Secure Payment

Vijay Atluri

Digital Currency- Characteristics

- Relies on IT and high speed communications networks to store, transmit and receive representations of value
- Relies on cryptography to provide security in open network environment
- Strives to reduce costs through economies of scale and technological advances
- Requires loading from funds held within the financial system

Electronic Payment Systems

- Token based
  - Use objects (tokens) that carry value and are based on prepayment
  - Categories
    - Electronic Cash: attempts to replace paper cash
      - DigiCash, Millicent
    - Electronic Purse:based on smart cards
      - MONDEX, CAFÉ
- Notational
  - transaction is tied to value stored elsewhere
    - electronic payment orders over the net
      - NetBill, NetCheque
    - credit card billing over the net
      - CyberCash, SET, First Virtual

Evaluation Aspects

- Transaction Cost
- Security
  - Authentication, message integrity, prevention of double spending, loss-tolerance, non-repudiation
- Privacy
  - Payment confidentiality, Payment anonymity, Payer untraceability
- On-line Verification
- Divisibility, Change-return Capability, Purse-to-purse transferability

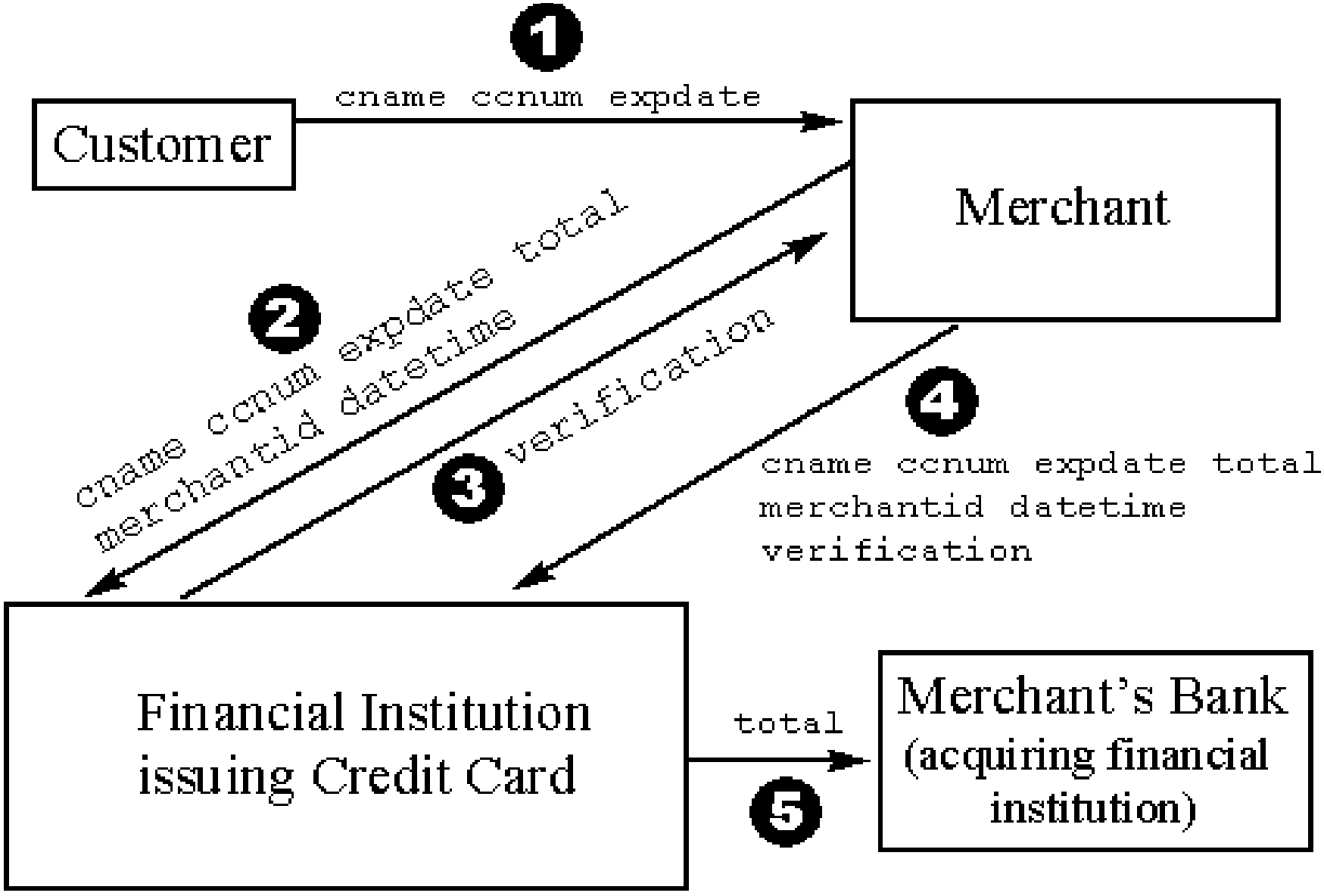
Micro/Mini payments

"Americans make more than 237 billion cash purchases totaling $600 billion each year, of this 84% is of purchases costing < $20."*

- Payment for low value payments on the Internet, e.g., intangible goods or online entertainment. Dealing with individuals selling goods
  - Micropayments (~< 15cents)
  - Minipayments ($.25 - $10.0)

    * According to MsterCard
- Issues include
  - A cost effective and scaleable system that is a simple and secure (protects privacy of transactions).
  - Cost of setting up accounting and billing procedures are minimal ?
  - Low overhead- Managing and consolidating microdebts

Conventional Credit Card Transactions



E-Payment Systems - Outline

- CyberCash
  - Merchant side services
  - Customer side services
    - CyberCoin Wallet
    - InstaBuy
- Mondex Electronic Cash
- Millicent
- DigiCash - CAFE and Smartcards
- DigiCash - eCash
- First Virtual
- NetBill
- S/MIME
- SSL
- SET
- Microsoft Wallet
- VeriFone

CyberCash Credit Services

- CyberCash is one of the leading innovators in e-money technologies. Offers a wide array of products and services (See www.cybercash.com)
- Merchant side services
  - One CyberCash service called Credit Services facilitates payment over the Internet.
  - Essentially an analog to the physical world credit card transaction
  - Anatomy of a Credit Card transaction
    - Two parts
      - The Authorization
      - The Capture

The Authorization

- Is the Customer's card authorized to charge the amount?
  An encrypted message (cname, ccnumber, expdate, total) sent between the Merchant and the Customer's credit card issuing financial institution.
  - The CyberCash "CashRegister" software is used to facilitate this.
  - Possible responses:
    - Approval
    - Decline
    - Referral -- response pending more information, call card issuer for assistance

The Capture

- Settlement of the charge
  - The sale amount is credited to the merchant's deposit account through their acquiring financial institution (that issued the card)
  - The sale amount is also posted to the cardholder's credit card account
- Two possibilities
  - Terminal capture - the authorized transactions are stored within the CyberCash CashRegister until the merchant batches them and submits them for capture.
  - Host capture- the authorized transactions are stored at the acquiring financial institutions or third party Processor's 'host' computer awaiting capture.

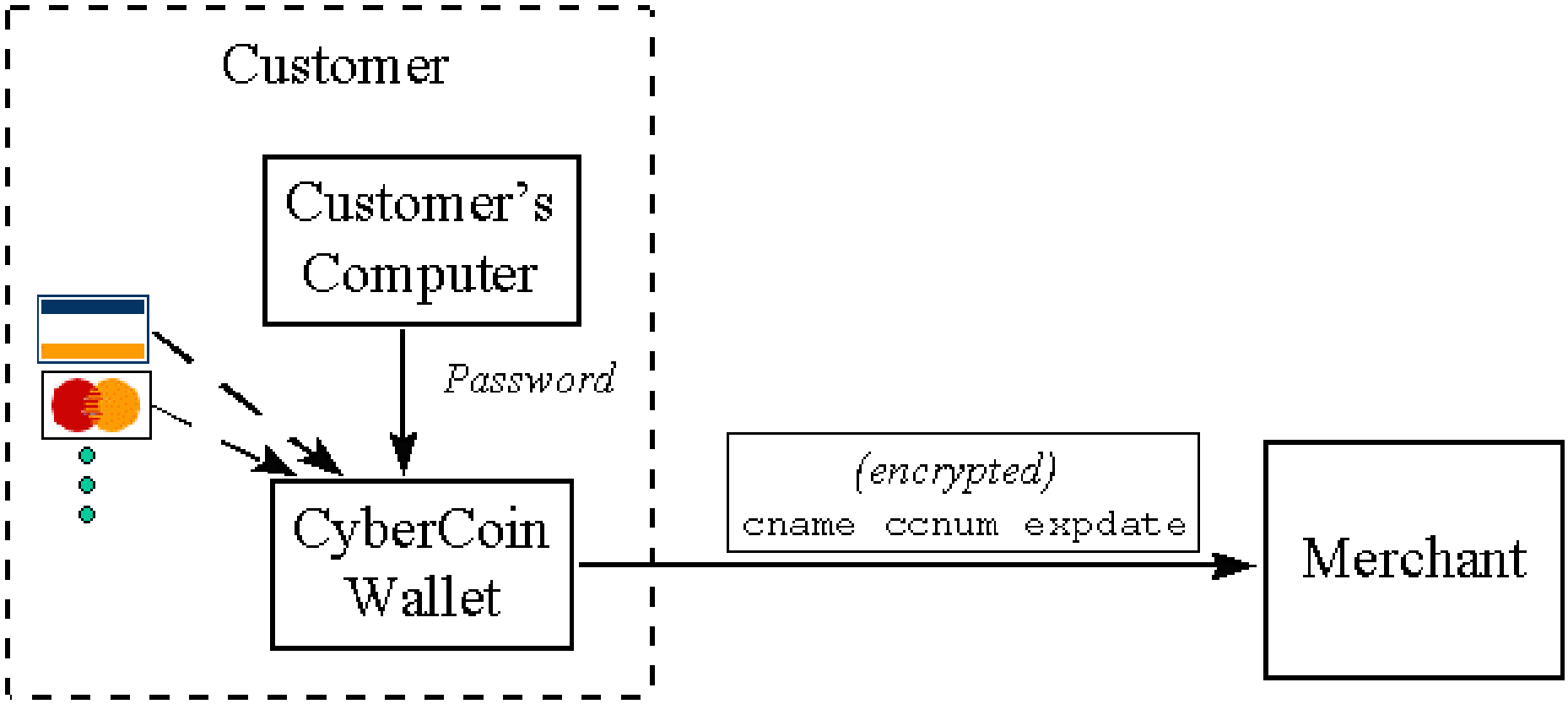
CyberCash Credit Services - Charges

- For a Merchant to establish and maintain a CyberCash Credit Services account, the charges are as follows (as of April, 1999 from the CyberCash web site):
  One-time Service Set-up fee ranging from $500 to $1,000
  Monthly service fees (a service access fee and transaction fees based on transaction volume) of $40 to $80, and/or $0.20 to $0.60 per transaction fees.
- This is in addition to any monthly service fees or per transaction fees charged to the Merchant by their Acquiring Financial Institution.

Customer Side Services

- CyberCash CyberCoin Wallet
- The Wallet is a client application that stores a Customer's traditional credit card information in an encrypted file - stored on the user's computer hard disk.
- A Wallet can contain several different credit cards.
- To initiate a purchase
  - The Wallet application is accessed and the credit card information is selected after the Customer supplies a password.
  - The selected credit card information is then transmitted in an encrypted message to the Merchant where authorization and capture can take place.
- Major limitations to this version of the Wallet
  - It is stored locally on the user's PC. A user must have a PC in the first place, and must use it for purchases.
  - Leaves the user's PC vulnerable to attack. e.g., attack the Wallet file...

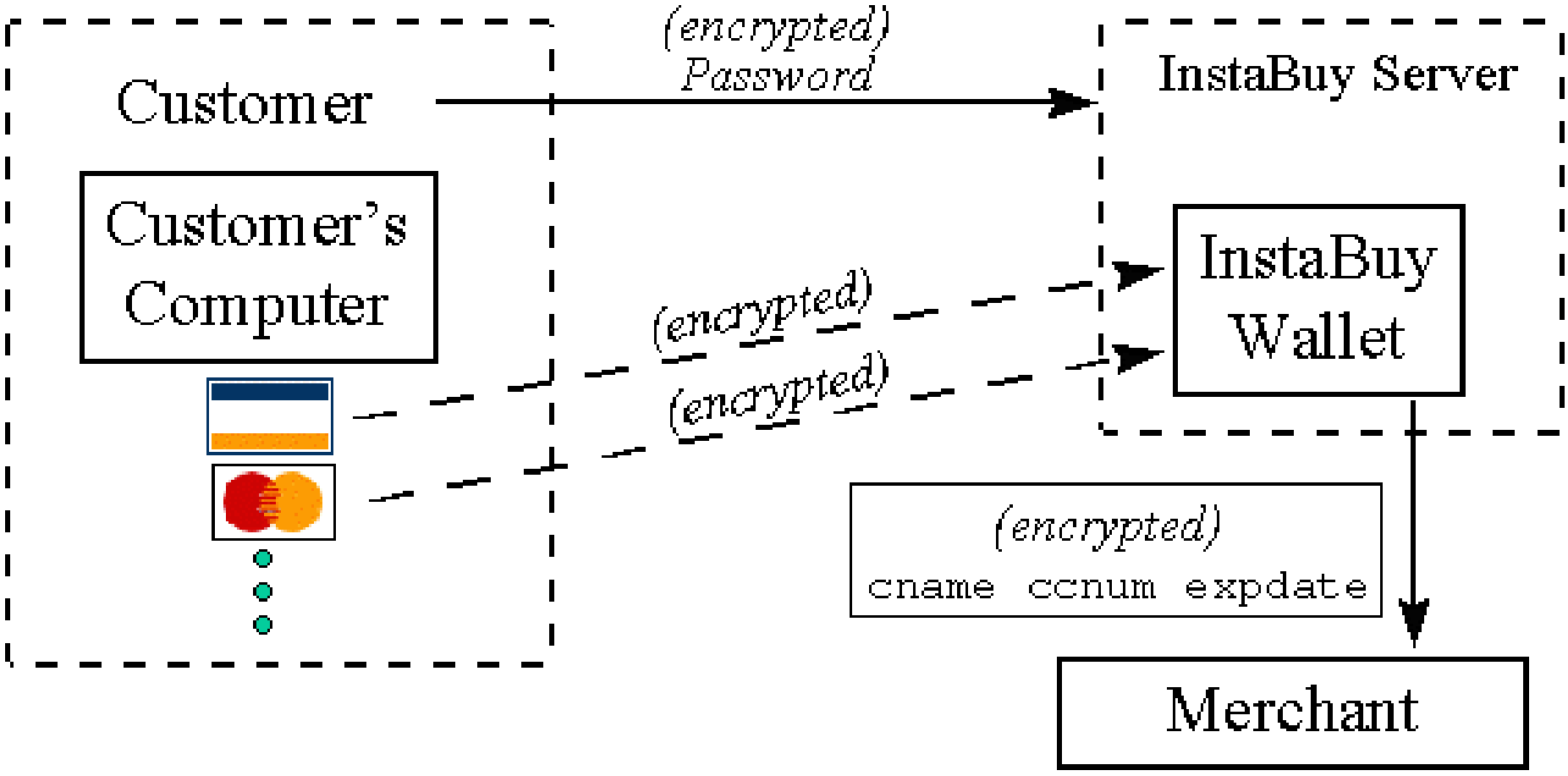
CyberCoin Wallet



Customer Side Services - InstaBuy
(www.instabay.com)

- Essentially places the Wallet in a secure on-line server.
  - [Analogy: HotMail (www.hotmail.com) stores your e-mail in an on-line server that can be accessed from any computer that has a web browser and access to the Internet].
- Customer stores credit card information in the InstaBuy server--all exchanges take place using encrypted communications such as SSL
- To initiate a purchase
  - the Customer "unlocks" their InstaBuy wallet using their password, and selects a credit card.
- Limitation. If wallet server is compromised, Customer's credit cards info can be stolen.

