E-commerce Systems

Electronic Payment Systems

E-payment systems

- To transfer money over the Internet
- Methods of traditional payment
  - Check, credit card, or cash
- Methods of electronic payment
  - Electronic cash, software wallets, smart cards, and credit/debit cards
  - Scrip is digital cash minted by third-party organizations

Requirements for e-payments

- Atomicity
  - Money is not lost or created during a transfer
- Good atomicity
  - Money and good are exchanged atomically
- Non-repudiation
  - No party can deny its role in the transaction
  - Digital signatures

Desirable Properties of Digital Money

- Universally accepted
- Transferable electronically
- Divisible
- Non-forgeable, non-stealable
- Private (no one except parties know the amount)
- Anonymous (no one can identify the payer)
- Work off-line (no on-line verification needed)

No known system satisfies all.

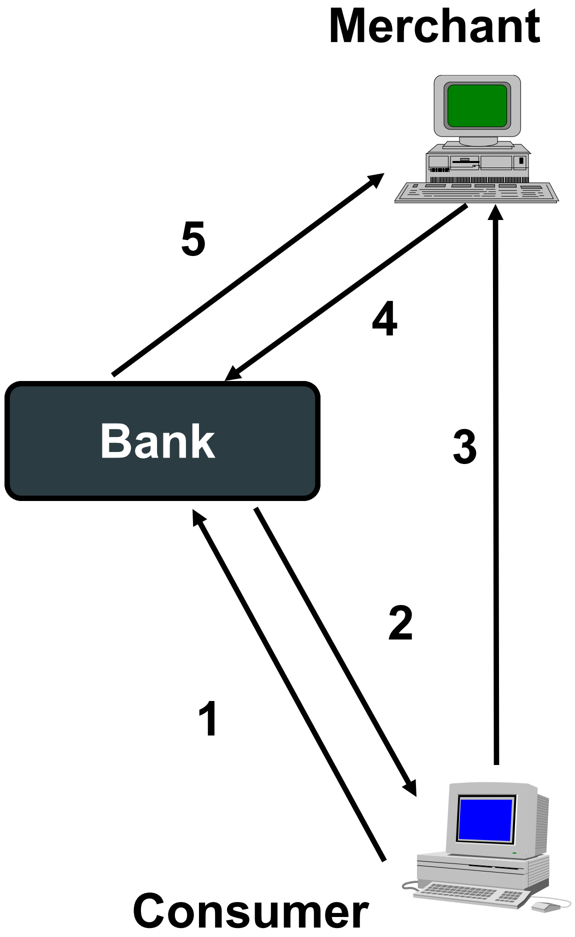
Types of E-payments

- E-cash
- Electronic wallets
- Smart card
- Credit card

Electronic Cash

- Primary advantage is with purchase of items less than $10
  - Credit card transaction fees make small purchases unprofitable
  - Micropayments
    - Payments for items costing less than $1

E-cash Concept



1. Consumer buys e-cash from Bank
2. Bank sends e-cash bits to consumer (after charging that amount plus fee)
3. Consumer sends e-cash to merchant
4. Merchant checks with Bank that e-cash is valid (check for forgery or fraud)
5. Bank verifies that e-cash is valid
6. Parties complete transaction: e.g., merchant present e-cash to issuing back for deposit once goods or services are delivered

Consumer still has (invalid) e-cash

Electronic Cash Issues

- E-cash must allow spending only once
- Must be anonymous, just like regular currency
  - Safeguards must be in place to prevent counterfeiting
  - Must be independent and freely transferable regardless of nationality or storage mechanism
- Divisibility and Convenience
- Complex transaction (checking with Bank)
  - Atomicity problem

Two storage methods

- On-line
  - Individual does not have possession personally of electronic cash
  - Trusted third party, e.g. online bank, holds customers' cash accounts
- Off-line
  - Customer holds cash on smart card or software wallet
  - Fraud and double spending require tamper-proof encryption

Advantages and Disadvantages of Electronic Cash

- Advantages
  - More efficient, eventually meaning lower prices
  - Lower transaction costs
  - Anybody can use it, unlike credit cards, and does not require special authorization
- Disadvantages
  - Tax trail non-existent, like regular cash
  - Money laundering
  - Susceptible to forgery

