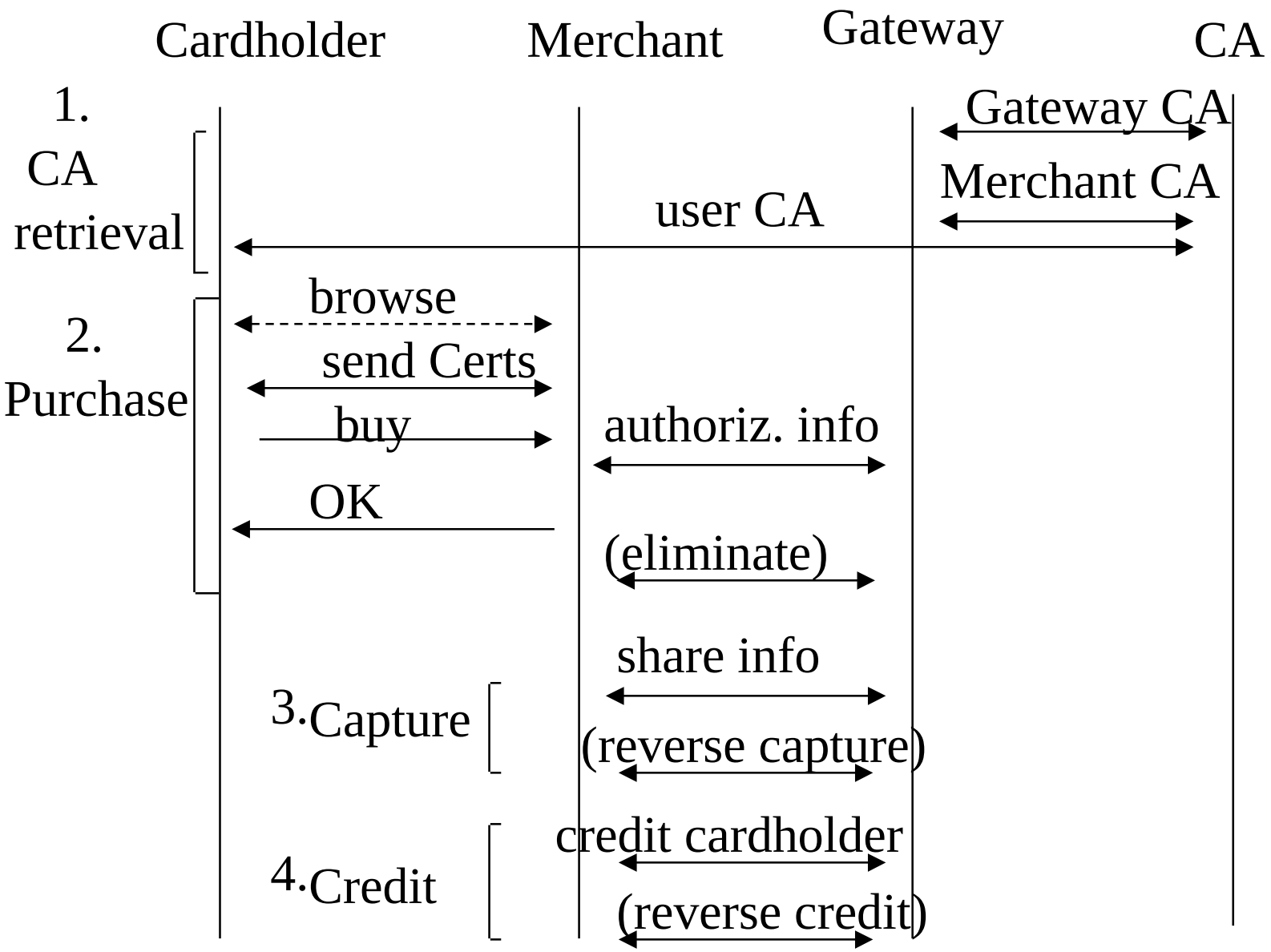
SET Secure Electronic Transactions

- Original participants: VISA and MasterCard, GTE, IBM, Microsoft, Netscape, SAIC, Terisa, Verisign.
- Officially announced February 1, 1996.
- SET enables safe business over insecure networks - i.e., the Internet.
- SET outlines a series of messages, as well as their contents and formats,to be sent between the participants of an Internet commerce transaction.
- SET uses X.509 and ASN.1 and PKCS for formats.
- Cryptography: DES, RSA and Elliptic Curves.