InstaBuy


Customer
Customer's Computer
(encrypted) Password
InstaBuy Server
InstaBuy Wallet
(encrypted)
(encrypted)
(encrypted)
cname ccnum expdate
Merchant

Mondex Electronic Cash

- Is an electronic cash scheme that uses smart card technology
- Similar to the NYC Metrocard
- Electronic cash value is stored on a microchip
  - Value can be added and then deducted using special readers
- Mondex International Ltd. is a subsidiary of MasterCard International

Mondex Electronic Cash (Cont'd)

- A variety of Mondex enabled appliances are envisioned:
  - Balance device - displays the current balance (value stored in the card).
  - Telephones, vending machines, etc. with Mondex card slot - ability to deduct value from the card
  - Point of Sale terminals with Mondex card slot - deducts purchase amount from the card
  - Mondex ATM machine - transfers value from bank account to card
  - Mondex Wallet - device like a calculator with 2 Mondex card slots. Can be used to transfer value from one card to another.
  - Device to attach to PC - makes on-line purchases using Mondex card in this device

Mondex Electronic Cash (Cont'd)

- Advantages:
  - Card value can be represented in any currency - can be used to make purchases internationally
  - Easy to add value to the card at ATM machines
  - More secure than cash since card can be protected with PIN
  - Lower per-transaction cost than credit or debit cards since value transfer takes place locally (just like cash). Good for mini/micropayments
  - Anonymity - no audit record kept, just like cash
- Disadvantages:
  - Until Mondex enabled appliances become ubiquitous
  - Like cash, if Mondex card is lost, you loose your money

Millicent - MicroPayments

- Micropayments - transactions value < $0.25
- What costs that much - examples
  - Phone call (Internet phone call), Newspaper (selected articles), Stock quote, Clip art, Pay per view access to a web page, video, music, etc.
- Need to enure: costs related to processing a transaction has to be less than what the payment is.
- Costs include:
  - Processing Costs - Computer time, disk space, communications, etc.
  - Accounting Costs - Costs for Merchant to track payments
  - Credit Risks - Insurance, security, etc.

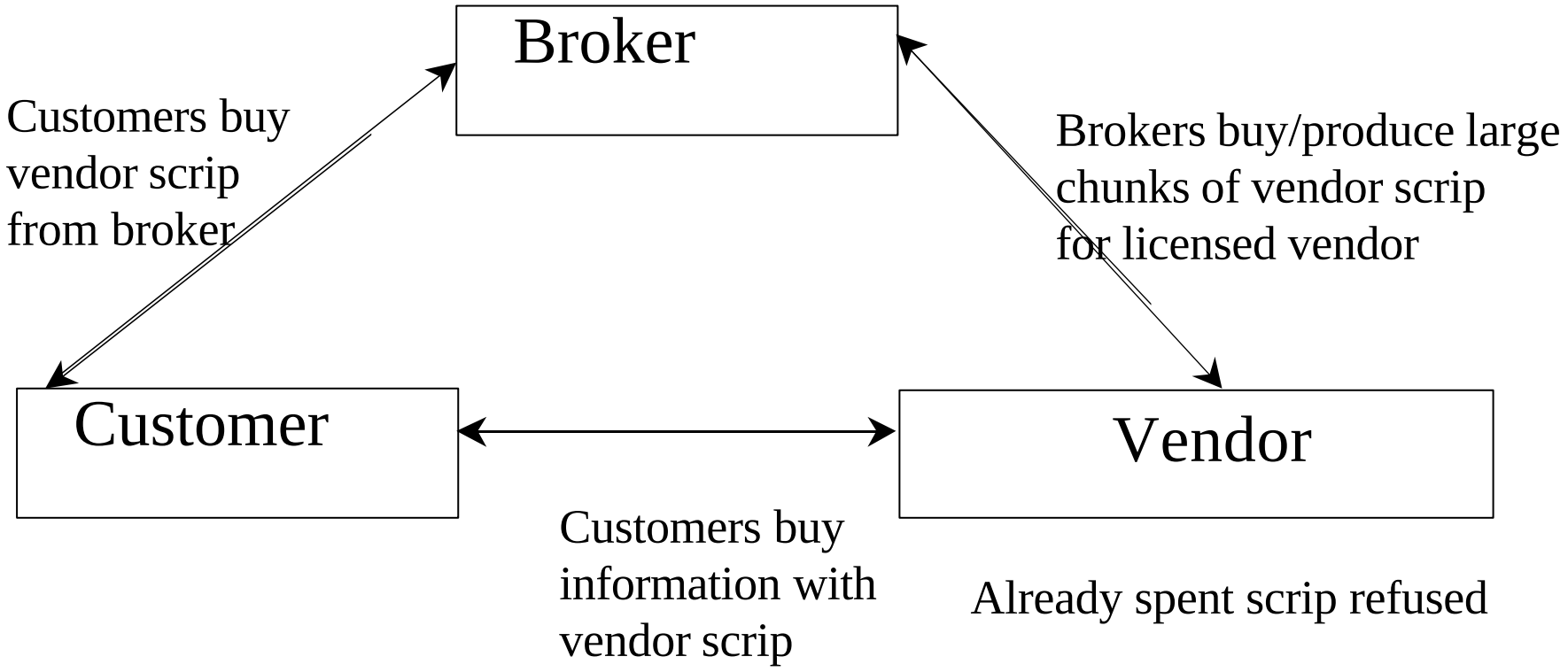
Millicent System

- Developed by Digital Corp.
- Based on scrip broker model
  - overcomes traditional scrip model's requirement of having vendors and consumers to have prior relationships before transacting
  - Components
    - Scrip broker - Sells scrip (credit) to Customers in exchange for cash
    - Customer - Purchases scrip from a Broker. Scrip value is stored locally with Customer
    - Vendor (Merchant) - Sells a license to Broker (in exchange for cash) to generate a specific kind of scrip (the vendor's scrip) that can be used by the Customer to exchange for goods and services
    - Scrip - like a coupon with a specific value - can only be redeemed with a specific vendor. Can be exchanged (through a broker) for scrip from a different vendor.

Millicent System

- Its operation-A broker, e.g., a bank accepts payments from, and issues its own scrip to, a consumer. The broker then scrips credits from vendors.
- Results in- each consumer has one account with a broker and each vendor has an account with a few brokers
- Provides “adequate” security by employing an encryption scheme with low computational requirements(costs more to break the protocol than value of the scrip) ======>High potential for fraud

Millicent System



Millicent Software

- 3 main software components that implement the Millicent model
  - The MilliCent Wallet - used to buy and hold broker scrip, convert back and forth to vendor scrip as needed, and spend it in exchange for goods & services.
  - MilliCent Broker Server - converts real money into scrip, and converts between different forms of scrip used by different vendors
  - MilliCent Vendor Server - administers content pricing, and validates scrip used for payment.

Millicent - Advantages

- Scrip can be issued at any value from a few cents to many $$
- Customer purchases Scrip in one large transaction- would benefit from a volume discount. Thus keeping per (scrip) transaction costs low
- Anonymity
  - No receipt is given for goods or services and no user authentication is necessary
- From the Millicent web site:
  - The broker knows the identity of the customer, but does not know what the customer purchases
  - The vendor knows what is purchased, but does not know the identity of the customer

Millicent - Advantages (Cont'd)

- Fraud is minimized (or at least localized) since each vendor has their own scrip and the value of individual scrip is low.
- Broker fraud is minimized because:
  - Customer and vendor software can independently check scrip and maintain account balances, so broker fraud can be detected
  - The good reputation of a broker is important for attracting customers, and that reputation would be lost if customers have trouble with the broker.
  - Customers do not hold much scrip at any one time, so a broker would have to commit many fraudulent transactions to make a significant gain, and that makes it more likely that the broker would be caught.

Millicent Limitations

- Much trust is put in the Broker. However, with many Brokers to choose from (and the speed of negative news on the Internet) bad Brokers won't stay in business long.

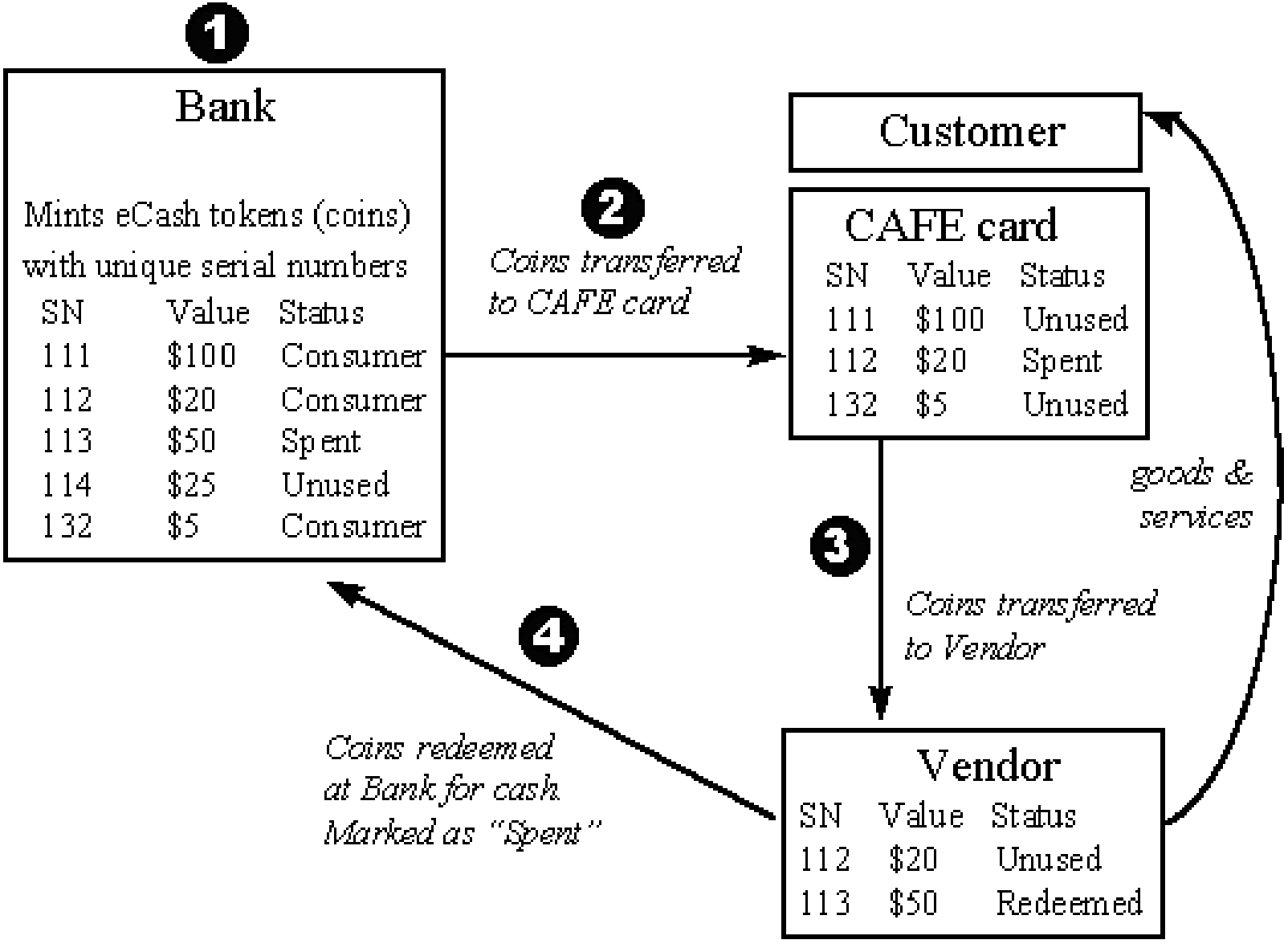
DigiCash - CAFE and Smartcards

- CAFE - Conditional Access For Europe
- Three uses:
  - 1.Consumer payments
  - 2.Access to information services
  - 3.Identification
- Proposed device is more like a small calculator than a credit card.
- Seems to be geared more towards physical store transactions rather than on-line payments.
- Card will store value like Mondex, however, each transaction will be logged allowing for reimbursement if card malfunctions or is lost.
- Special "Guardian" processor chip that keeps track of each "coin" spent

DigiCash - CAFE and Smartcards

- All monetary units ("coins") have a serial number
  Each transaction records the serial numbers
  - prevents double spending of coins
- During a transaction, the monetary units (coins) are transferred from the device to the merchant's system and marked as "spent" in the device.
- The merchant must then redeem these coins with a financial institution in order to realize their value.
- CAFE prototype project was finished in Feb. 1996
  new work was being continued in a project called OPERA
  http://www.digicash.com/projects/opera/

DigiCash - CAFE and Smartcards



DigiCash - CAFE and Smartcards

- CAFE prototype project was finished in Feb. 1996
  new work was being continued in a project called OPERA
  http://www.digicash.com/projects/opera/
- DigiCash has more projects involved with smart cards including:
  - SOSCARD - Secure Operating System Smart Card
  - CRISP - Cryptographic Reduced Instruction Set Processor Smartcard
  - BLUE - latest smartcard technology that includes a variety of cryptography capabilities
    http://www.digicash.com/smartcards/blue/