Electronic Cash Security

- Complex cryptographic algorithms prevent double spending
  - Anonymity is preserved unless double spending is attempted
- Serial numbers can allow tracing to prevent money laundering
  - Does not prevent double spending, since the merchant or consumer could be at fault

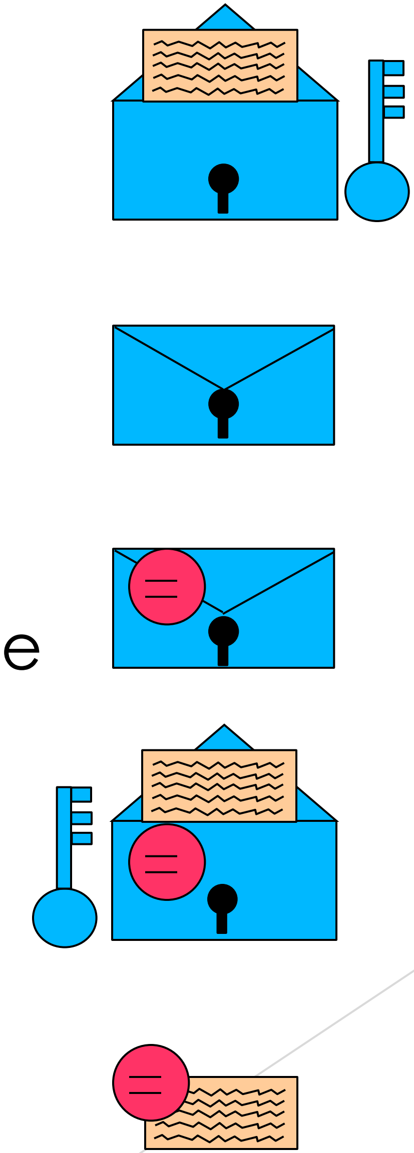
Blind Signatures

- **Goal**
  - to have the bank sign documents without knowing what they are signing.
- **Why?**
  - Anonymity with Authentication

How to sign with blind fold?

- **How?**
  Basic: Sign anything

1. You encrypt the message
2. Send it to the bank
3. The bank signs the message and returns it
4. You decrypt the signed message
5. You spend it



Cut and Choose

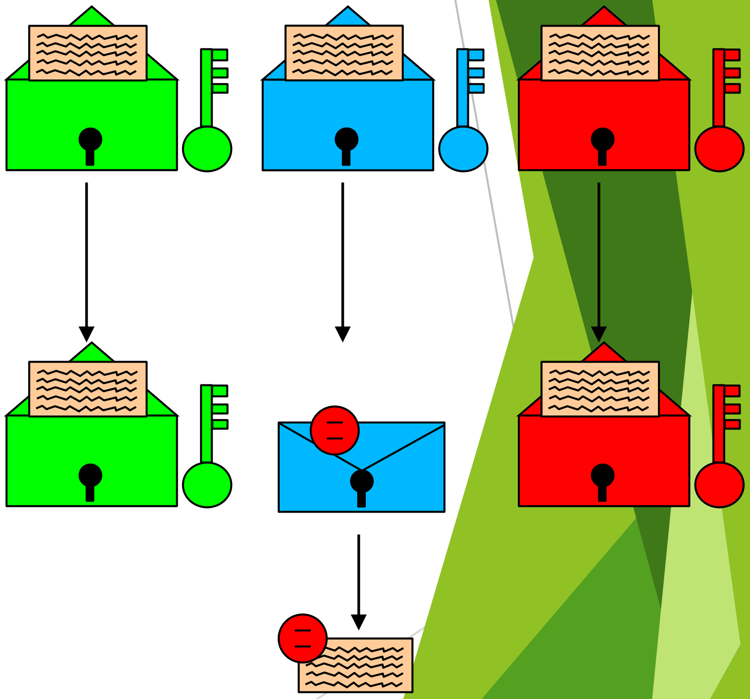
- **Problems**

  The bank honors anything I write down
- **Solution:** the Cut-and-choose algorithm

1. Prepare *n* copies of the messages and *n* different keys, and send them to the bank

2. The bank requests the keys for and opens *n* - 1 of them, and verifies them. It then signs the remaining one.

3. The bank sends back the signed message, which can then be decrypted and spent



Anonymous digital cash?