SET Secure Electronic Transactions

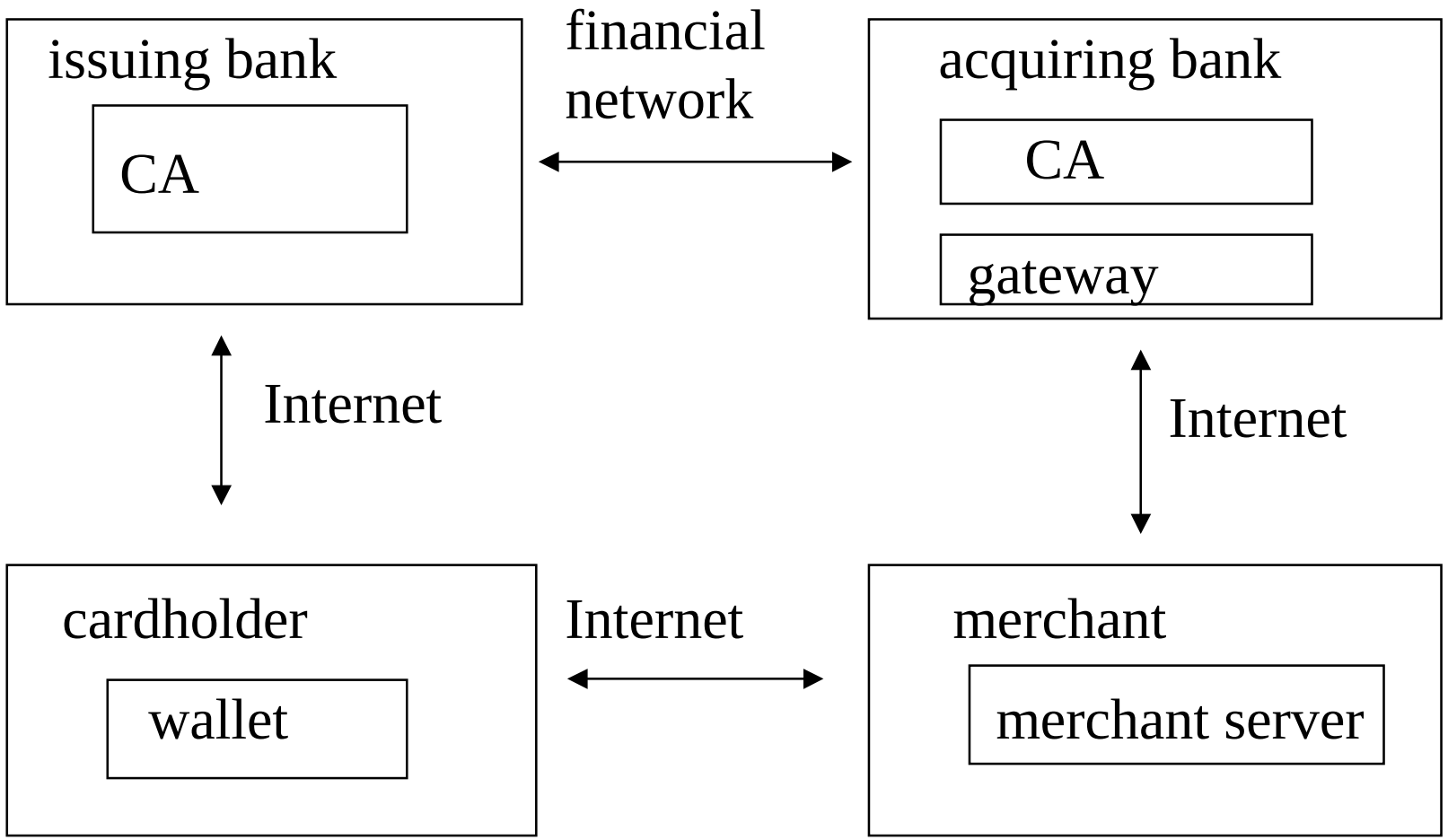
- Cardholder
- Merchant
- Issuer - provider cardholder’s card
- Acquirer - processes card authorizations and payments to the merchant
- Payment Gateway - institution that works on behalf of the acquirer to process merchant’s payment messages, bridge between SET and existing credit card networks
- Certificate Authority -provides cardholder, merchant, payment gateway certificates