DigiCash - eCash

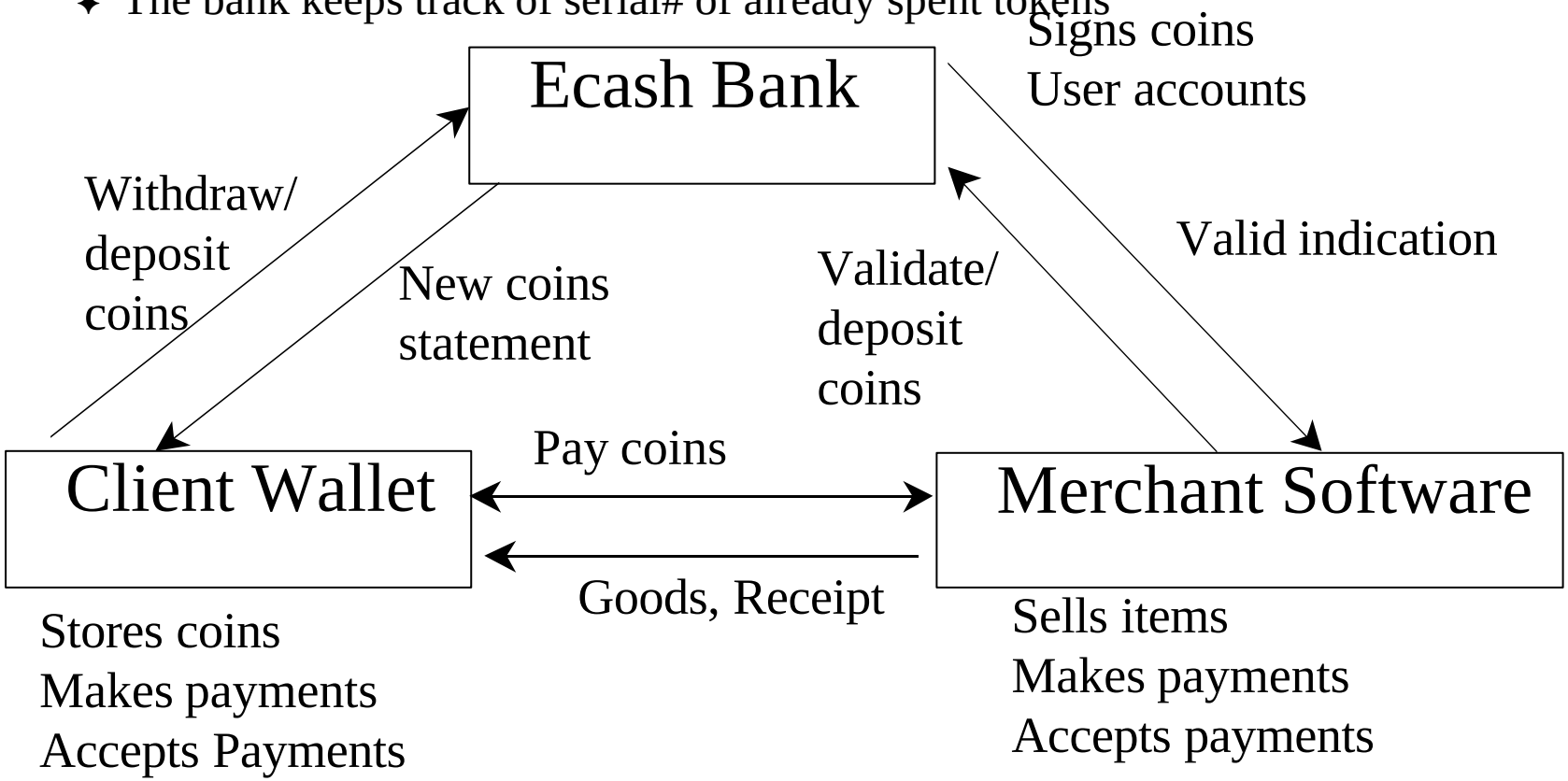
- A bearer certificate that is developed by DigiCash
- eCash are coins or *tokens* that represent some value
- Each token is a sequence of numbers that securely encode the representative value
- The players:
  - Issuing Bank - a bank that accepts payment (in whichever local currency) in exchange for eCash coins
    Issuing banks can also accept eCash coins and return the equivalent cash in the local currency
    Finally, banks also verify eCash coins so they are not double-spent
  - Customer/consumer - Has an account at the issuing bank and uses eCash "Purse" software to affect withdraw of eCash coins and spending of eCash with Merchants
    A consumer must have a valid account with an Issuing bank
  - Merchants - Accept eCash from customers, check their validity with a bank and then redeem eCash coins for real cash

DigiCash - eCash

- Issuing an eCash coin is accomplished with the following process:
  - 1 The eCash purse software generates coins of various denominations
    e.g., Alice decides she would like to have eCash coins in $50, $20, $10, $5 and $1 denominations
    Each coin is given a random number (typically 100 digits in length)
    Each coin is encrypted using the customer's public key
  - 2.Each coin is then sent to the Issuing bank where a *blind signature* is placed on it.
    e.g., $50 will be deducted from Alice's bank account and a "$50 signature" will be stamped on the coin by the bank
    The signature will include a sequence number (id) that the bank generates
    This allows the bank to recognize the its signature in the future, without knowing who actually is spending the coin.
    The bank records this information in a local database.
  - 3.The signed coins are returned to the consumer and stored in the eCash purse for future use.

DigiCash - eCash

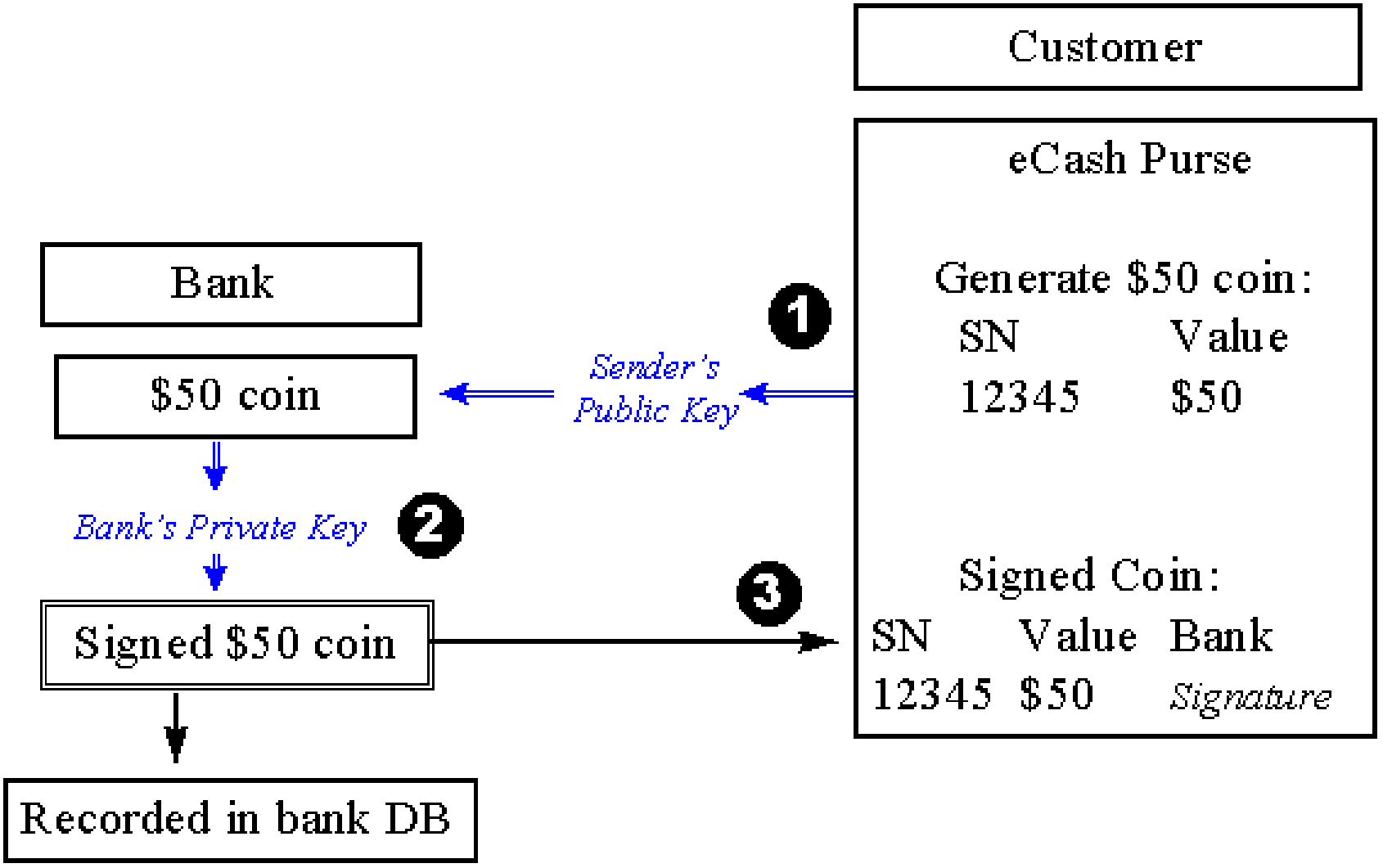
- Its operation-
  - A consumer issues, using DigiCash purse SW, blank tokens and sends them to the bank for certification
  - Bank certifies tokens, debits consumer's account and send back consumer
  - Before accepting a token, a vendor receives first the bank verification that this token has not been spent
  - The bank keeps track of serial# of already spent tokens



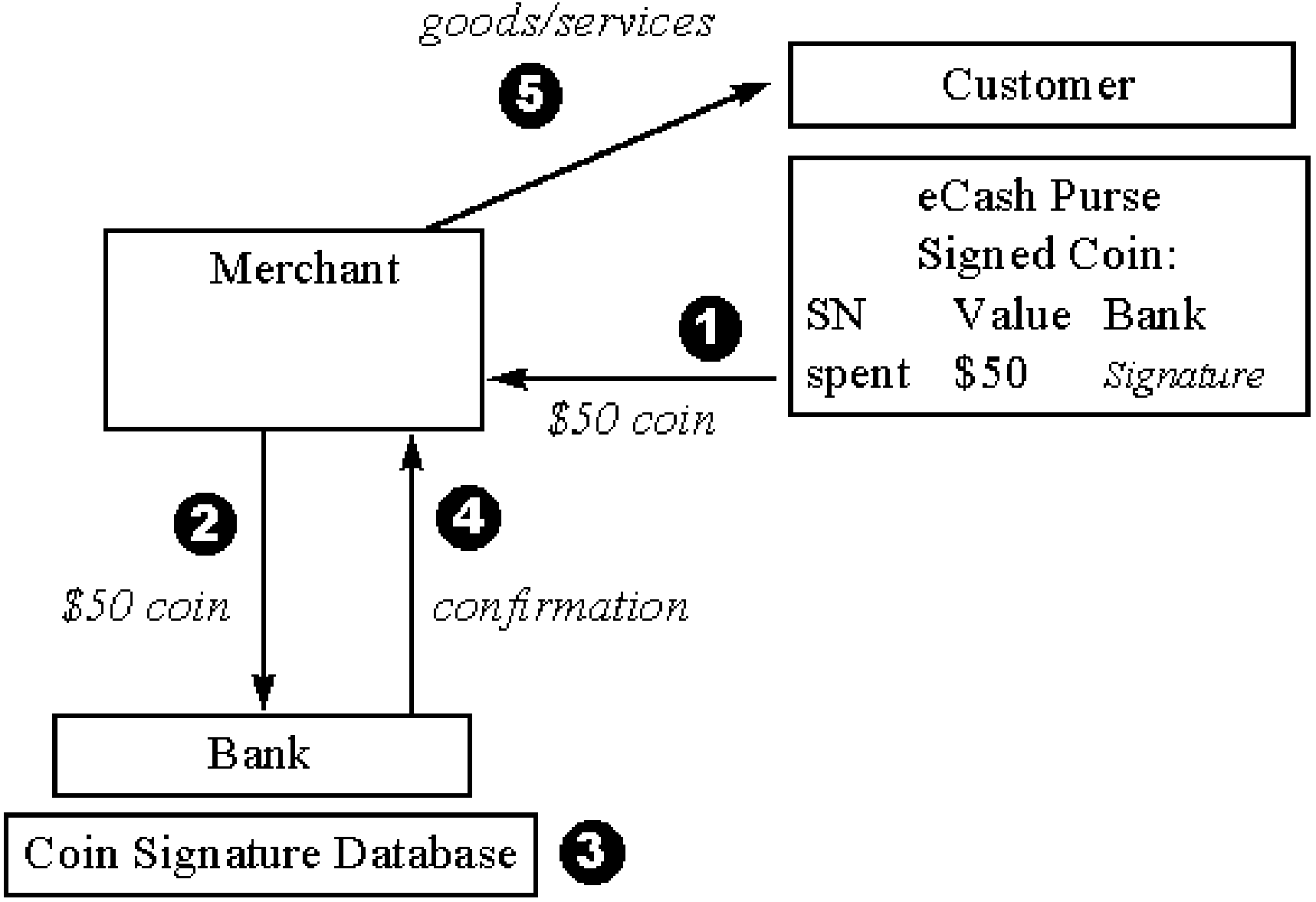
DigiCash - eCash

- Spending an eCash coin is accomplished with the following process:
  - 1.Merchant requests payment - if customer agrees, then eCash coins are selected and "removed" from the eCash purse by invalidating their serial numbers.
    Each coin is then sent to the Merchant.
  - 2.The merchant forwards the coins to the bank to see if they have been spent before.
  - 3.The bank looks up the coin's signature in its database and informs the merchant if the coins are valid.
  - 4.If the coins are valid, the merchant is given a confirmation notice and the cash value is transferred to the Merchant's bank account.
    The bank will then invalidate the signature of the coin in the database to prevent it from being spent again.
  - 5.Good or services are then provided to the customer.