- Protocol #1
- Protocol #2
- Protocol #3
- Protocol #4

Detecting Double Spending

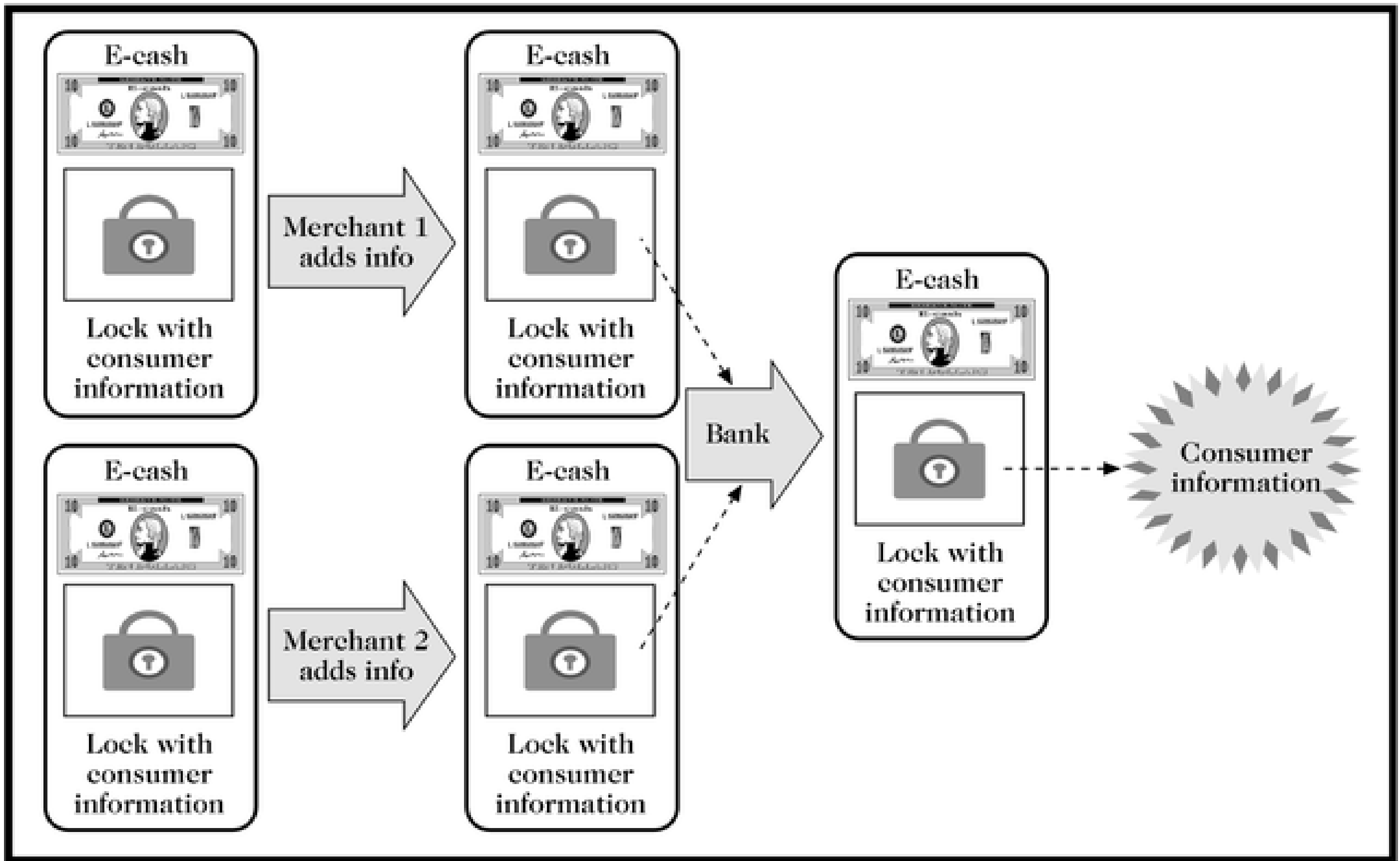

E-cash
Lock with consumer information
Merchant 1 adds info
E-cash
Lock with consumer information
E-cash
Lock with consumer information
Merchant 2 adds info
E-cash
Lock with consumer information
Bank
E-cash
Lock with consumer information
Consumer information

FIGURE 7-3 *Detecting double spending*

Past and Present E-cash Systems

- E-cash not popular in U.S., but successful in Europe and Japan
  - Reasons for lack of U.S. success not clear
    - Manner of implementation too complicated
    - Lack of standards and interoperable software that will run easily on a variety of hardware and software systems