SET Secure Electronic Transactions



SET Secure Electronic Transactions

SET Software components



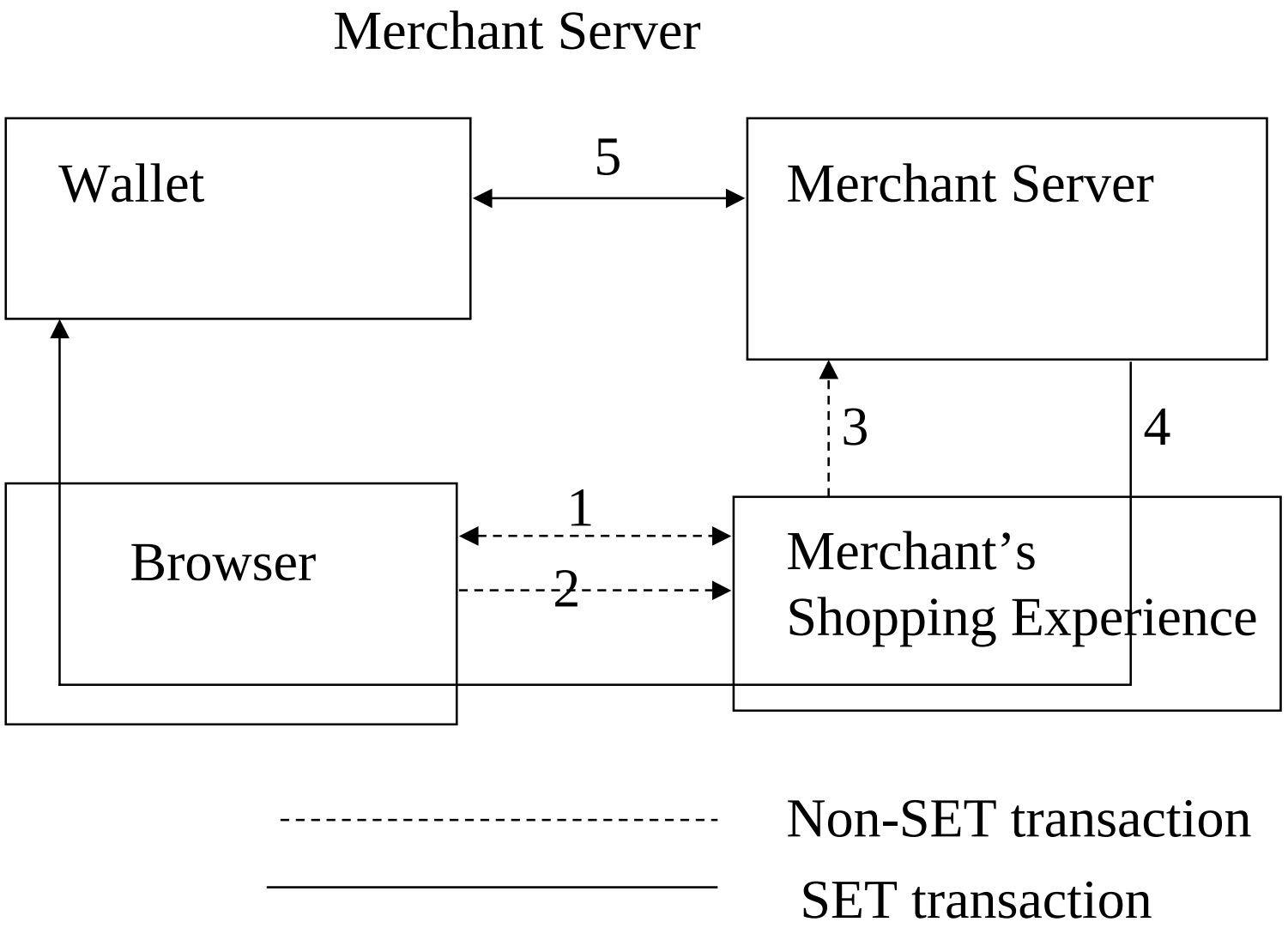
SET Secure Electronic Transactions

- Wallet functionalities:
- -Initiate payment process with merchant
- -Inquire and receive payment info from merchant
- -Inquire and receive payment status from merchant
- -Inquire about order status
- -Accept messages from cardholder’s acquirer
- -Initiate request for cardholder certificates
- -Register to CA
- -Receive cardholder certificates
- -Inquire about status of requested certificates

SET Secure Electronic Transactions

- Existing Wallets:
- X-Pay Java Credit Wallet
- CyberCash Internet Wallet
- CommerceSTAGE Secure Credit Cardholder
- GlobeSet Wallet
- IBM Consumer Wallet
- Microsoft Wallet
- WebWallet
- PayPurse
- vWallet
- NetPay Wallet

SET Secure Electronic Transactions



SET Secure Electronic Transactions

- Merchant server’s core functionality
- -Respond to wallet’s initiation message
- -Receive purchase request and respond
- -Receive and respond to status inquiry from cardholder
- -Receive registration request from cardholder, provide either registration form or address where the form is
- -Generate certificate request to CA, process response
- -Inquire about certificate status, process response
- -Authorize cardholder’s purchase
- -Reverse previously authorized purchase (with acquirer)
- -Handle batch processing with acquirer

SET Secure Electronic Transactions

- Handle capture of funds with acquirer
- Handle reversal of capture of funds with acquirer
- Request acquirer to issue a credit to a cardholder and handle the response
- Generate reversal of granted credit and handel response
- Obtain registration forms from CA
- Handle all errors in the SET protocol

SET Secure Electronic Transactions

- Existing merchant servers
- X-Pay Server
- CyberCash Cashregister
- CommerceSTAGE Secure Credit Payment
- GlobeSet POS (point of sale)
- IBM Payment Server
- NetPay Merchant
- PayWare
- vPOS