DigiCash - eCash



DigiCash - eCash



Secure exchanges

- Buyer generates the note number n, picks the a random number r and sends $x=nr^e$ where e is bank's public key to certify a certain amount of money (say $10)
- Bank withdraws $10 from buyers account and uses its private key d for certifying the $10 note. The certification $y = x^d = (nr^e)^d = n^d r^{ed} = n^d r$. Bank sends y to buyer
- Buyer computes $z = y/r = n^d$
- To buy, buyer sends z to the merchant
- Merchant sends z to the bank, also computes $z^e = n$
- Bank also computes $z^e = n$ and records n to avoid double spending

DigiCash - eCash

- Privacy is its distinct feature- based on the notion: a bank issuing a token should not have to know which consumer receives which tokens.
- Limitations- Online verification of token could be a problem
- DigiCash claims (via their web page, April, 1999) the following banks are presently issuing eCash:
  Deutsche Bank (Germany)
  Swiss NetPay AG (Switzerland)
  EUnet (Finland)
  St.George (Australia)
  Den norske Bank (Norway)
  Bank Austria (Austria)
- Several trials were conducted with these banks throughout 1997 and 1998

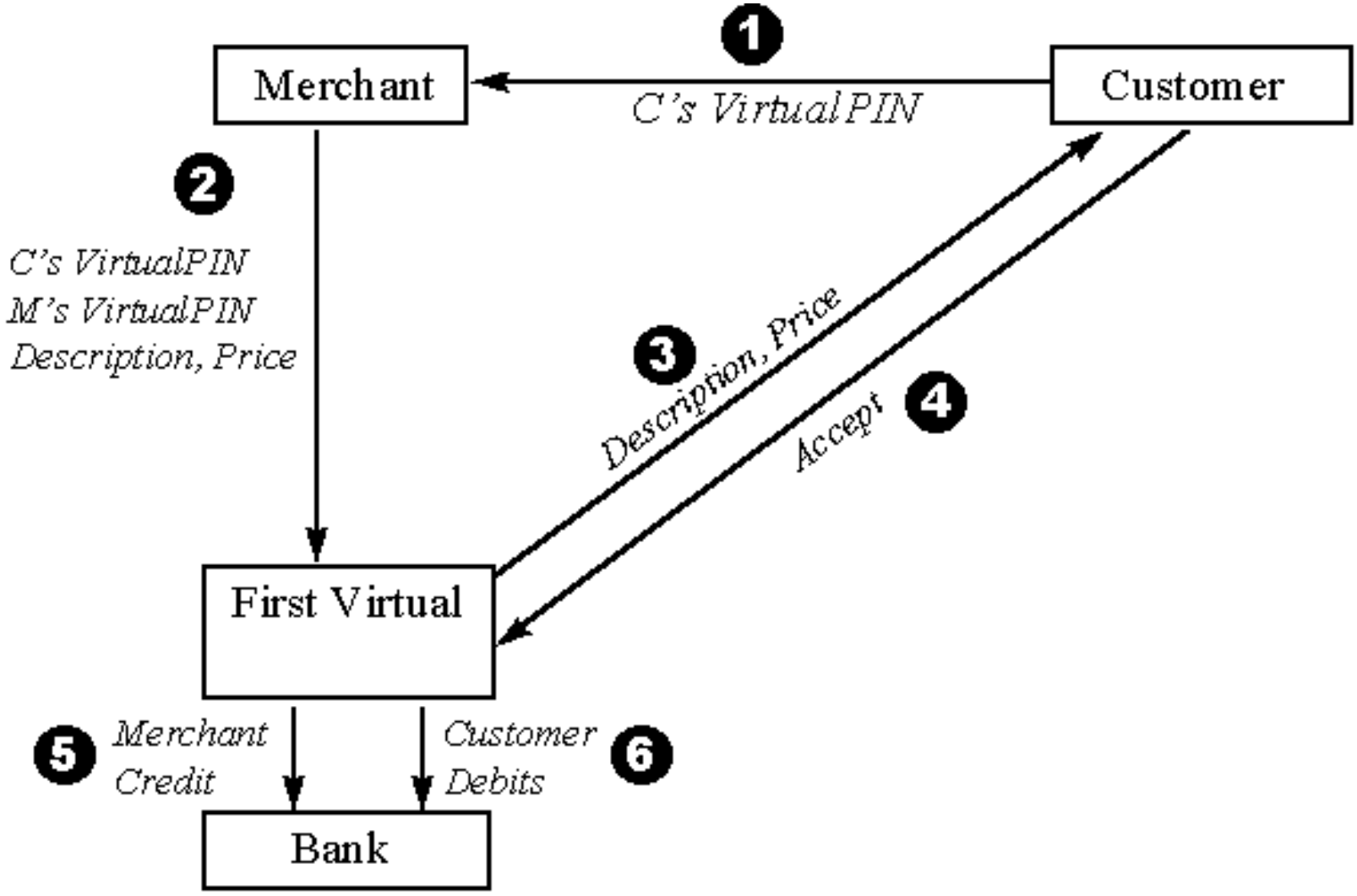
First Virtual

- Main idea behind FV is to use e-mail as a means to purchase low valued items (a few cents).
- A FV *account* has the following information:
  - An associated email address.
  - A state (one of active, seller-only, suspended, or invalid).
  - An associated real-world account, along with
    a) a method to transfer funds from the real-world account to the First Virtual account
    b) a method to transfer funds from the First Virtual account to the real-world account.
    c) A predefined currency for funds transfer.
  - All of this is associated with a *VirtualPIN*

First Virtual

- To make a purchase:
  - 1.To initiate a purchase, the Customer sends their VirtualPIN to the Merchant
  - 2.The Merchant sends the Customer's VirtualPIN, the Merchant's VirtualPIN and the description and Price of the transaction.
  - 3.FirstVirtual sends an e-mail to the Customer asking for confirmation
  - 4.The Customer sends confirmation back to First Virtual:
    Accept - Customer accepts the transaction and will pay
    Decline - Customer will not pay for the transaction
    Fraud - The Customer suspects fraud (e.g., VirtualPIN was used by someone else)
  - 5.First Virtual then accumulates Merchant transactions and credits their bank accounts
  - 6.First Virtual also accumulates Customer transactions and charges their credit cards each month

First Virtual



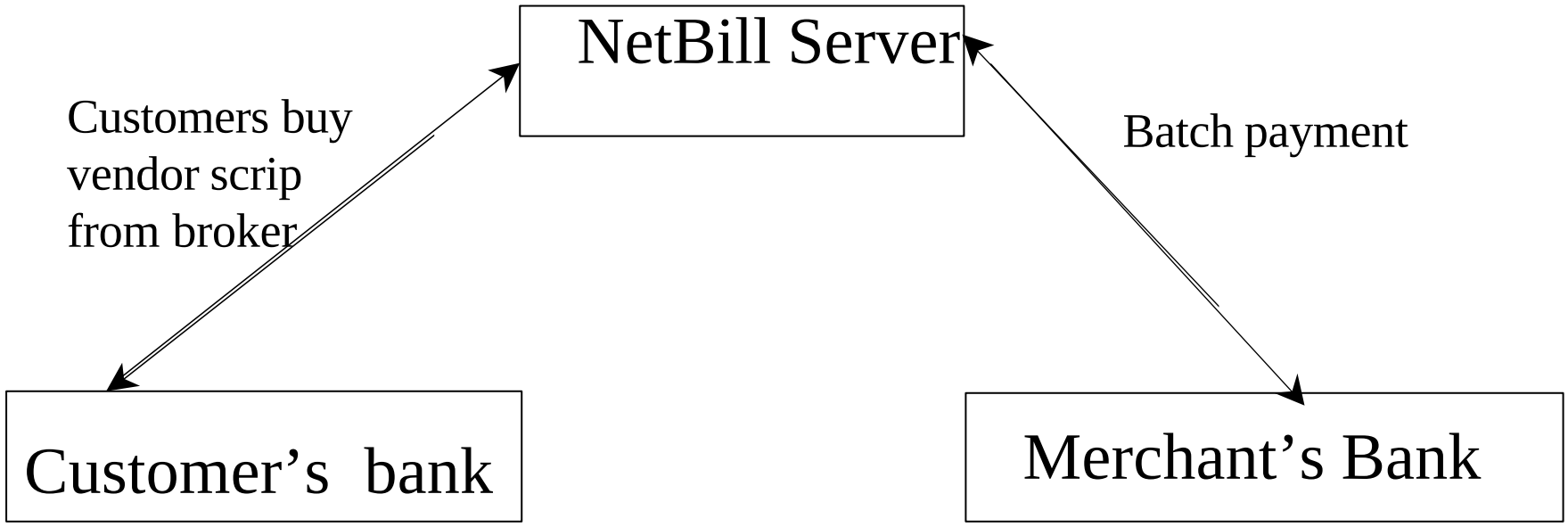
First Virtual

- Since many small transactions are aggregated and only processed monthly, transaction overhead is reduced.
- So this is a good method for microcommerce
- A Customer does not have to Accept a transaction, even if they have already received good or services from the Merchant However, if they do this too often, their VirtualPIN will be suspended
- If a VirtualPIN is stolen, a Customer can reply "Fraud"
- FV is no longer in this line of business

NetBill

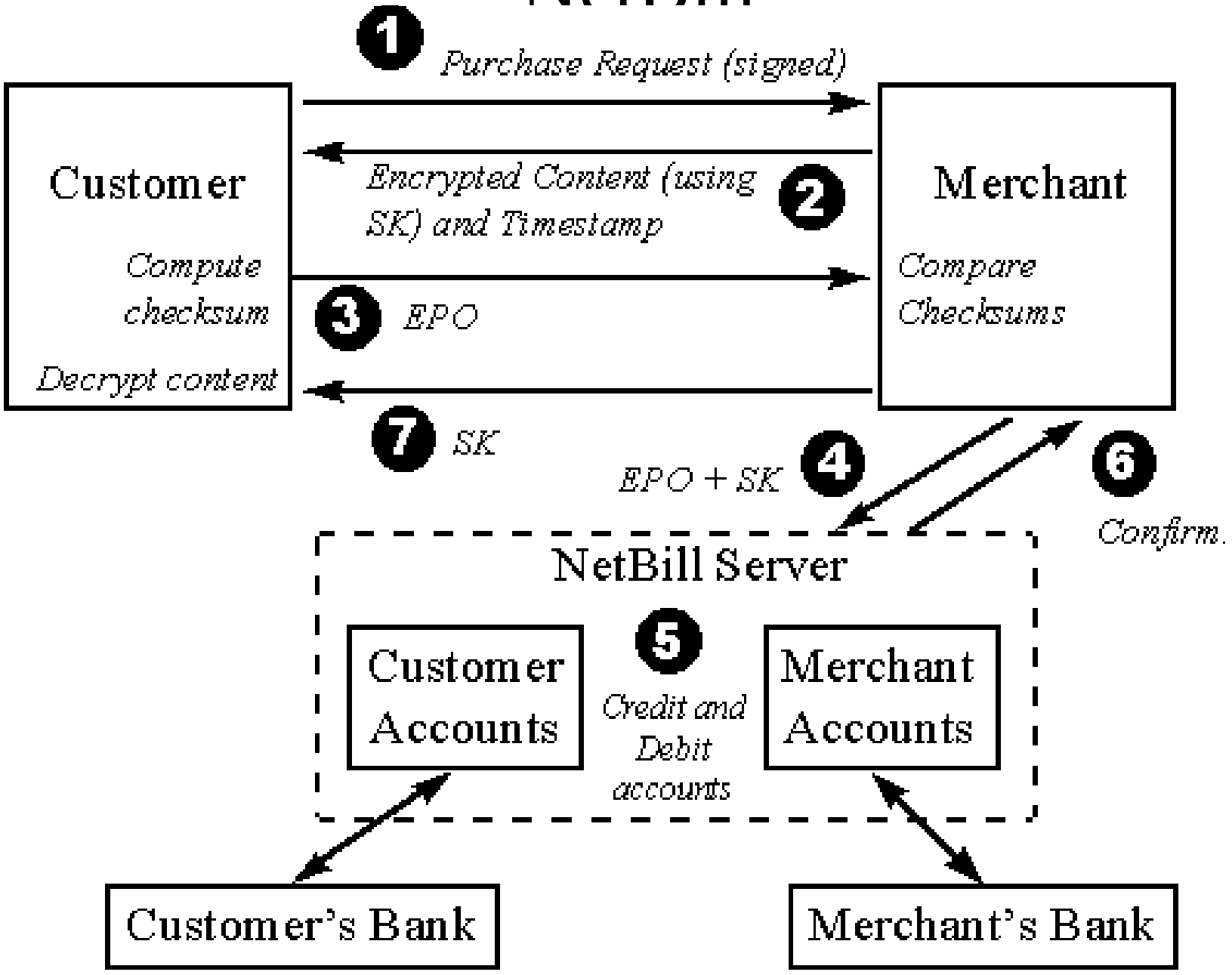
- NetBill is directed at *delivering* and *charging for* digital products and services
- Originally started as a research project at Carnegie-Mellon Univ.
- Purchases are handled through an Electronic Payment Order (EPO)
- NetBill is currently in an early trial stage. You may open an account and receive 1,000 free BiblioBucks to spend...
- The players:
  - Consumer: Orders content (documents, movies, etc.) on-line. Guaranteed receipt of content
  - Merchant: Provides on-line content. Charges for downloading encrypted version of content.
  - NetBill server: Verifies Consumer's NetBill account has sufficient funds and transfers payment to Merchant's account.
    NetBill also acts as CA for Customers and Merchants
- Both Customers and Merchants must establish an account with the NetBill server.
- Such an account is backed by a financial institution.
- A Customer then receives some credits in their NetBill account by debiting their bank account

NetBill


NetBill Server
Customers buy
vendor scrip
from broker
Batch payment
Customer’s bank
Merchant’s Bank

- A typical purchase transaction proceeds as follows:
  - 1.The customer places a Purchase Request with the Merchant.
    This can be an order for some software, an electronic book, etc.
    This request is signed by the Customer's digital signature.
  - 2.The Merchant encrypts the content with a secret key (SK), calculates a *checksum* on the results, and delivers it to the Customer along with a timestamp.
  - 3.The Customer computes the checksum on what was received.
    The Customer gathers the checksum, accepted price, product identifier and timestamp (called the electronic payment order, or **EPO**) and sends this back to the Merchant.
  - 4.The Merchant then compares the checksum of what was sent, with the original checksum.
    If the checksums match, then the Merchant is assured the Customer has received the content in tact.
    The Merchant takes the EPO, includes the secret key (SK) and forwards all of this to the NetBill server.
    This is signed with the Merchant's Private key
  - 5.The NetBill server reads the EPO and checks the Customer's NetBill account to see that they have enough to cover the price.
    If so, then the Customer's NetBill account is debited, the Merchant's NetBill account is credited and the secret key (SK) is stored along with a log of the transaction.
  - 6.The NetBill server then sends a confirmation to the Merchant.
  - 7.Finally, the Merchant, after receiving the confirmation from NetBill, forwards the secret key (SK) to the Customer so they can decrypt the content.

NetBill


1
Purchase Request (signed)
Customer
Merchant
Encrypted Content (using SK) and Timestamp
2
Compute checksum
Compare Checksums
3
EPO
Decrypt content
7
SK
EPO + SK
4
6
Confirm.
NetBill Server
5
Customer Accounts
Credit and Debit accounts
Merchant Accounts
Customer's Bank
Merchant's Bank

NetBill

- Periodically, Merchant can "cash in" on their NetBill account.
- Clearly, NetBill assumes communications resources are inexpensive.
- Systems gracefully handles failures:
  - If Merchant server goes down after EPO is sent, then NetBill can supply SK to customer
  - If content is not delivered completely, Merchant can re-send
  - If Customer does not have enough in their NetBill account, an error message can be returned
- System as described is not anonymous. NetBill knows all...
- Future versions of NetBill may hide actual content from NetBill...

Secure Payment Protocols

- Secure Socket Layer (SSL)
- Secure Multipurpose Internet Mail Extension (S/MIME)
- Secure Electronic Transaction (SET)

SSL (Secure Socket layer)

- a standard security approach for World Wide Web browsers and servers on the Internet
  - based on TCP/IP protocol: work with ftp, http, etc.
  - RSA public key cryptography
  - data encryption,
  - server authentication (Digest),
  - message integrity (MAC), and
  - optional client authentication.