Past and Present E-cash Systems

- Checkfree
  - Allows payment with online electronic checks
- Clickshare
  - Designed for magazine and newspaper publishers
  - Miscast as a micropayment only system; only one of its features
  - Purchases are billed to a user’s ISP, who in turn bill the customer

Past and Present E-cash Systems

- CyberCash
  - Combines features from cash and checks
  - Offers credit card, micropayment, and check payment services
  - Connects merchants directly with credit card processors to provide authorizations for transactions in real time
    - No delays in processing prevent insufficient e-cash to pay for the transaction
- CyberCoins
  - Stored in CyberCash wallet, a software storage mechanism located on customer's computer
  - Used to make purchases between .25c and $10
  - PayNow -- payments made directly from checking accounts

Past and Present E-cash Systems

- DigiCash
  - Trailblazer in e-cash
  - Allowed customers to purchase goods and services using anonymous electronic cash
  - Recently entered Chapter 11 reorganization
- Coin.Net
  - Electronic tokens stored on a customer’s computer is used to make purchases
  - Works by installing special plug-in to a customer’s web browser
  - Merchants do not need special software to accept eCoins.
  - eCoin server prevents double-spending and traces transactions, but consumer is anonymous to merchant

Aggregation

- Used when individual transactions are too small for credit card (e.g. $2.00)
- Consumer and Merchant sign up with Aggregator
- Consumer makes purchase. Merchant notifies Aggregator.
- Aggregator keeps Consumer’s account. When amount owed is large enough (or every month), charges to Consumer’s credit card
- Aggregator sends money (less fees) to Merchant
- QPASS, CyberCash, GlobeID

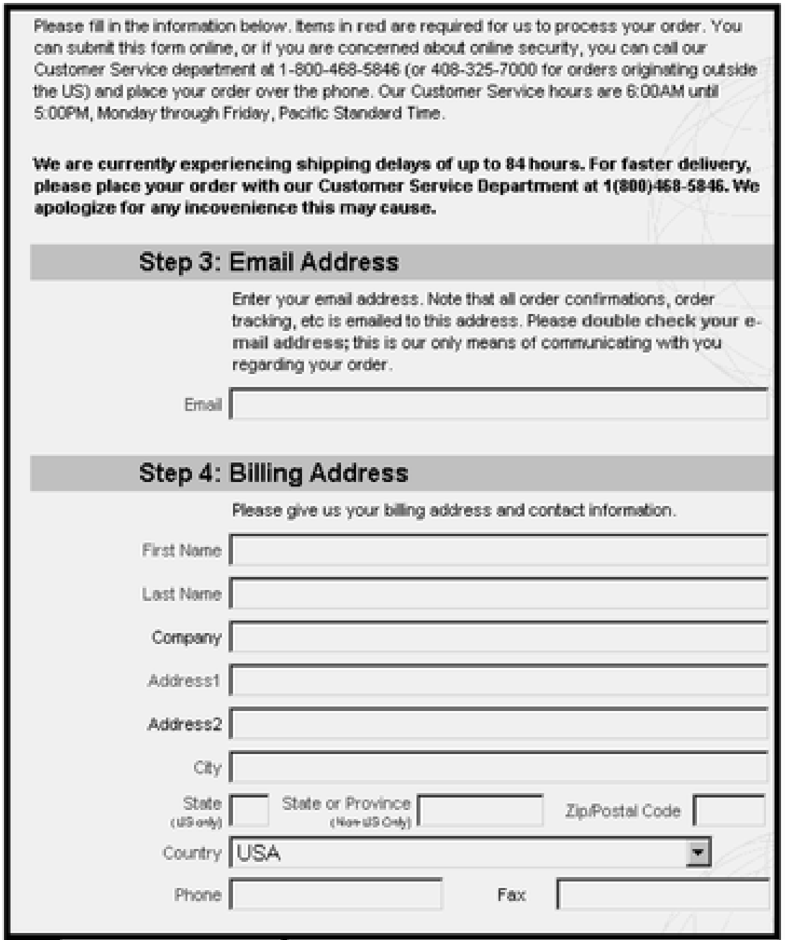
Past and Present E-cash Systems

- MilliCent
  - Developed by Digital, now part of Compaq
  - Electronic scrip system
  - Participating merchant creates and sells own scrip to broker at a discount
    - Consumers register with broker and buy bulk generic scrip, usually with credit card
    - Customers buy by converting broker scrip to vendor-specific scrip, i.e. scrip that a particular merchant will accept
  - Customers can purchase items of very low value
  - Brokers required for two reasons:
    - Small payments require aggregation to insure profitability
    - System is easier to use -- customer need only deal with one broker for all their scrip needs

