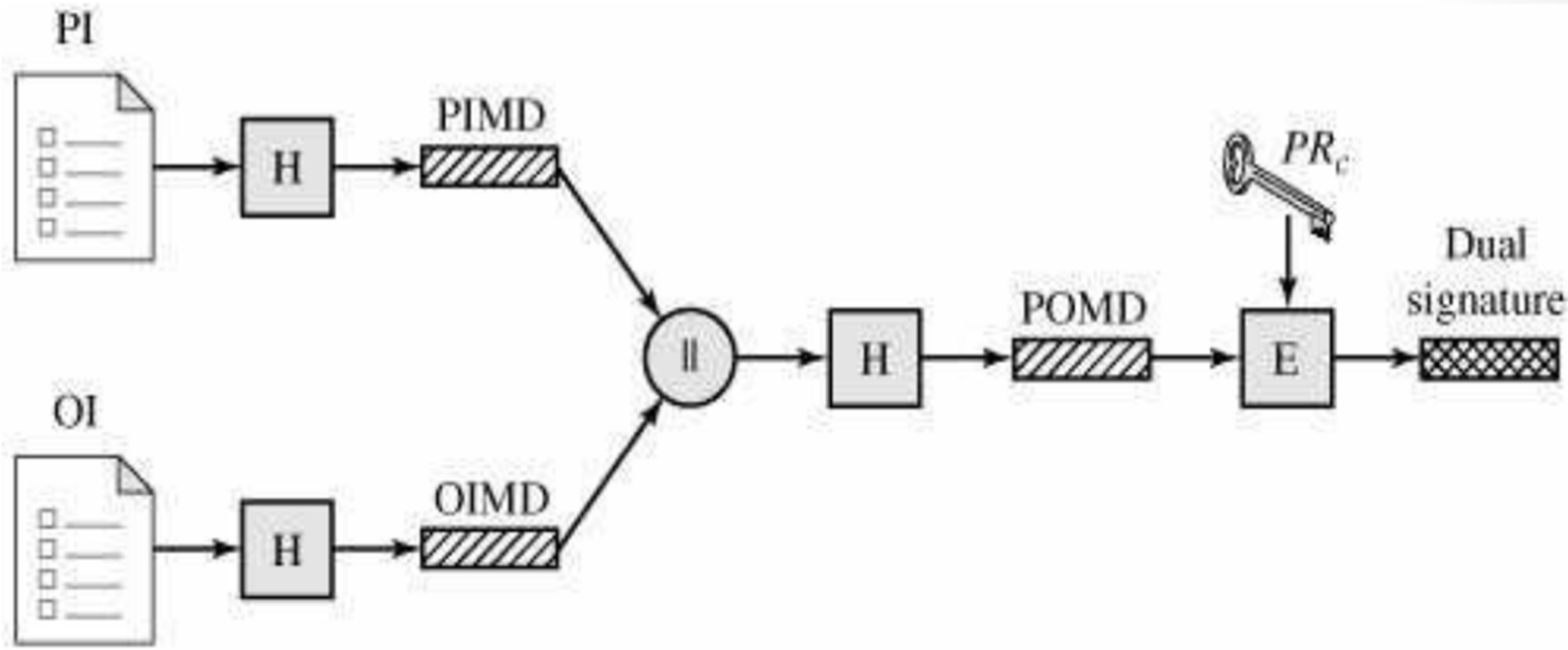
SET Transaction

1. Customer opens account: customer obtains a credit card account
2. Customer receives a certificate: an X.509v3 digital certificate, which is signed by the bank. The certificate verifies the customer's RSA public key and its expiration date
3. Merchants have their own certificates: Posses two certificates for two public keys owned by the merchant: one for signing messages, and one for key exchange.Also has a copy of the payment gateway's public-key certificate
4. Customer places an order: order form includes list of
5. items, their price, a total price, and an order number
6. Merchant is verified
7. Customer sends order and payment to the merchant, along with the customer's certificate
8. Merchant requests payment authorization: merchant sends the
9. payment information to the payment gateway
10. Merchant confirms order
11. Merchant provides goods or service
12. Merchant requests payment

Dual Signature

- Is to link two messages that are intended for two different recipients
- Customer creates dual messages
  - Order information (OI) to merchant
  - Payment information (PI) to bank
- Neither party needs details of the other
- But **must** know they are linked
- Use a dual signature for this
  - signed concatenated hashes of OI and PI