SET Secure Electronic Transactions

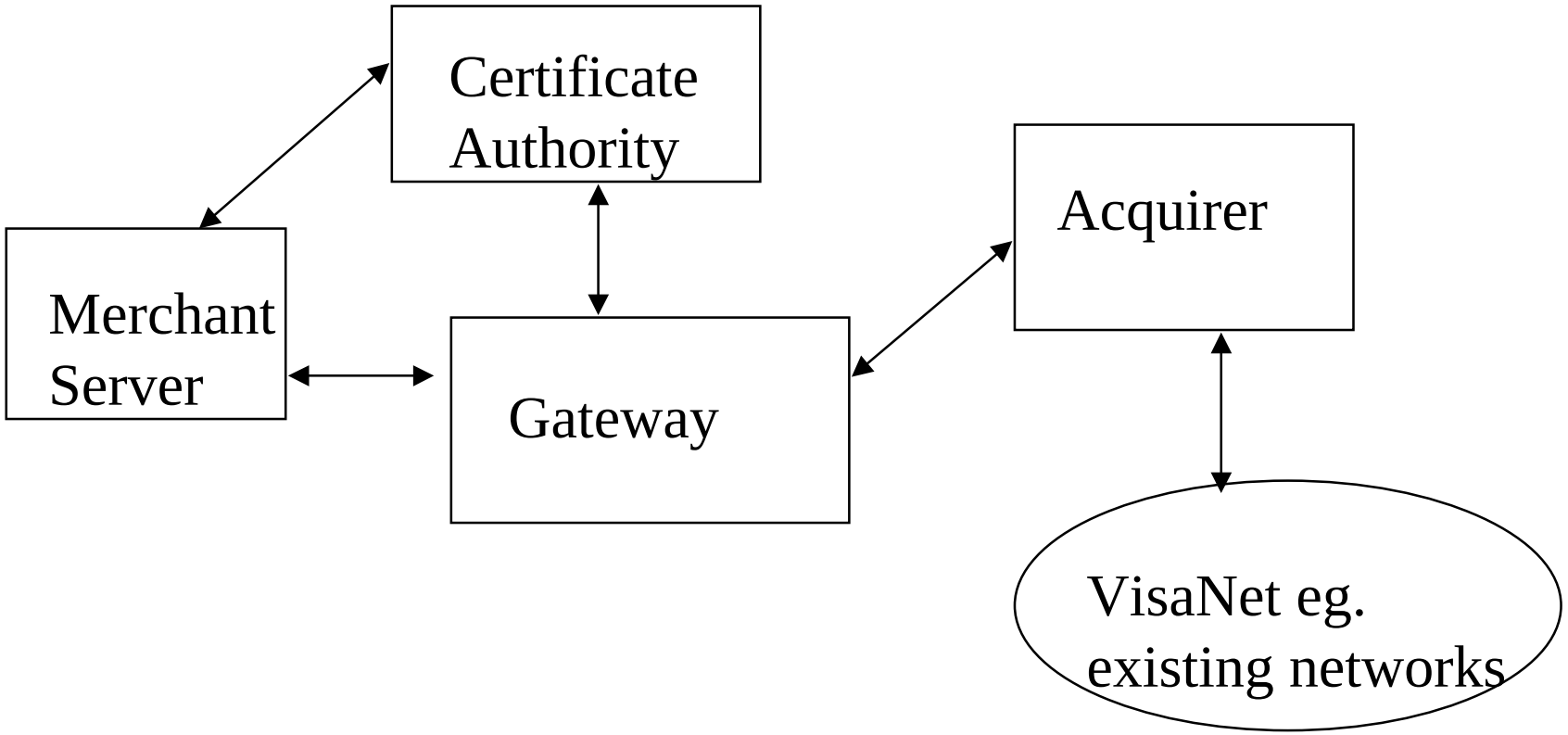
- Certification Authority’s core functionality:
- -Receive, process and respond to cardholder’s initiation message
- -Receive, process and respond to merchant’s certificate initiation message
- -Receive, process and respond to cardholder’s registration messages
- -Receive, process and respond to cardholder’s and merchant’s requests for certificates
- -Receive, process and respond to cardholder’s and merchant’s request for status of their certificates

SET Secure Electronic Transactions

- Existing Certificate Authorities
- Entrust/CommerceCA
- CommerceSTAGE Secure Certificate Authority
- CyberTrust Certificate Management Systems
- GlobeSet CA
- IBM Payment Registry

SET Secure Electronic Transactions

- Payment Gateway
- Allows SET to work within the existing infrastructure without drastic changes



SET Secure Electronic Transactions

- In addition to obvious functionalities as a gateway
- Gateway gives a current Certificate Revocation
- List to the merchant server
- Gateway has special gateway certificates

- Existing Gateways
- X-Pay Server
- CommerceSTAGE Secure Payment Gateway
- GlobeSet Gateway
- IBM Payment Gateway

SET Secure Electronic Transactions

- Cryptographic techniques in SET
- DES, note, DES is broken by brute force, DES modes from FIPS 81: ECB, CBC, CFB, OFB

- RSA (following PKCS Public-Key Cryptography Standards defined by RSA Laboratories)
- In SET two pairs of public-private keys, one for signing, the other for encryptation
- SET follows PKCS#7 Cryptographic Message Syntax Standard for transfer syntax, (ASN.1, resembles X.509 datatypes)

SET Secure Electronic Transactions

- OAEP Optimal Asymmetric Encryptation Padding
- Used in SET, a cryptographically strong padding method, distributes randomly the bits of a PKCS#7 block, each bit is equally hard to obtain.
- SHA-1 Secure Hash Algorithm 1, is currently used in SET.
- Elliptic Curve cryptography is a future alternative for RSA in SET, it is included in SET extensions.
- For signatures, SET has developed so called dual signatures. It enables the message to be sent to two players (like merchant, acquirer) so that each can verify hash of text meant to them.