Electronic Wallets

- Stores credit card, electronic cash, owner identification and address
  - Makes shopping easier and more efficient
    - Eliminates need to repeatedly enter identifying information into forms to purchase
    - Works in many different stores to speed checkout
  - Amazon.com one of the first online merchants to eliminate repeat form-filling for purchases

An Electronic Checkout Counter Form



Please fill in the information below. Items in red are required for us to process your order. You can submit this form online, or if you are concerned about online security, you can call our Customer Service department at 1-800-468-5846 (or 408-325-7000 for orders originating outside the US) and place your order over the phone. Our Customer Service hours are 6:00AM until 5:00PM, Monday through Friday, Pacific Standard Time.

We are currently experiencing shipping delays of up to 84 hours. For faster delivery, please place your order with our Customer Service Department at 1(800)468-5846. We apologize for any incovenience this may cause.

Step 3: Email Address

Enter your email address. Note that all order confirmations, order tracking, etc is emailed to this address. Please **double check your e-mail address; this is our only means of communicating with you** regarding your order.

Email

Step 4: Billing Address

Please give us your billing address and contact information.

First Name

Last Name

Company

Address1

Address2

City

State (US only) State or Province (Non-US Only) Zip/Postal Code

Country USA

Phone Fax

FIGURE 7-9 *A typical electronic checkout counter form*

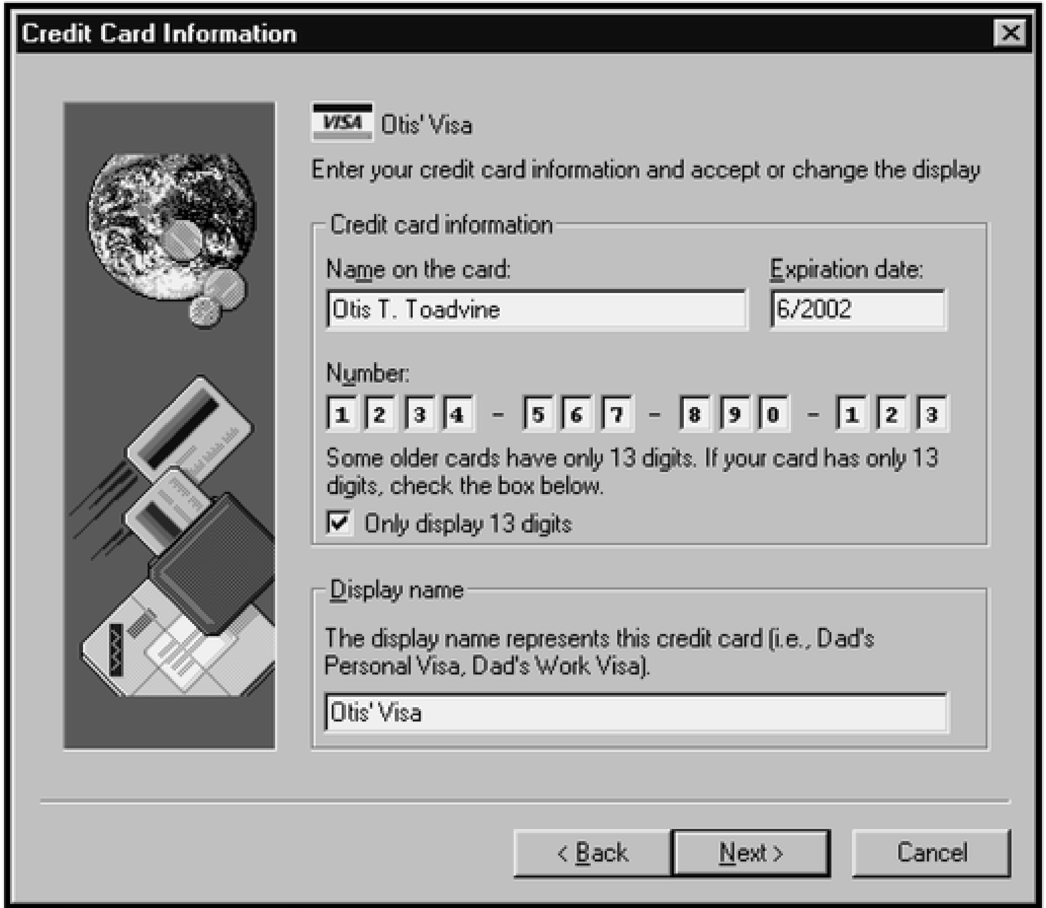
Electronic Wallets

- Agile Wallet
  - Developed by CyberCash
  - Allows customers to enter credit card and identifying information once, stored on a central server
  - Information pops up in supported merchants’ payment pages, allowing one-click payment
  - Does not support smart cards or CyberCash, but company expects to soon
- eWallet
  - Developed by Launchpad Technologies
  - Free wallet software that stores credit card and personal information on users’ computer, not on a central server; info is dragged into payment form from eWallet