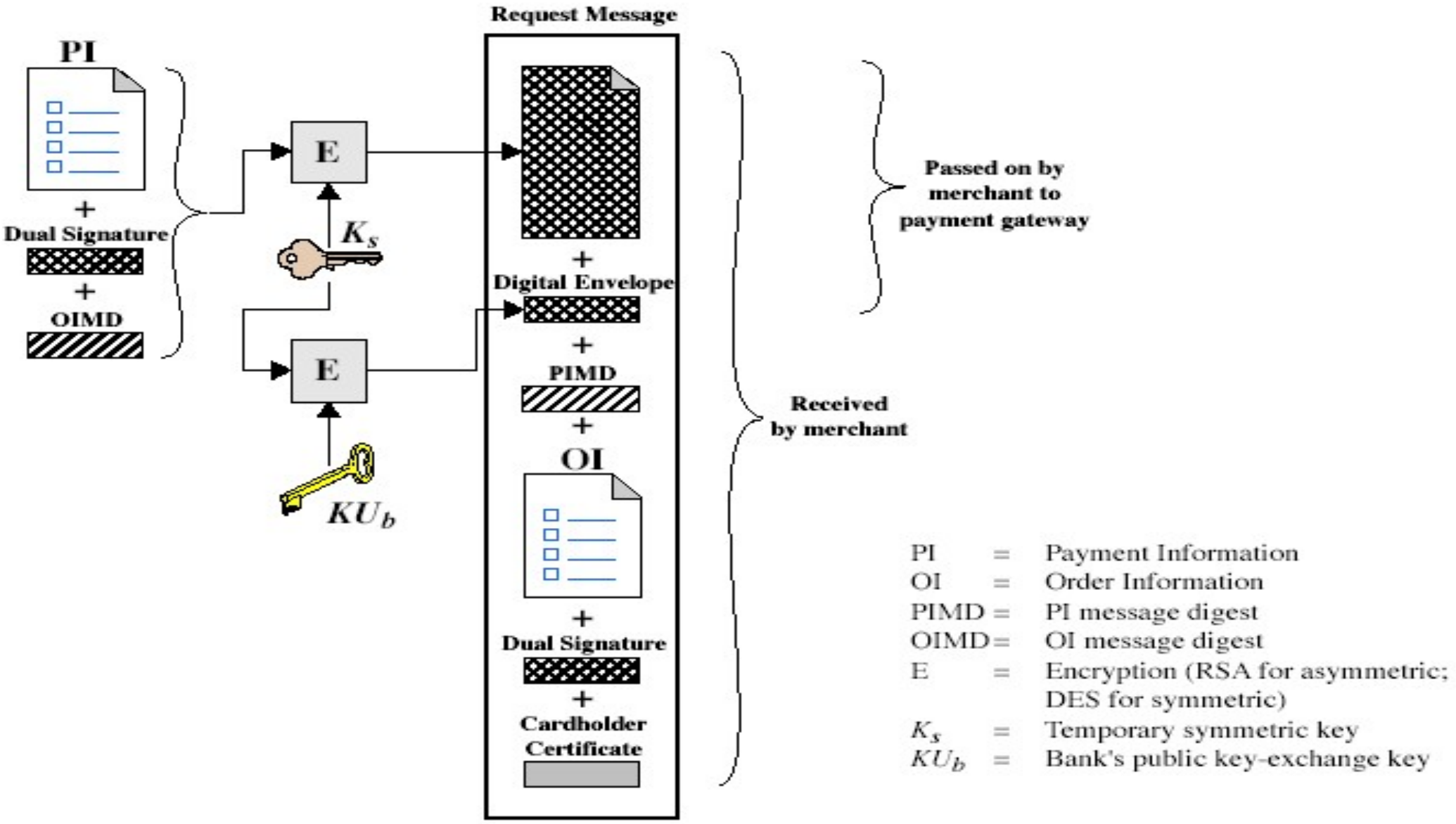
Dual Signature



PI = Payment information
OI = Order information
H = Hash function (SHA-1)
|| = Concatenation