SET Secure Electronic Transactions

- Elliptic Curve Enabled Secure Electronic Transactions (ECSET)
- RSA is replaced by Elliptic Curve Digital Signature Algorithm (ECDSA). It has shorter keys and smaller signatures than RSA.(ECDSA is a public key algorithm)
- Elliptic curves are usually on finite fields Z_p
- Example: an elliptic curve over Z_3 is the union of infinity point and the set $\{(x,y) : y^2 = x^2 + ax + b,\ x,y \in Z_3\ \}$
- SET proposes 163 bit keys for most players and 239 bit keys for the root CA if ECDSA is used. Notice, that the key lengths are much smaller than what SET proposes for RSA (1024, 2048 bits).

SET Secure Electronic Transactions

- SET Certificates
  - Developed from X.509 certificates by adding SET specific fields
  - Certificate Management Architecture
  - Root CA (RCA) - distributes CRL if BCA disabled
  - Brand CA (BCA) - distributes CRLs (Cert.Rev.Lists)
  - Geo-Political CA (GCA) - optional
  - Cardholder CA - issues Cardholder Certificates
  - Merchant CA - issues Merchant Certificates
  - Payment Gateway CA - issues Payment Gateway Certificates

SET Secure Electronic Transactions

- Only RCA, BCA, GCA and PCA are required to maintain certificate revocation lists
- CCAs and MCAs not, because their certificates are never revoked, they are cancelled.
- SET uses different kind of certificates
  - Digital Signature Certificates - entity's public signature key
  - Key Encryptation Certificates - holds entity's public encryptation key
  - Certificate and Certificate Revocation List Signing Certificates - there certificates contain copies of entity's public certificate and CRL signing keys

SET Secure Electronic Transactions

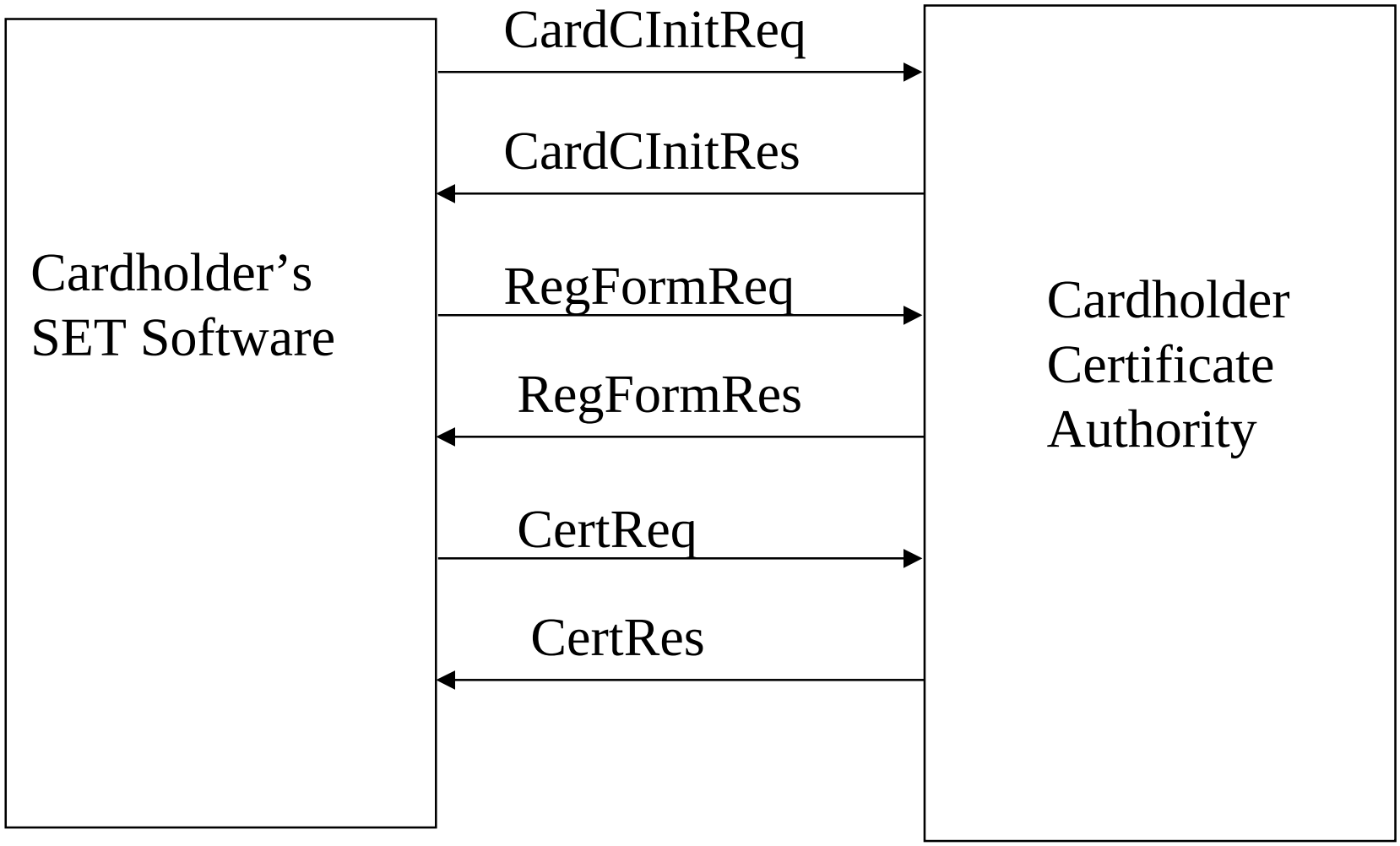
- SET certificates are X.509 certificates with versio 3 in SET v1.0. SET certificates contain may additional fields, such as the brand of the certificate - this field makes impossible to cheat by changing userCertificate to cACertificate, there are also cardholder’s account number etc. fields.
- Cardholder Certificate Cancellation - if user’s private keys are stolen, he initiates issuer-based cancellation, bank labels the certificate cancelled
- Merchant Certificate Cancellation
- Payment Gateway Certificate Revocation