S/MIME

- De facto standard for secure electronic messaging - endorsed from lotus , Microsoft, Netscape and Qualcomm.
- Can be used for
  - Secure e-mail,
  - EDI,
  - EC on line ordering services
  - Medical record transport for healthcare application
  - Secure Messaging for Legal Applications

S/MIME

- Enterprise-ready, open standards-based email security
- low-cost email security solution from RSA
- message privacy : confidentiality
- digital signatures : authentication
- tamper detection : uses a secure hashing function to detect message tampering (integrity).

Netscape Messenger

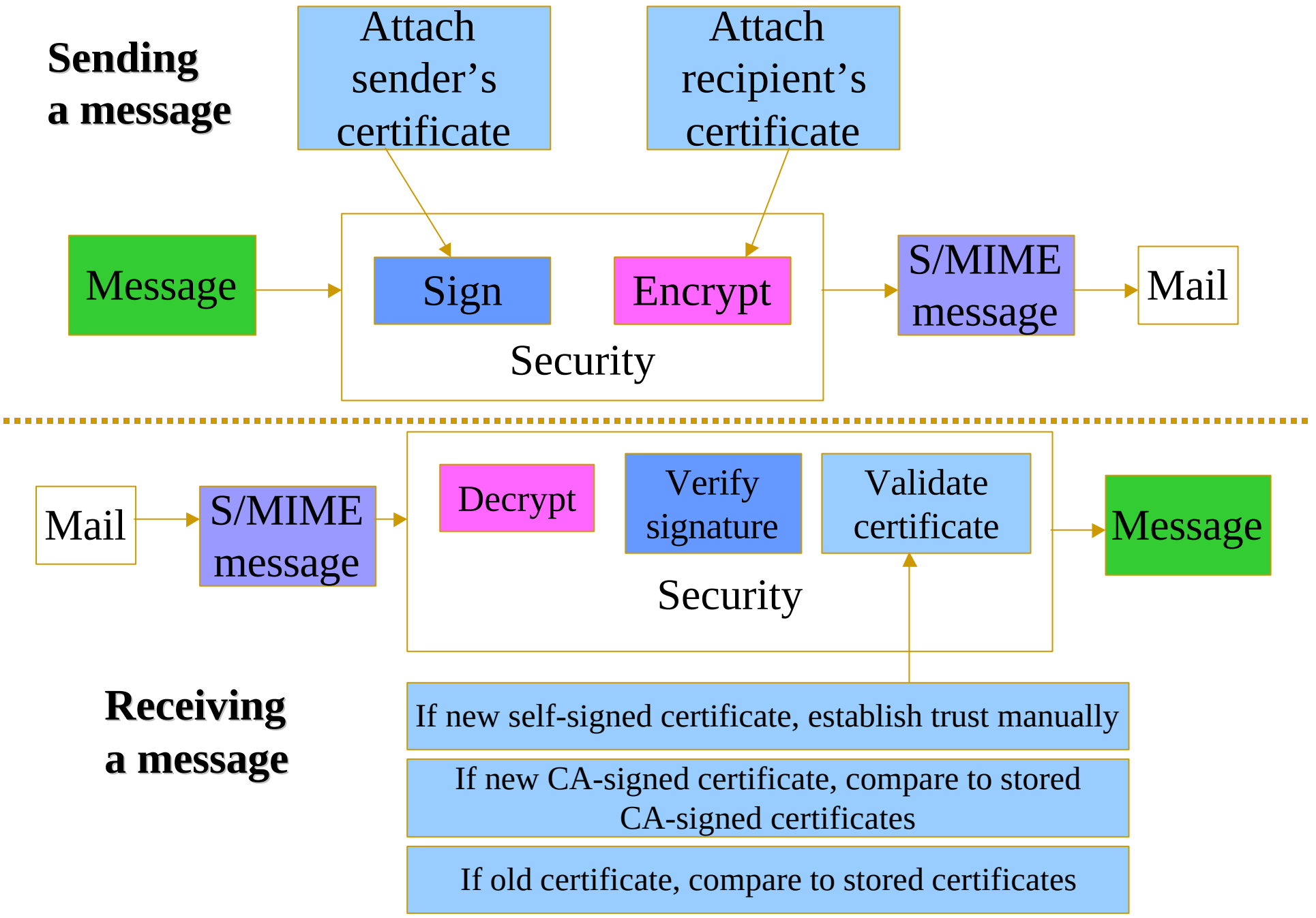
- Employ S/MIME standard
- Encrypting or digitally signing an outgoing email message.
  - (un)encrypted and (un)signed
- Decrypting or checking the digital signature on an incoming email message.

How does it work

- To encrypt an outgoing message,
  - need to obtain a valid certificate from each and every recipient in the address list (cannot be a discussion group or mailing list).
  - Update recipient’s certificate (CAs or signers can help in this)
- To sign the outgoing message,
  - must obtain a valid certificate for the sender.
  - Update sender’s certificate.

What is a Certificate or a Digital ID?

- Your Digital ID is an "electronic certificate" which installs itself on your computer and works with your browser and e-mail software.
- It contains your e-mail address and name or nickname, plus the technology to digitally sign, encrypt and decrypt the messages and documents you send over the Internet.


Sending
a message
Attach
sender's
certificate
Attach
recipient's
certificate
Message
Sign
Encrypt
Security
S/MIME
message
Mail
Mail
S/MIME
message
Decrypt
Verify
signature
Validate
certificate
Security
Message
Receiving
a message
If new self-signed certificate, establish trust manually
If new CA-signed certificate, compare to stored
CA-signed certificates
If old certificate, compare to stored certificates

Secure Electronic Transaction (SET)

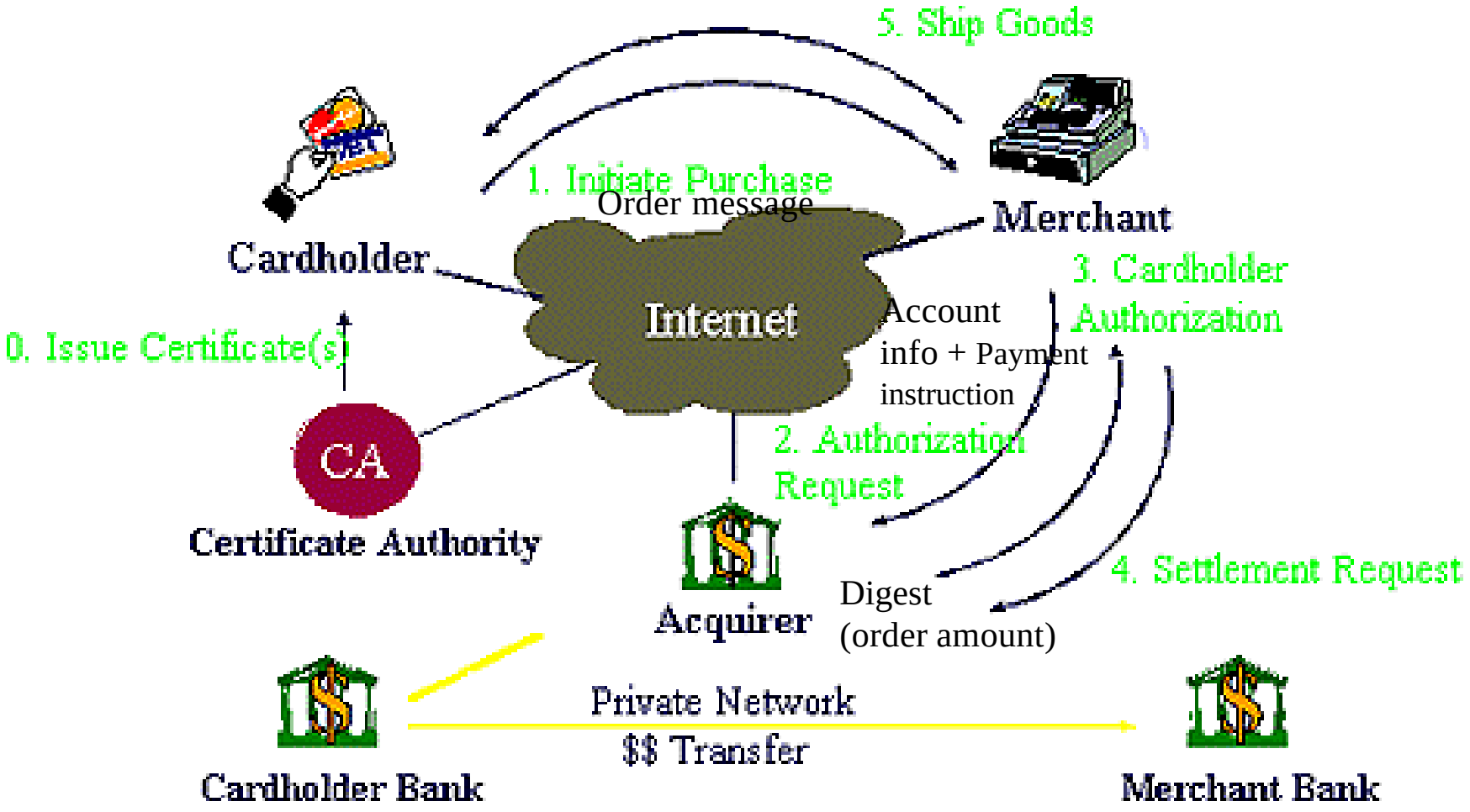
- SET is a technical standard for safeguarding payment card purchases made over open networks.
- SET employs digital certificates to verify the actual cardholder is making the purchase, and that the actual merchant is receiving it.
- Visa's web page on SET: http://www.visa.com/nt/ecomm/security/set.html including a nifty animated demonstration of a SET session.
- http://www.setco.org
- SET relies heavily on a public key infrastructure that includes:
  - Open networks such as the Internet
  - Public key cryptography (combination of public key (RSA) and secret key (DES))
  - Digital Certificates that bind a public key to an entity
  - Certification authorities to generate digital certificates

SET features

- provide *confidentiality* of information about financial data
- ensure payment *integrity*
- *authenticate* merchants, banks, and cardholders during SET transactions.
- Ability to work with a wide variety of hardware and software (*interoperability*)

- SET defines protocols and standards that deal directly with the payment process.
- SET does not deal with any other portion of the shopping process (e.g., catalog browsing and searching).

Four main entities involved in a SET transaction



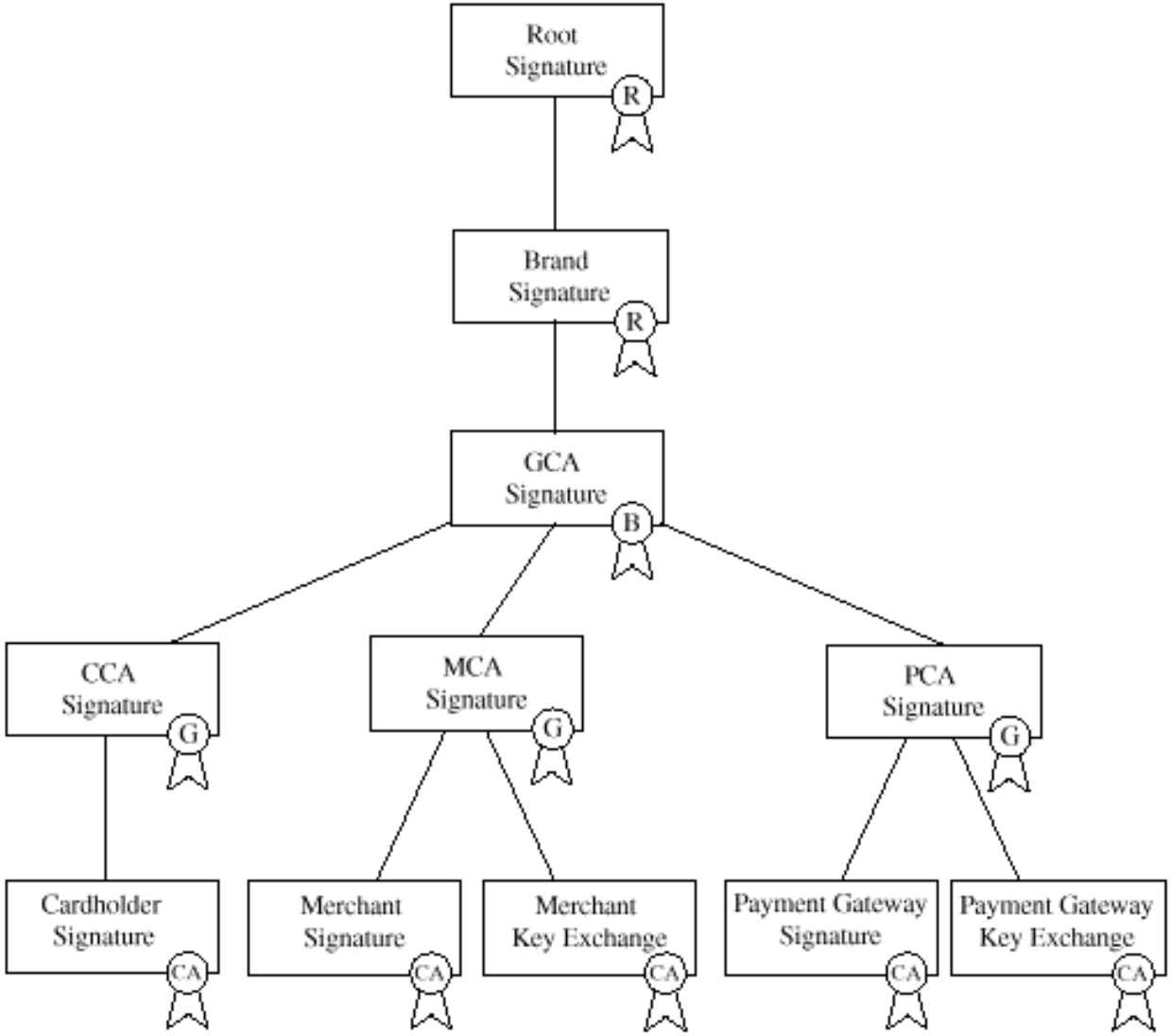
Major Components of SET

- 1.An electronic wallet - SET calls this a *Cardholder Wallet*.
  This is where the customer/consumer's credit card information is stored in some secure fashion (e.g., encrypted with a password).
  The wallet must be able to communicate and interoperate with other SET components such as the Merchant Server and Payment gateway.
- 2.The Merchant Server - This is software that is maintained by a merchant. It's job is to automatically process credit card authorizations and payments.
- 3.A Payment Gateway - software run by an acquiring financial institution or a other party that processes merchant authorization and payment messages (including payment instructions from cardholders) and interfaces with private financial networks.
- 4.A Certification Authority (CA) - as we discussed previously, a CA issues and verifies digital certificates. A CA is needed to generate certificates for:
  Wallets - The user of the wallet and their public key
  Merchant Servers
  Payment Gateways