  - Information is encrypted and password protected
  - Works with Netscape and Internet Explorer

Electronic Wallets

- Microsoft Wallet
  - Comes pre-installed in Internet Explorer 4.0, but not in Netscape
  - All information is encrypted and password protected
  - Microsoft Wallet Merchant directory shows merchants setup to accept Microsoft Wallet

Entering Information Into Microsoft Wallet



Credit Card Information

VISA Otis' Visa

Enter your credit card information and accept or change the display

Credit card information

Name on the card: Otis T. Toadvine

Expiration date: 6/2002

Number: 1234 - 567 - 890 - 123

Some older cards have only 13 digits. If your card has only 13 digits, check the box below.

☑ Only display 13 digits

Display name

The display name represents this credit card (i.e., Dad's Personal Visa, Dad's Work Visa).

Otis' Visa

FIGURE 7-10 *Entering credit card information into Microsoft Wallet*

Smart Cards

- Magnetic stripe
  - 140 bytes, cost $0.20-0.75
- Memory cards
  - 1-4 KB memory, no processor, cost $1.00-2.50
- Optical memory cards
  - 4 megabytes read-only (CD-like), cost $7.00-12.00
- Microprocessor cards
  - Embedded microprocessor
    - (OLD) 8-bit processor, 16 KB ROM, 512 bytes RAM
    - Equivalent power to IBM XT PC, cost $7.00-15.00
    - 32-bit processors now available

Smart Cards

- Plastic card containing an embedded microchip
- Available for over 10 years
- So far not successful in U.S., but popular in Europe, Australia, and Japan
- Unsuccessful in U.S. partly because few card readers available
- Smart cards gradually reappearing in U.S.; success depends on:
  - Critical mass of smart cards that support applications
  - Compatibility between smart cards, card-reader devices, and applications

Smart Card Applications

- Ticketless travel
  - Seoul bus system: 4M cards, 1B transactions since 1996
  - Planned the SF Bay Area system
- Authentication, ID
- Medical records
- Ecash
- Store loyalty programs
- Personal profiles
- Government
  - Licenses
- Mall parking

. . .