SET Secure Electronic Transactions

- Thumbprints - in SET thumbprints are made to certificates, CRLs, Brand CLR Identifiers.
- Thumbprint is made by putting the data through a hash function. The receiver of a thumbprint compares it to his local storage and tries to decide whether he already has sent the certificate, i.e., has the thumbprint in his local database or if he needs to send it. The method seems relatively safe as it only means whether to send a certificate or assume that the other side has it. It the other side does not have, it will ask for the certificate.
- Inclusion of a thumbprint in SET is optional and the receiver need not use it.

SET Secure Electronic Transactions

Example of SET transaction



SET Secure Electronic Transactions

The PDUs are defined in ASN.1 with DER-coding:

```
CardCInitReq ::= SEQUENCE {
    rrpid           RRPID,
    lid-EE          LocalID,
    chall-EE        Challenge,
    brandID         BrandID,
    thumbs          [0] EXPLICIT Thumbs OPTIONAL
}
```

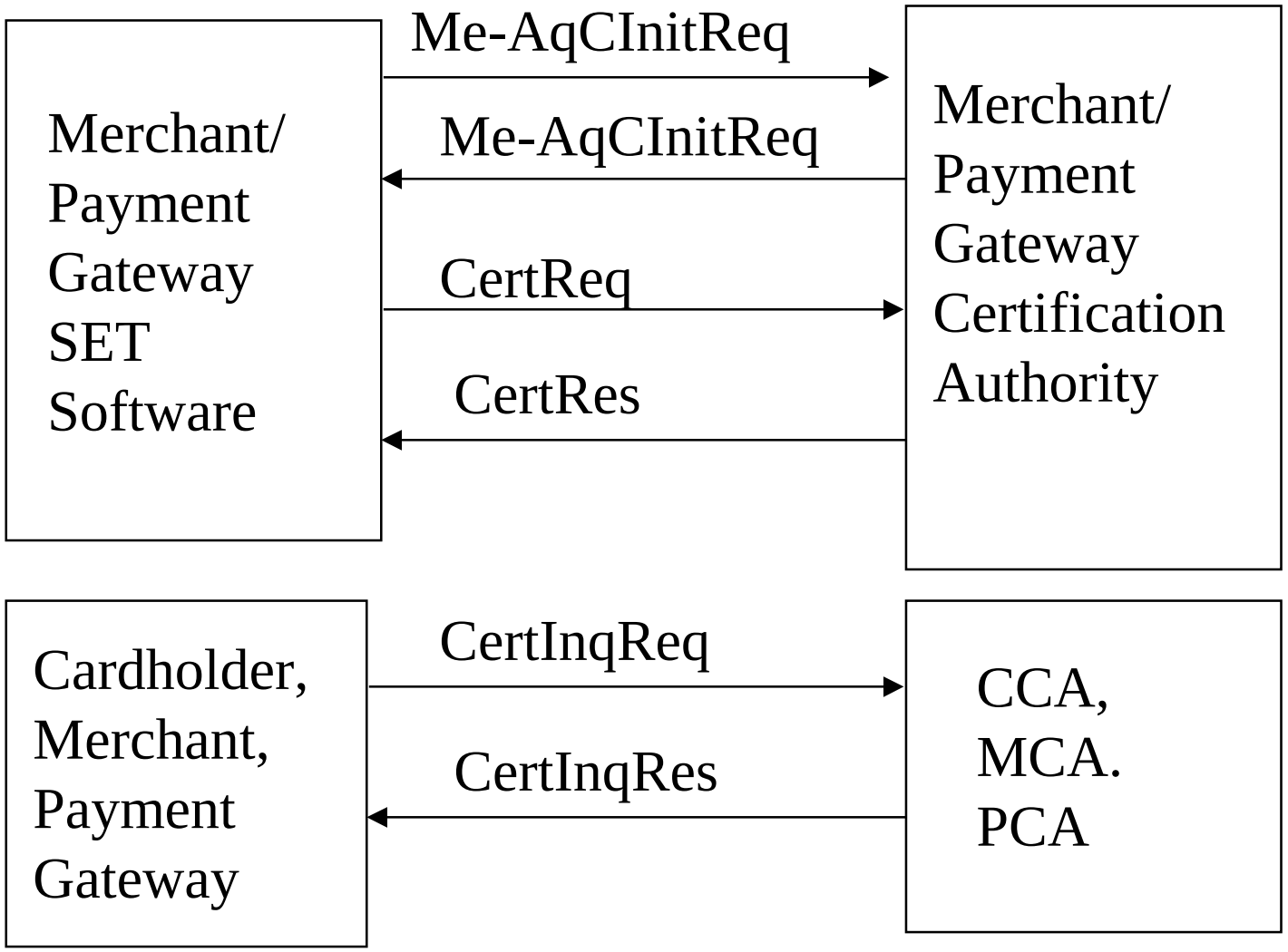
rrpid= request/response pair identification,