Cryptography in SET

- Public key cryptography
- Secret key cryptography (where the secret key is shared between tow parties for a single session using Public key cryptography techniques)
- Digital Signatures (signing a mesage digest with one's own private key)
- Certificates for:
  - Cardholders (consumers with credit cards) - Certificate is approved and issued by the Issuing financial institution
  - Merchants (who accept credit cards) - Certificate is approved (possibly issued) by the Acquiring financial institution.
  - Acquiring financial institutions - Certificate is issued by "Brand" financial institutions (think Visa/MC)
  - Payment gateway - Certificates for computer systems that process credit card information. These are issued by "Brand" financial institutions

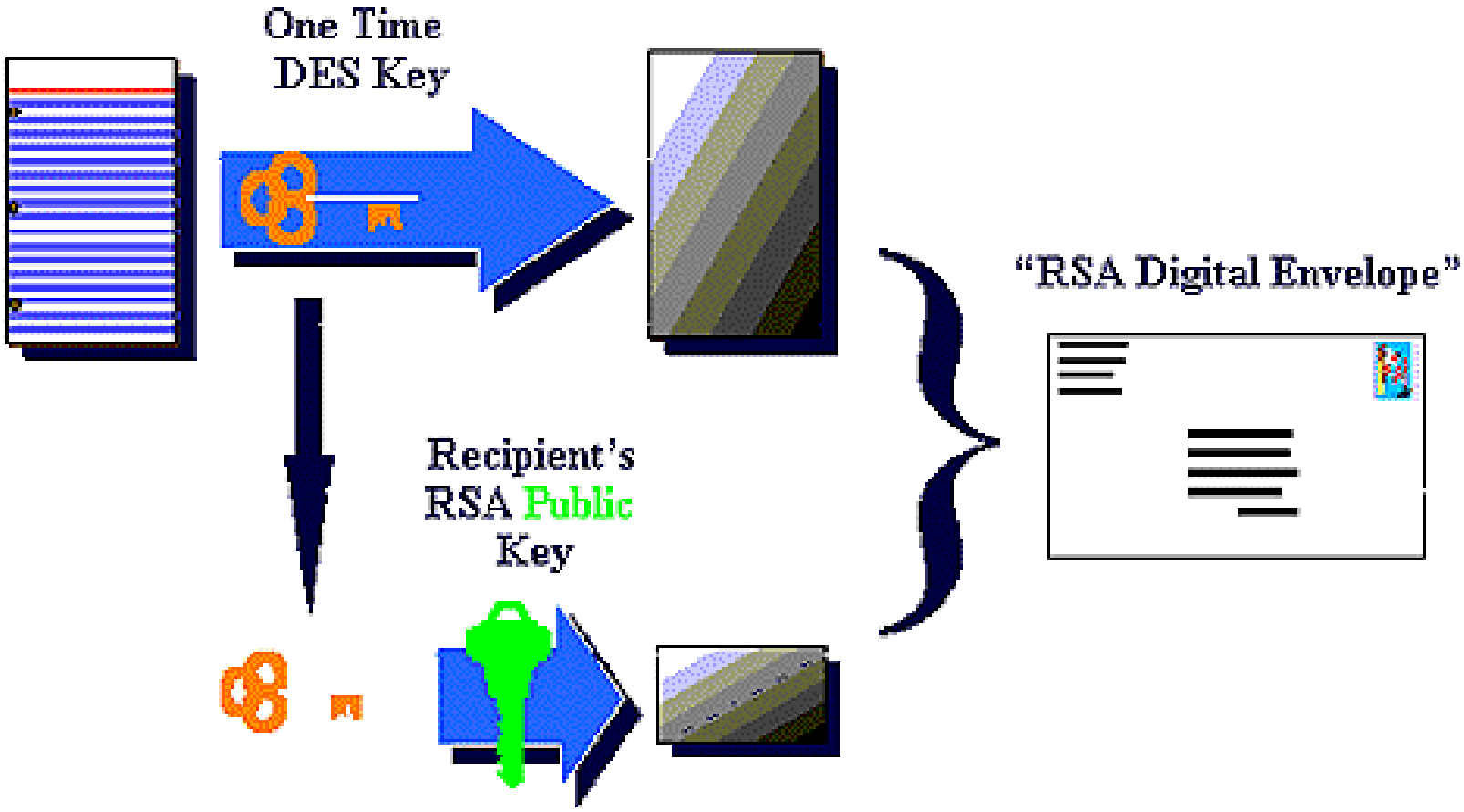
A certificate tree



Algorithms in SET

- Messages are first encrypted with 56-bit DES keys, which are then transmitted between two parties using 1024-bit RSA public key “envelope.” The 56-bit DES key is encrypted with the recipient’s public key and appended to the encrypted message. The recipient can then easily extract the encrypted DES key, decrypt it with his own private key, and use the DES key to complete the decryption of the bulk of the message.

Encrypt SET messages



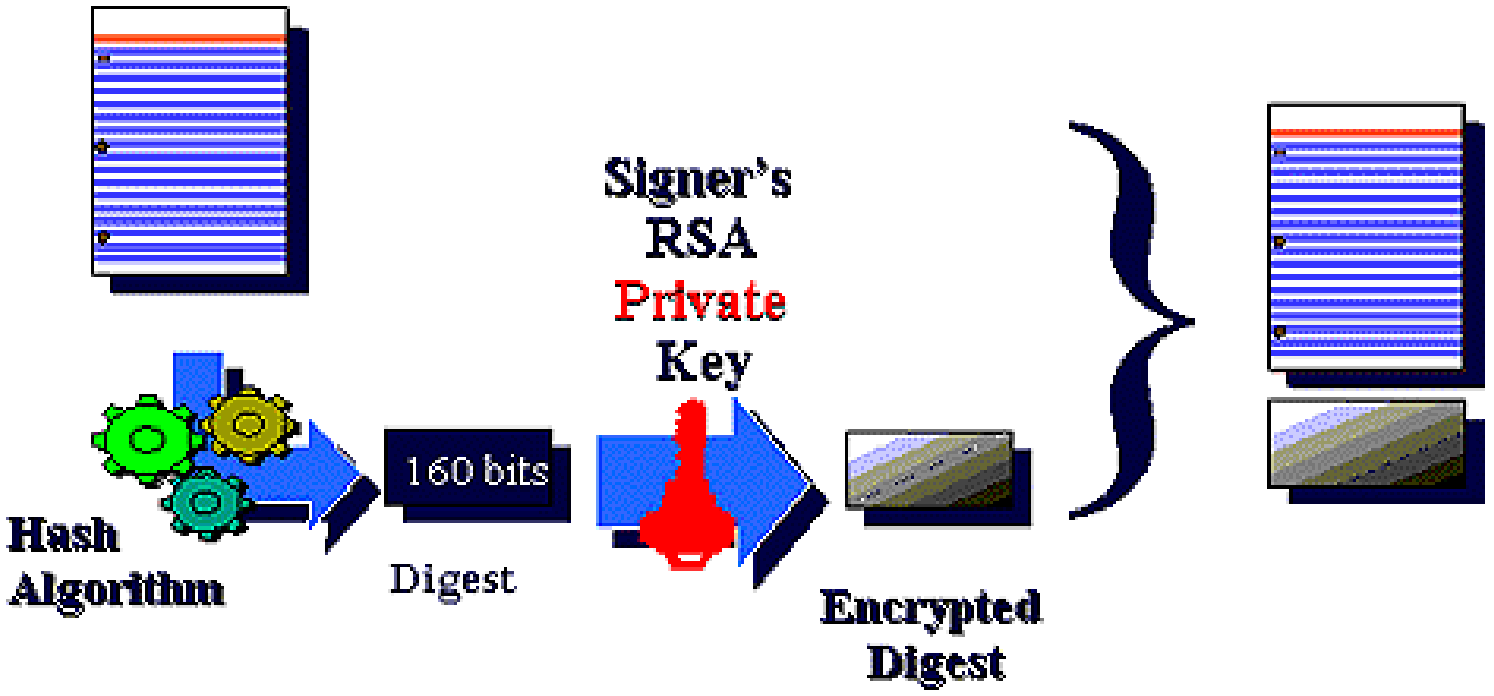
Dual Signatures in SET

- Motivation:
  - The payment is only made if the merchant accepts his offer.
  - The cardholder does not want the bank to see the term of the offer, nor
  - The cardholder does not want the merchant to know his account number.
  - The acquirer should only pay the amount that the card holder and the merchant agree upon.

Dual Signatures in SET

- Sign both messages with a single signature and encrypt them separately with recipients' public keys.
- Recall a digital signature is a digest of the message encrypted with the Sender's private key.
  This is helpful for authentication of the message - only the sender could have "signed" the message with their private key.
- With a Dual Signature, we have two messages (Message1, Message2) that will be sent to two different receivers.
  We want Receiver 1 to know that the two messages are bound together without Reciver 1 knowing the contents of Message 2.
  We want Receiver 2 to know that the two messages are bound together without Reciver 2 knowing the contents of Message 1.

Digital Signature Process



Complexity of disclosing a message

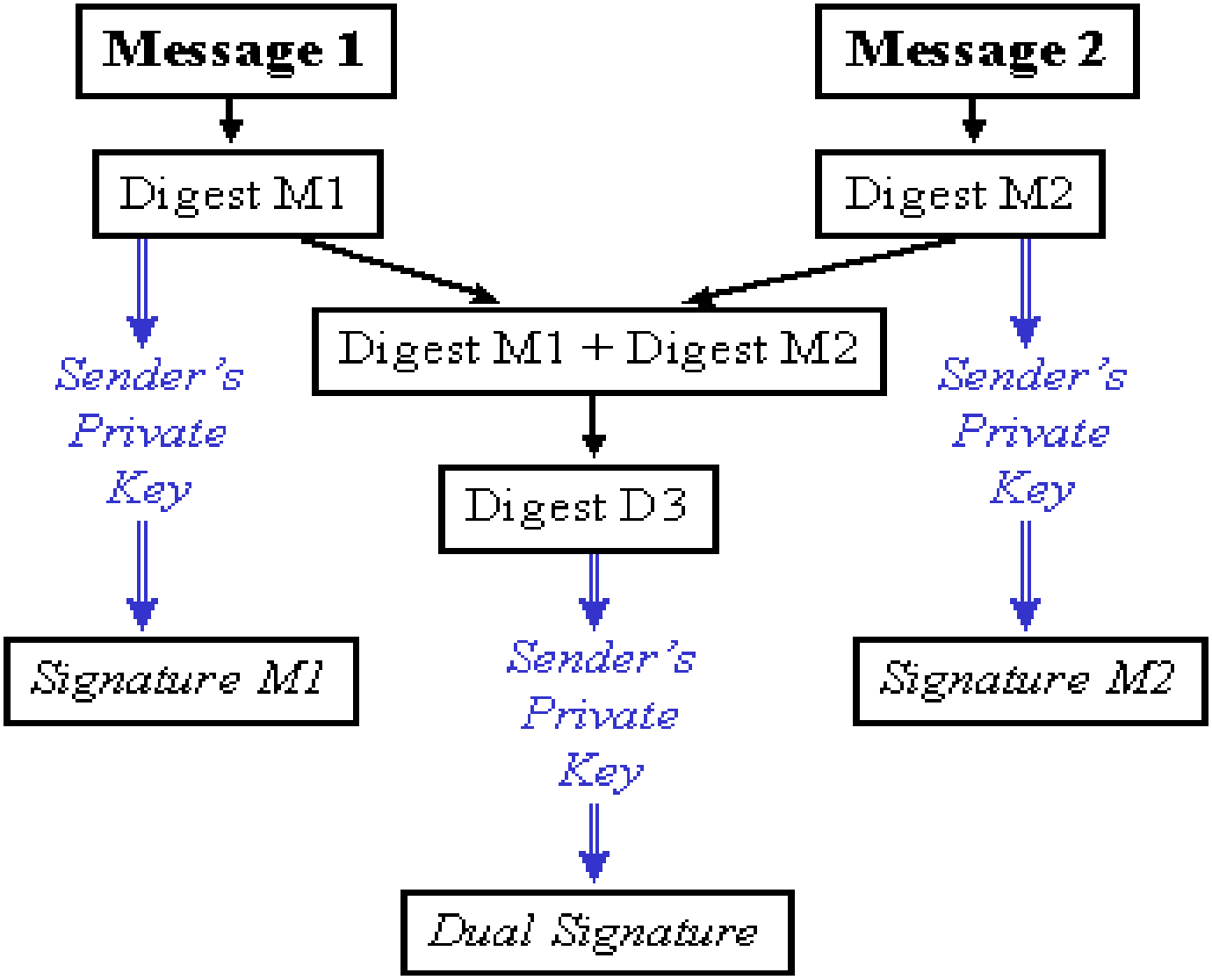
- existing estimates for a brute force attack on a 1024 bit RSA modulus are approximately 1.5×10^{11} MIPS-year
- Estimates vary for DES cracking, but most put it in the range of one million MIPS years.