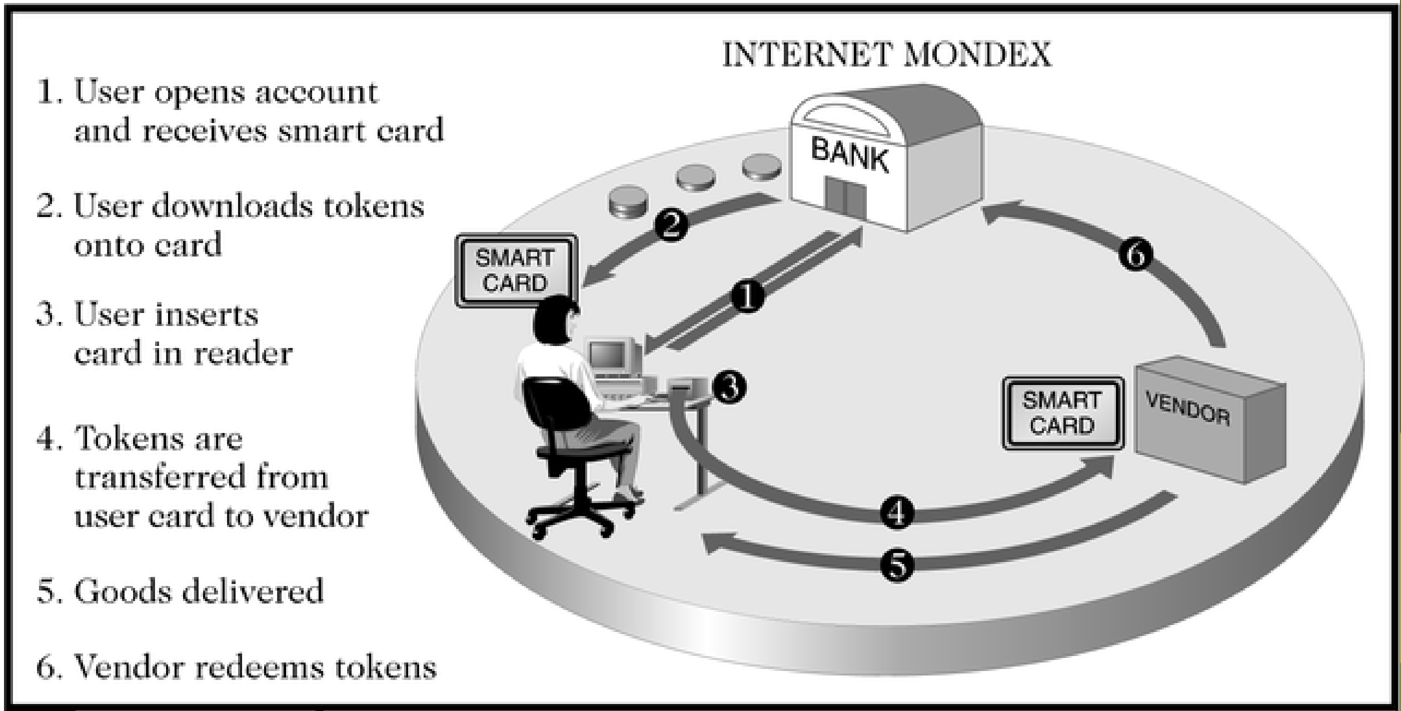
Advantages and Disadvantages of Smart Cards

- Advantages:
  1. Atomic, debt-free transactions
  2. Feasible for very small transactions (information commerce)
  3. (Potentially) anonymous
  4. Security of physical storage
  5. (Potentially) currency-neutral
- Disadvantages:
  1. Low maximum transaction limit (not suitable for B2B or most B2C)
  2. High Infrastructure costs (not suitable for C2C)
  3. Single physical point of failure (the card)
  4. Not (yet) widely used

Mondex Smart Card

- Holds and dispenses electronic cash (Smart-card based, stored-value card)
- Developed by MasterCard International
- Requires specific card reader, called Mondex terminal, for merchant or customer to use card over Internet
- Supports micropayments as small as 3c and works both online and off-line at stores or over the telephone
- Secret chip-to-chip transfer protocol
- Value is not in strings alone; must be on Mondex card
- Loaded through ATM
  - ATM does not know transfer protocol; connects with secure device at bank

Mondex Smart Card Processing



1. User opens account and receives smart card
2. User downloads tokens onto card
3. User inserts card in reader
4. Tokens are transferred from user card to vendor
5. Goods delivered
6. Vendor redeems tokens

FIGURE 7-12 *Mondex smart card processing*

Mondex transaction

- Here's what happens "behind the scenes" during a Mondex transaction between a consumer and merchant. Placing the card in a Mondex terminal starts the transaction process:

  1. Information from the customer's chip is validated by the merchant's chip. Similarly, the merchant's card is validated by the customer's card.
  2. The merchant's card requests payment and transmits a "digital signature" with the request. Both cards check the authenticity of each other's message. The customer's card checks the digital signature and, if satisfied, sends acknowledgement, again with a digital signature.
  3. Only after the purchase amount has been deducted from the customer's card is the value added to the merchant's card. The digital signature from this card is checked by the customer's card and if confirmed, the transaction is complete.