lid EE=local id. generated by cardholder’s software,

chall-EE=cardholder’s software challenge to CCA

SET Secure Electronic Transactions

- More SET transactions for certificates



SET Secure Electronic Transactions

- SET standards are in the tree {joint-iso-itu-t(2) internationalRA(23) set(42) }. SET-protocol is otherwise a typical OSI application protocol, similar to X.500, but lower level usage is not by OPERATION macro (ROSE) but more simply as

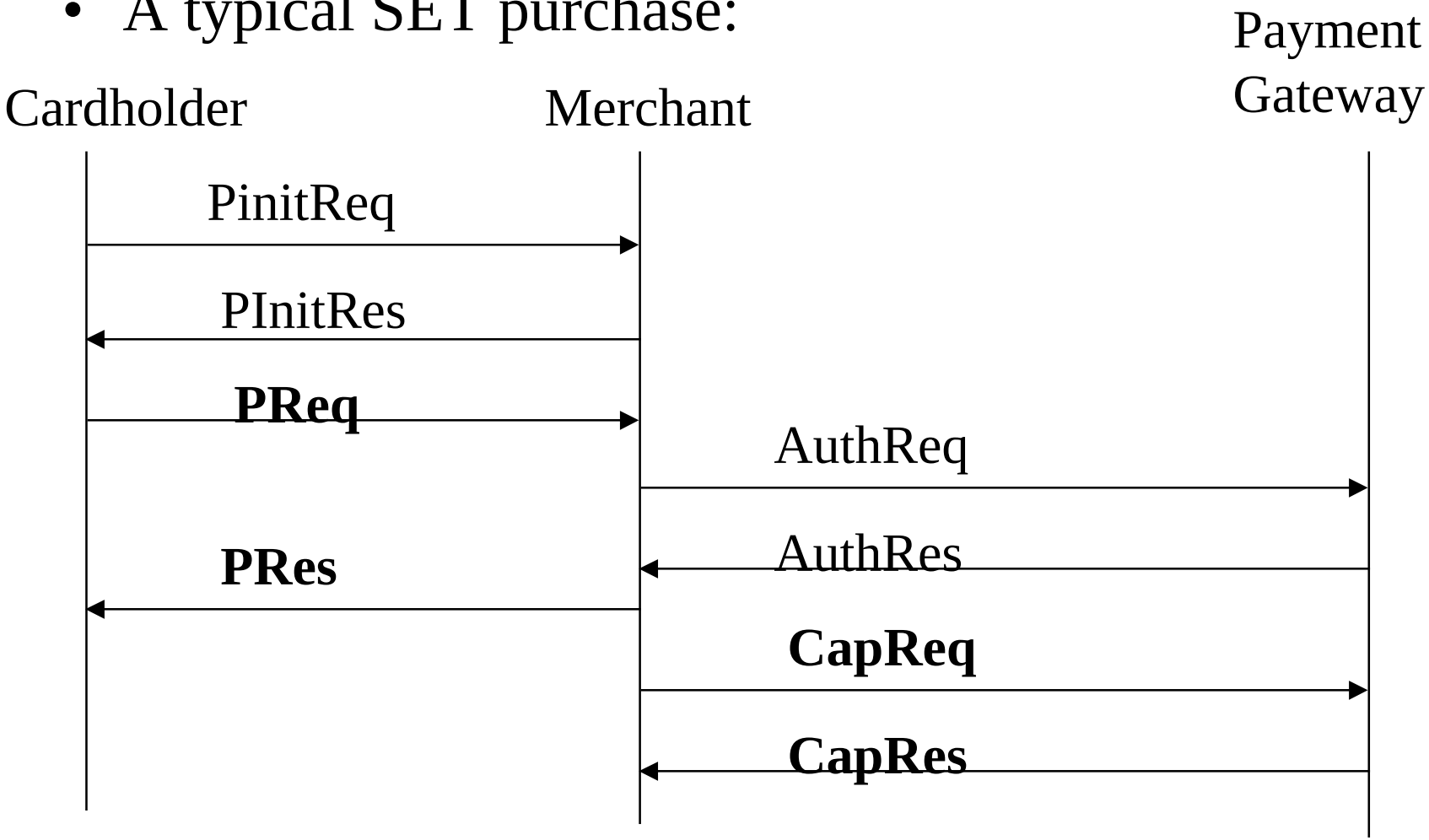
```
Message ::= CHOICE {
    ....
    certificateRequest [28] EXPLICIT CertReq,
    certificateResponse [29] EXPLICIT CertRes,
    ....
    error [999] EXPLICIT Error}
```

SET Secure Electronic Transactions

- Dropping OPERATION-macro means that automatic tools cannot be easily used for generating code for lower levels, but is natural as the usual protocol development method for TCP/IP uses no automatic tools for mapping application protocols on lower levels (simply code socket interface calls manually) .
- SET protocol is intended to run on HTTP. For protocol development this means manual gluing OSI application protocols inside TCP/IP PDUs.
- The negative effect may be that use of TTCN for testing is more difficult.