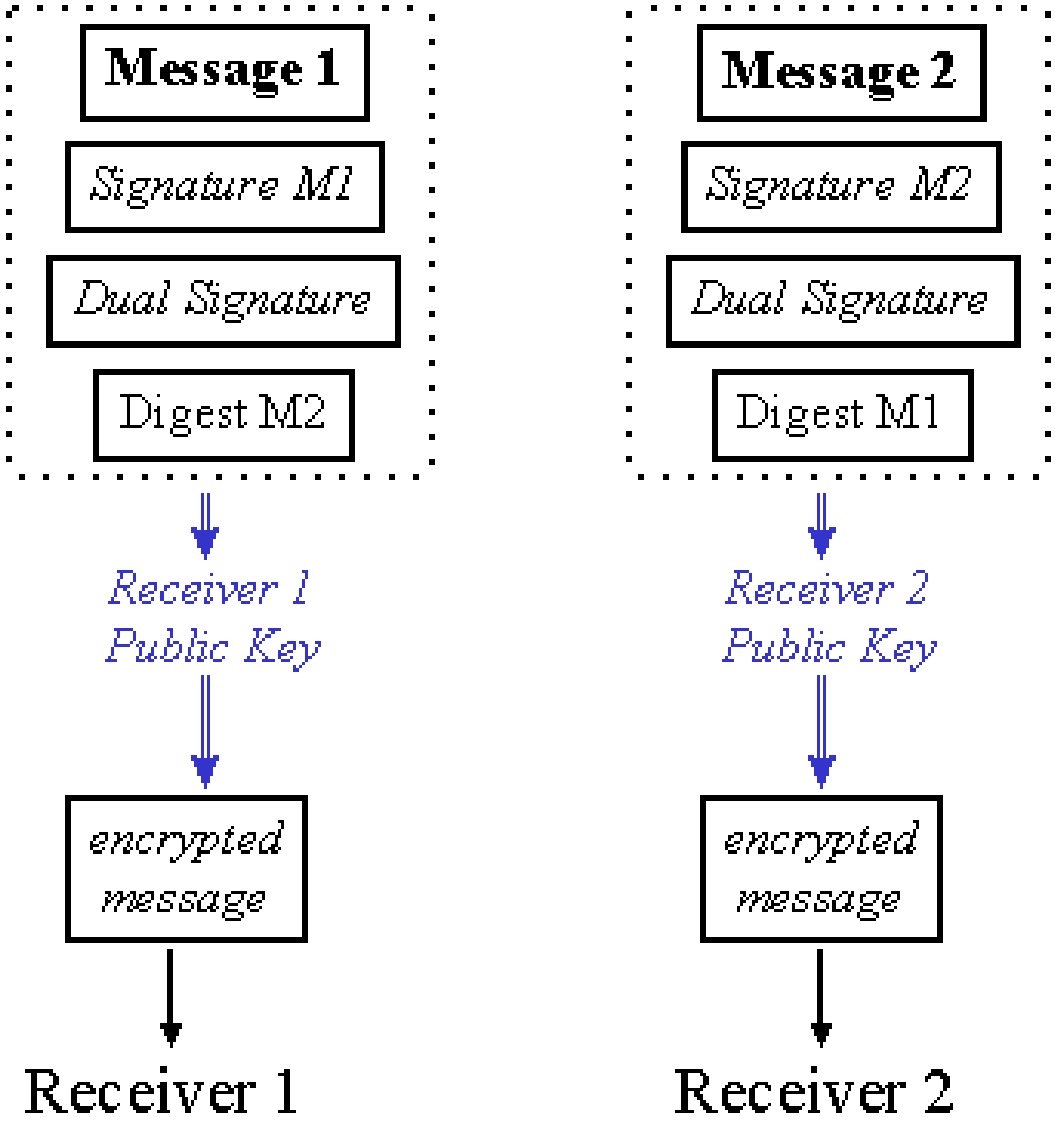
Message Integrity

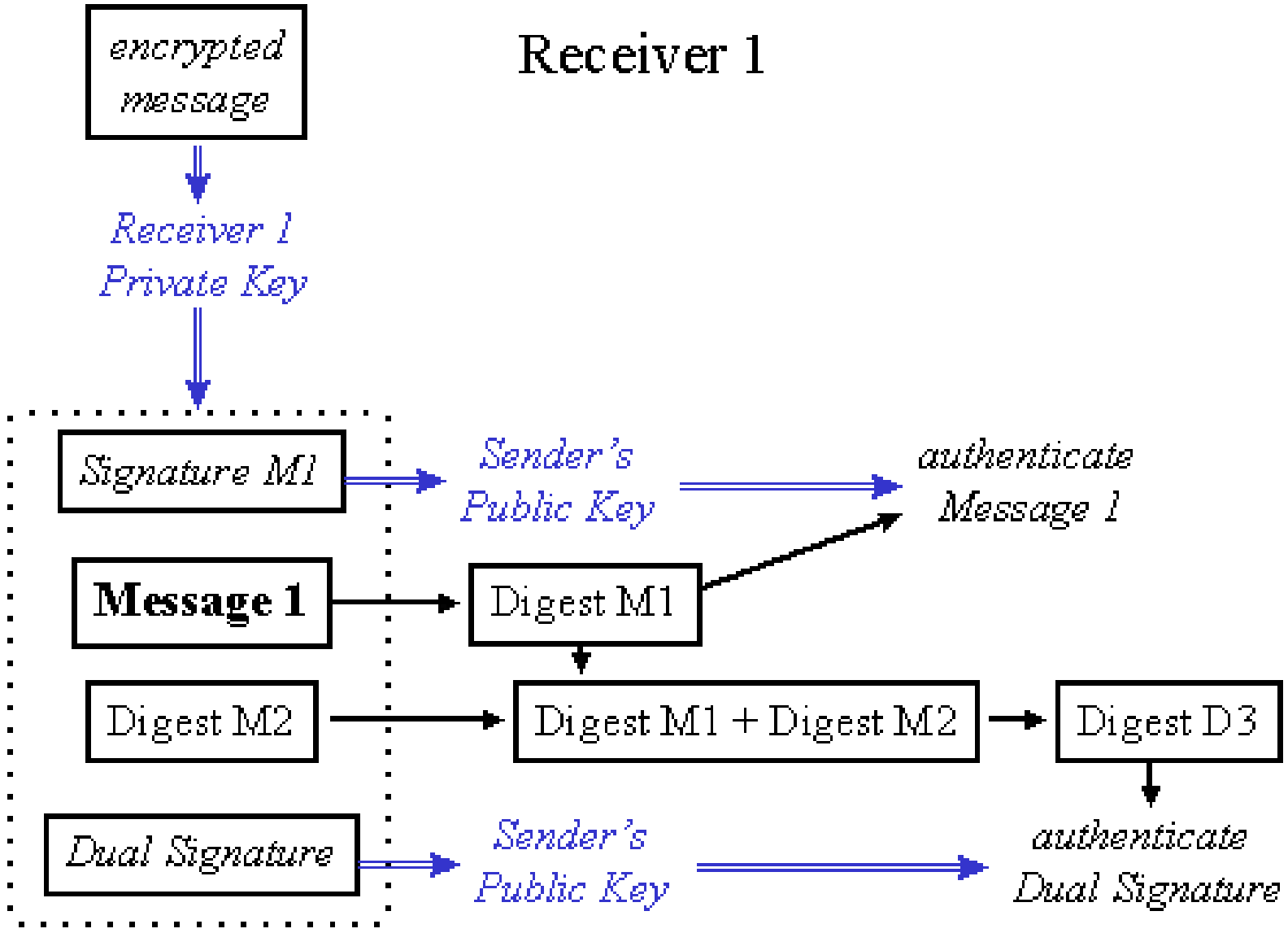
- Message Digest
- Changing a single bit in the message will change roughly half the bits in the message digest.
- The odds of two messages having the same digest are roughly one in 10^{48}

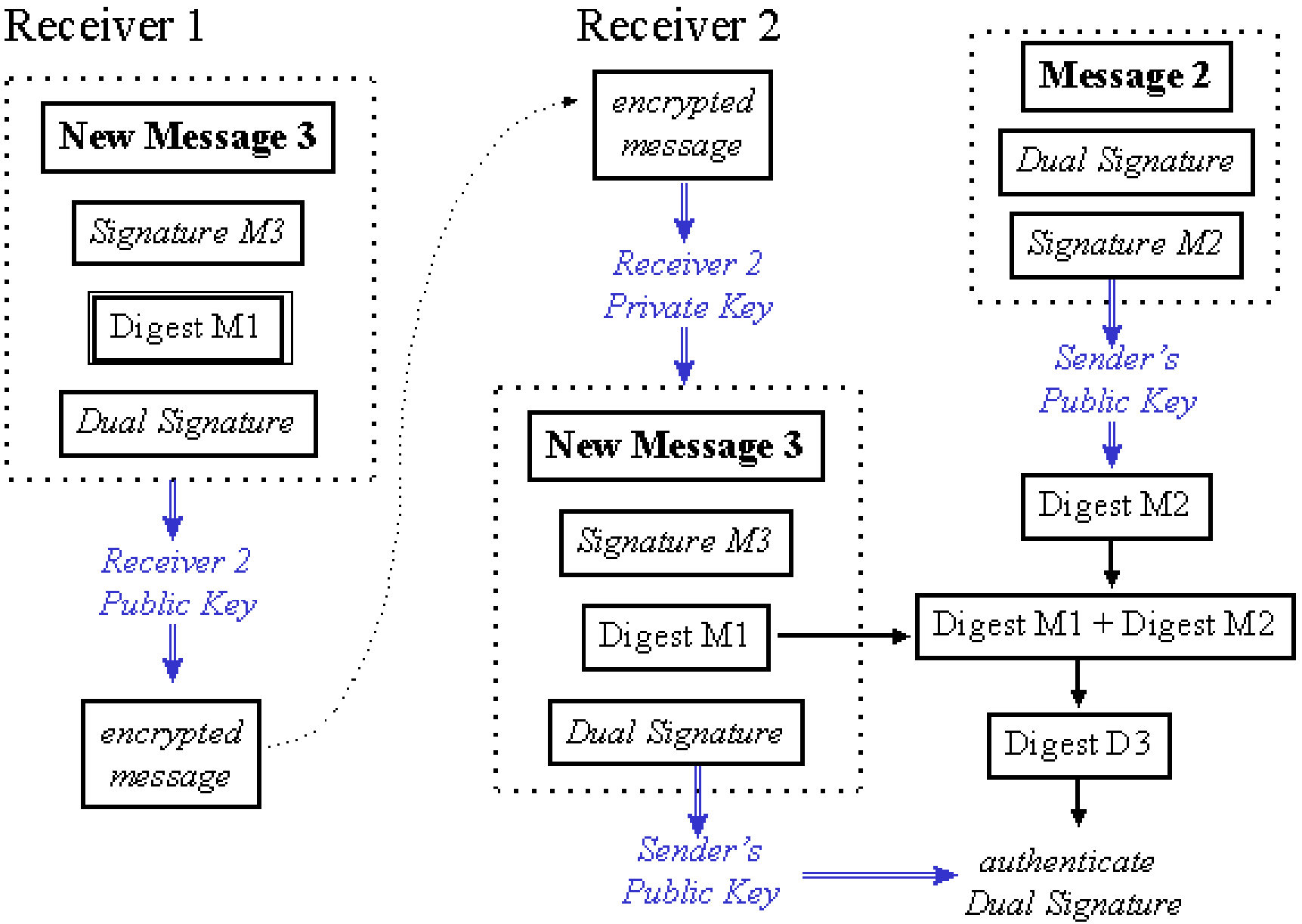
How does the digest work

- The message recipient can verify the signature by first calculating his own digest of the received message, then decrypting the original digest with the sender's public key, and then comparing the two.
- If the two digests -- one created by the sender, one by the receiver -- are identical, the sender has simultaneously authenticated both the message sender, and the message itself.


Message 1
Message 2
Digest M1
Digest M2
Digest M1 + Digest M2
Sender's Private Key
Sender's Private Key
Digest D3
Sender's Private Key
Signature M1
Signature M2
Dual Signature


Message 1
Signature M1
Dual Signature
Digest M2
Receiver 1
Public Key
encrypted
message
Receiver 1
Message 2
Signature M2
Dual Signature
Digest M1
Receiver 2
Public Key
encrypted
message
Receiver 2

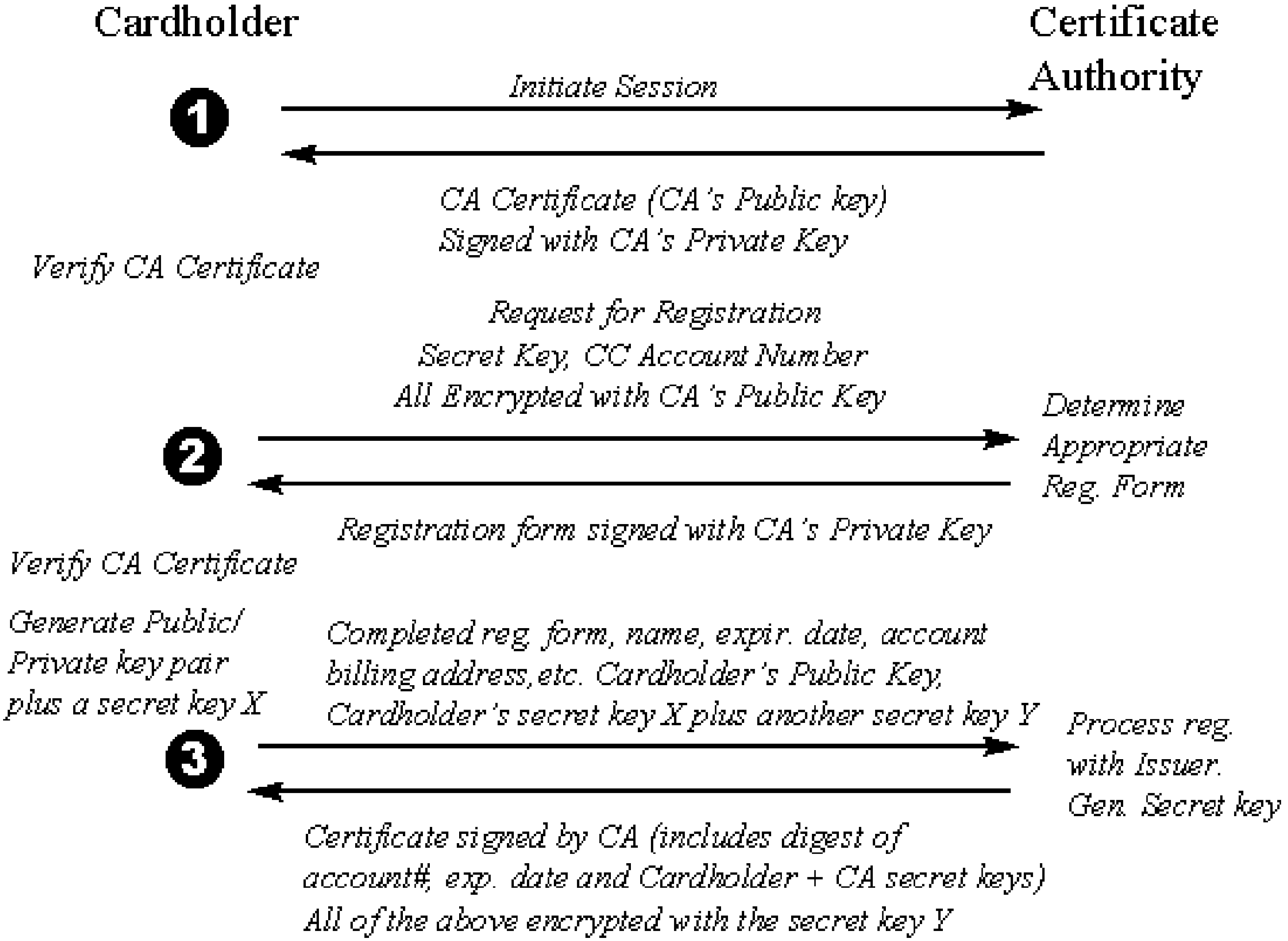

Receiver 1
encrypted message
Receiver 1 Private Key
Signature M1
Sender's Public Key
authenticate Message 1
Message 1
Digest M1
Digest M2
Digest M1 + Digest M2
Digest D3
Dual Signature
Sender's Public Key
authenticate Dual Signature