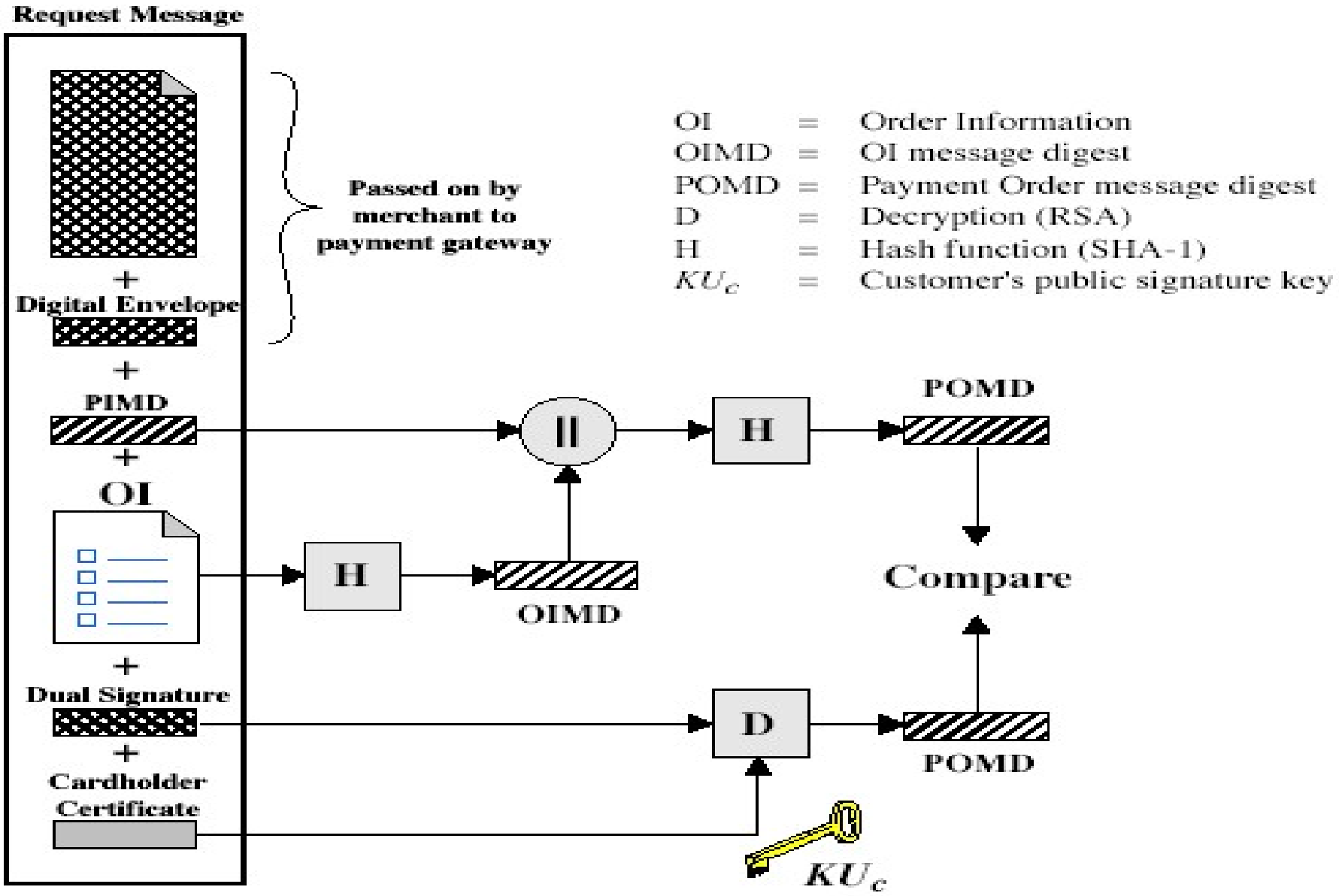
PIMD = PI message digest
OIMD = OI message digest
POMD = Payment order message digest
E = Encryption (RSA)
PR_c = Customer's private signature key

Purchase Request – Customer



PI	=	Payment Information
OI	=	Order Information
PIMD	=	PI message digest
OIMD	=	OI message digest
E	=	Encryption (RSA for asymmetric; DES for symmetric)
K_s	=	Temporary symmetric key
KU_b	=	Bank's public key-exchange key

Purchase Request – Merchant



Purchase Request – Merchant

1. Verifies cardholder certificates using CA sigs
2. Verifies dual signature using customer's public signature key to ensure order has not been tampered with in transit and that it was signed using cardholder's private signature key
3. Processes order and forwards the payment information to the payment gateway for authorization (described later)
4. Sends a purchase response to cardholder