SET Secure Electronic Transactions

- A typical SET purchase:



Optional Message, regular font. **Mandatory Message, boldface**

SET Secure Electronic Transactions

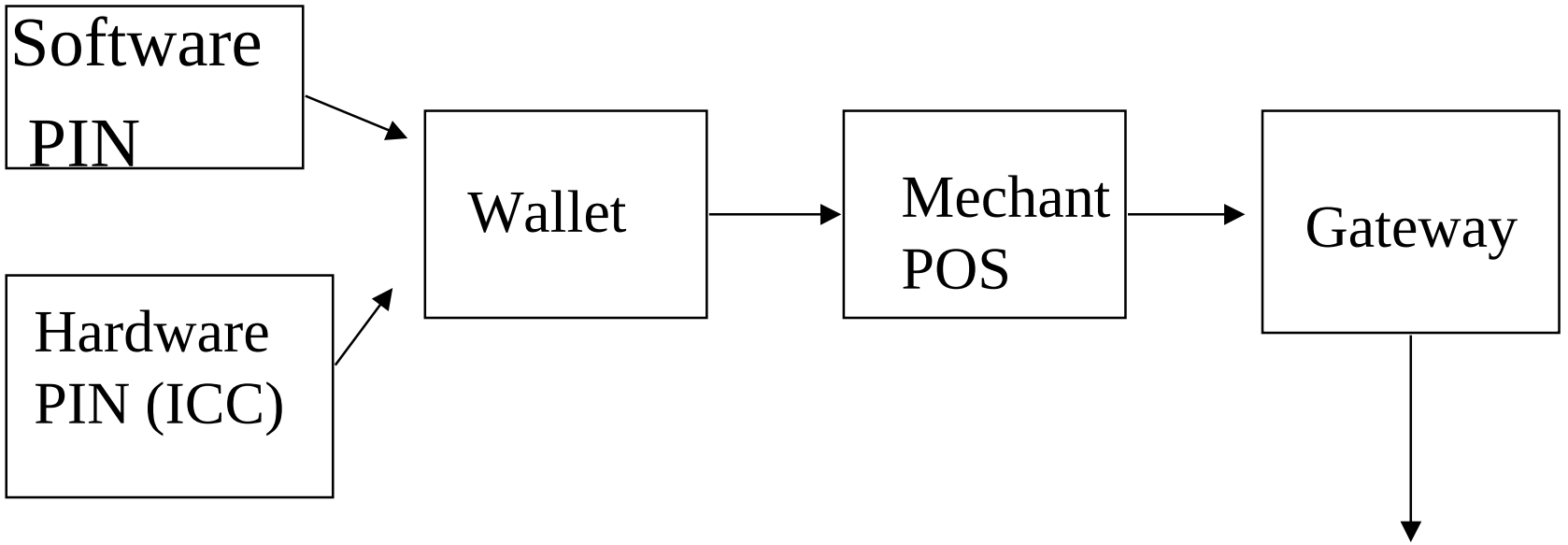
- A complete list of SET services will not be presented.
- It is enough to say, that there are quite many messages and the SET protocol is a typical OSI application protocol with remote operation type calls.The protocol entities are typical state machines as in OSI usually.
- Looking at the ASN.1 definitions it is a bit curious, that SIGNED SEQUENCE is not used in the messages, also error handing seems a bit ad hoc, but in general, seems a bit clumsy but OK.

SET Secure Electronic Transactions

- SET Extensions: Proposed additions to SET v1.0 protocol, this could be in SET v2.0, to be sure, you better check what is in SET v2.0 later.
- SET Debit Architecture: merchant and payments gateway should implement
  - PINs (Personal Identification Numbers)
  - Integrated Circuit Cards (smart cards) and security tokens
  - Elliptic Curve Cryptography (ECC)
- JPO Japanise Payment Options
  - enables Japanise customers use present methods

SET Secure Electronic Transactions

- Cardholder enters his PIN and it will be inserted to his PAData (information of the cardholders card data).



ICC has a small silicon microchip containing 8K to 16K bytes of data. ICC may be capable of generating RSA or ECDSA signatures. POS=point of sale

SET Secure Electronic Transactions

- SETCo
  - December 1997 Visa and MasterCard formed SET Secure Electronic Transactions LLC, known commonly as SETCo
  - SETCo is a membership organization with the parts:
  - SET Support Community
  - Technology Partners Group
  - General Partners
  - SETCo Board of Directors
  - You must pay fees to join this organization.

SET Secure Electronic Transactions

- SETCo owns the SET trademark SETMark.
- SET Compliance testing is arranged by SETCo, naturally, compliance testing is fairly expensive, about $50000. Included testing software (The Open Group's Test Environment Toolkit), technical support, license fees. Tests run through SET Checklist. You must retest every 6 months with the newest tools from SETCo.
- SETCo has permanent panels:
  - Business Panel, Technical Panel, Contingency Planning Panel, other nonpermanent panels.