Receiver 1
New Message 3
Signature M3
Digest M1
Dual Signature
Receiver 2
Public Key
encrypted message
Receiver 2
encrypted message
Receiver 2
Private Key
New Message 3
Signature M3
Digest M1
Dual Signature
Sender's
Public Key
Message 2
Dual Signature
Signature M2
Sender's
Public Key
Digest M2
Digest M1 + Digest M2
Digest D3
authenticate
Dual Signature

Main Transactions in SET

- 1.Cardholder registration
- 2.Merchant registration
- 3.Purchase request
- 4.Payment authorization
- 5.Payment capture

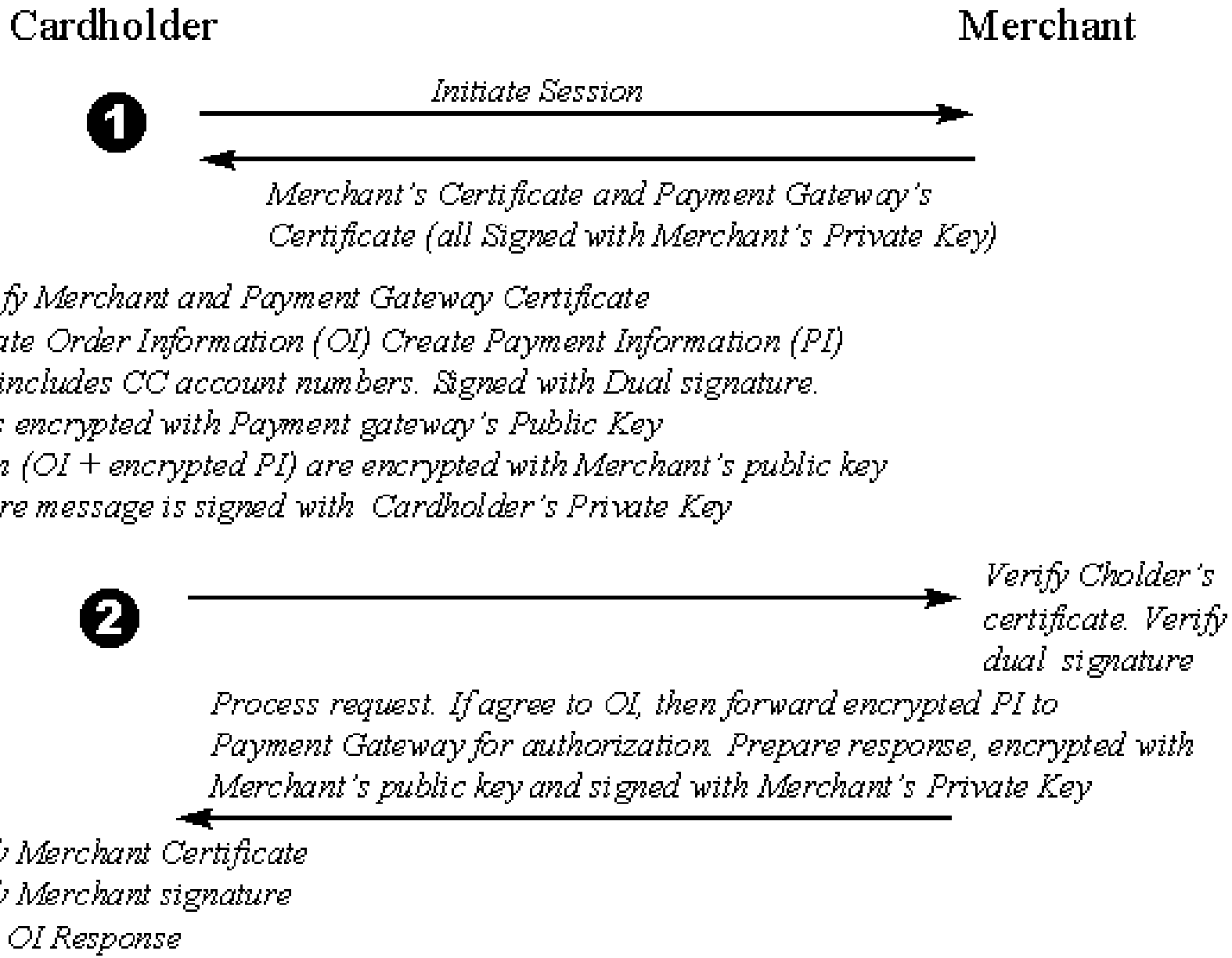
Cardholder registration



Merchant registration

- Similar to Cardholder registration.
- Result is a authorized certificate (includes public key).

Purchase request



Payment authorization

Merchant **Payment G-way**

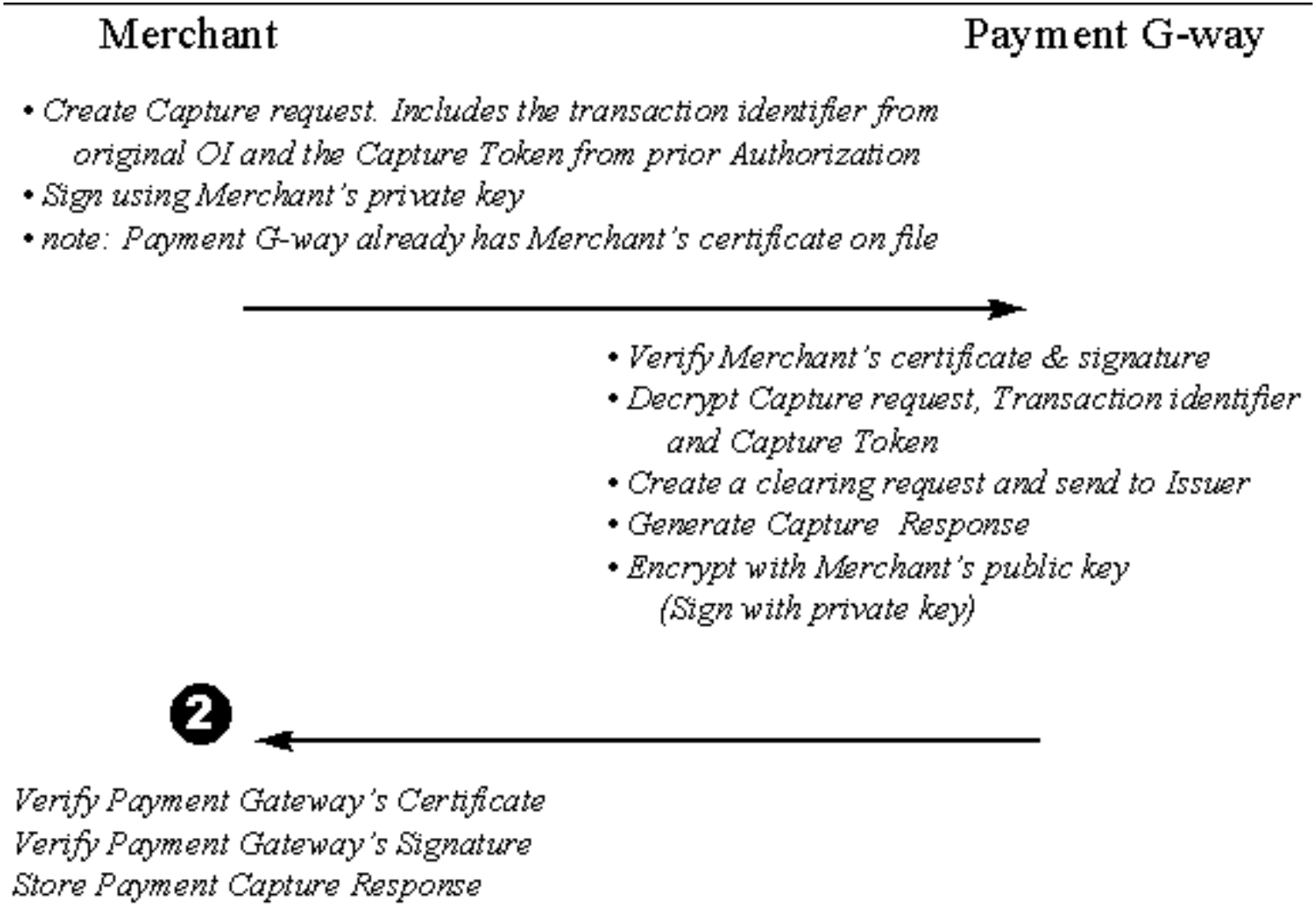
- *Create Payment Authorization request*
- *Sign using Merchant's private key*
- *note: Payment G-way already has Merchant's certificate on file*
- *Include PI from cardholder (recall this was encrypted with Payment gateway's Public Key)*

- *Verify Merchant's certificate & signature*
- *Decrypt PI and verify cardholder's certificate and signature*
- *Verify dual signature*
- *Perform authorization at Issuer*
- *Generate authorization response*
- *Generate a "Capture Token" (used later)*
- *Encrypt with Merchant's public key (Sign with private key)*

❷

Verify Payment Gateway's Certificate
Verify Payment Gateway's Signature
Store Payment Authorization Response and Capture Token

Payment capture



Authentication Authority

- A secure, trusted Certificate Authority distributes digitally signed certificates for each party in the transaction, assuring the authenticity of their public keys.
- Through the use of Certificate Authorities and the SET protocol, cardholders can rely on the Certificate Authority to ensure the identity of the merchant with whom they are dealing, and not worry about misuse of their credit card information.

Procedure to set up a secure messager

- To obtain a certificate for your self from a CA (e.g., verisign, AT&T, GTE)
  - $19.95/Month for class II
- To obtain certificates from others through email messages, accessing web pages or Java applets and verify the certificates with a CA.
- Set up security configuration in Netscape .

Full Service Class 1 Digital ID ($9.95/month)

- Sign and encrypt e-mail
- Quickly retrieve anyone's Digital ID using Netscape Messenger or Microsoft Outlook Express
- Use your Digital ID to register at participating web sites in one easy step
- $1,000 of NetSureSM protection against economic loss caused by corruption, loss or misuse of your Digital ID

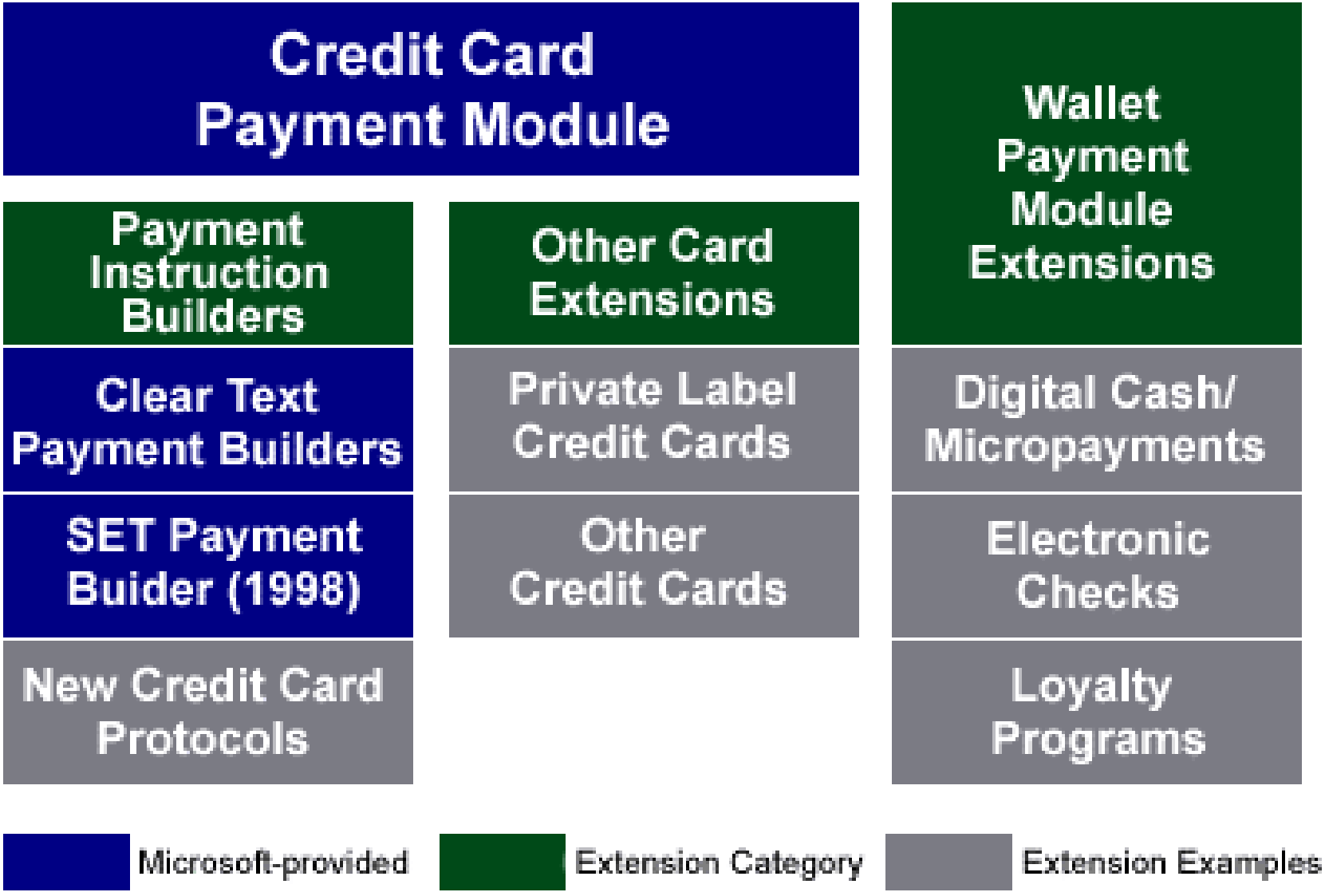
Full Service Class 2 Digital ID ($19.95/month)

- All the other benefits of a full-year, full service Class 1 Digital ID
- Achieve greater security for electronic transactions and signed email with verification of your personal identity not just your email address
- NetSure protection of $25,000

Microsoft Wallet

- Electronic wallet (either a plug-in for Netscape or ActiveX control of MS IE)
- Stores:
  - Billing and Shipping information
  - Credit card information
  - Information for other payment services (digital cash, electronic checks, or loyalty program data)
- MS Wallet provides an architecture that has built in support for SET plus additional support for other payment services.

Microsoft Wallet



Verifone

- Yet another software vendor with a SET and SSL compliant software suite.
- From the VeriFone web page:
  - **vWALLET -** provides consumers with a "virtual wallet,"
  - **vPOS -** allows the merchant to receive consumer originated payment transactions and send consumer and merchant originated payment transactions to the merchants acquiring banks vGATE Internet gateway.
  - **vGATE -** The VeriFone® vGATE Internet gateway is a secure computer system that mediates Internet-based payment transactions between the merchants servers and the acquiring banks card processing host.
  - **Omnihost -** translates transaction messages from the vGATE gateway to the appropriate output format for the acquiring host or directly to an interchange format.