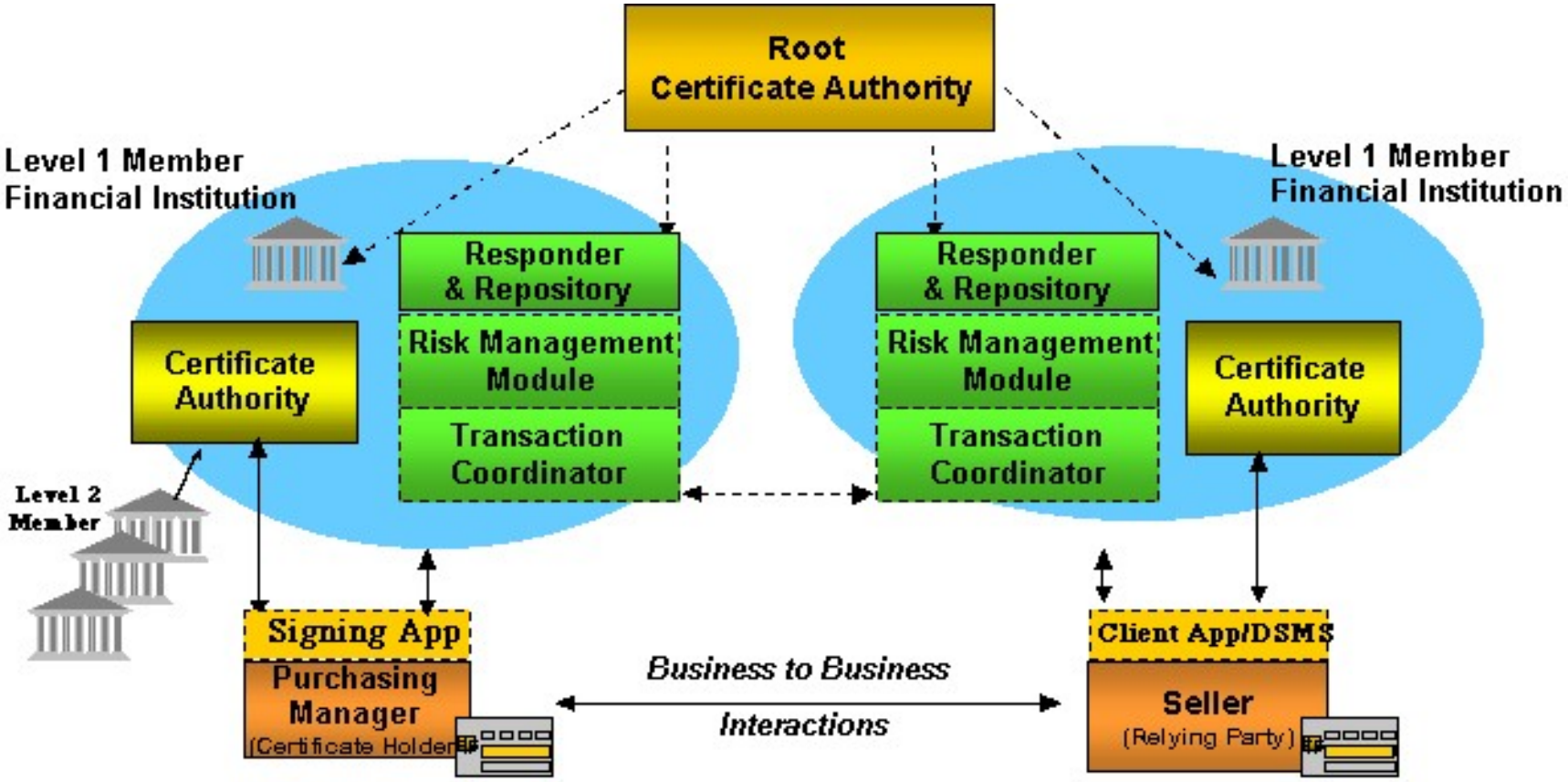
Payment Gateway Authorization

1. Verifies all certificates
2. Decrypts digital envelope of authorization block to obtain symmetric key and then decrypts authorization block
3. Verifies merchant's signature on authorization block
4. Decrypts digital envelope of payment block to obtain symmetric key & then decrypts payment block
5. Verifies dual signature on payment block
6. Verifies that transaction ID received from merchant matches that in PI received (indirectly) from customer
7. Requests and receives an authorization from issuer
8. Sends authorization response back to merchant

Payment Capture

- Merchant sends payment gateway a payment capture request
- Gateway checks request then causes funds to be transferred to merchants account
- Notifies merchant using capture response

Multiple CAs
Trust - Technical Architecture



Source: Identrus