Mondex Smart Card

- Disadvantages
  - Card carries real cash in electronic form, creating the possibility of theft
  - No deferred payment as with credit cards -cash is dispensed immediately
- Security
  - Active and dormant security software
    - Security methods constantly changing
    - ITSEC E6 level (military)
  - VTP (Value Transfer Protocol)
    - Globally unique card numbers
    - Globally unique transaction numbers
    - Challenge-response user identification
    - Digital signatures
  - MULTOS operating system
    - firewalls on the chip

Credit Cards

- Credit card
  - Used for the majority of Internet purchases
  - Has a preset spending limit
  - Currently most convenient method
  - Most expensive e-payment mechanism
    - MasterCard: $0.29 + 2% of transaction value
  - Disadvantages
    - Does not work for small amount (too expensive)
    - Does not work for large amount (too expensive)
- Charge card
  - No spending limit
  - Entire amount charged due at end of billing period

Payment Acceptance and Processing

- Merchants must set up merchant accounts to accept payment cards
- Law prohibits charging payment card until merchandise is shipped
- Payment card transaction requires:
  - Merchant to authenticate payment card
  - Merchant must check with card issuer to ensure funds are available and to put hold on funds needed to make current charge
  - Settlement occurs in a few days when funds travel through banking system into merchant’s account

Processing a Payment Card Order

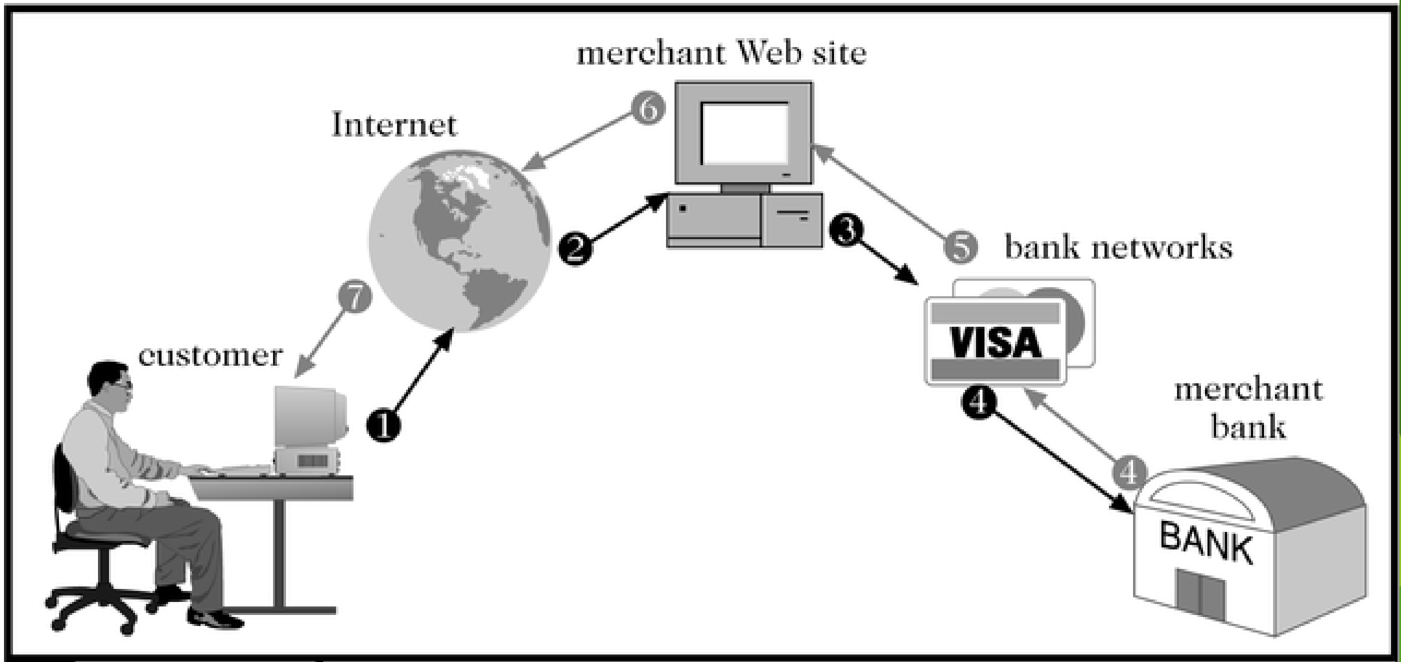


FIGURE 7-13 *Processing a payment card order*

Open and Closed Loop Systems

- Closed loop systems
  - Banks and other financial institutions serve as brokers between card users and merchants -- no other institution is involved
  - American Express and Discover are examples
- Open loop systems
  - Transaction is processed by third party
  - Visa and MasterCard are examples

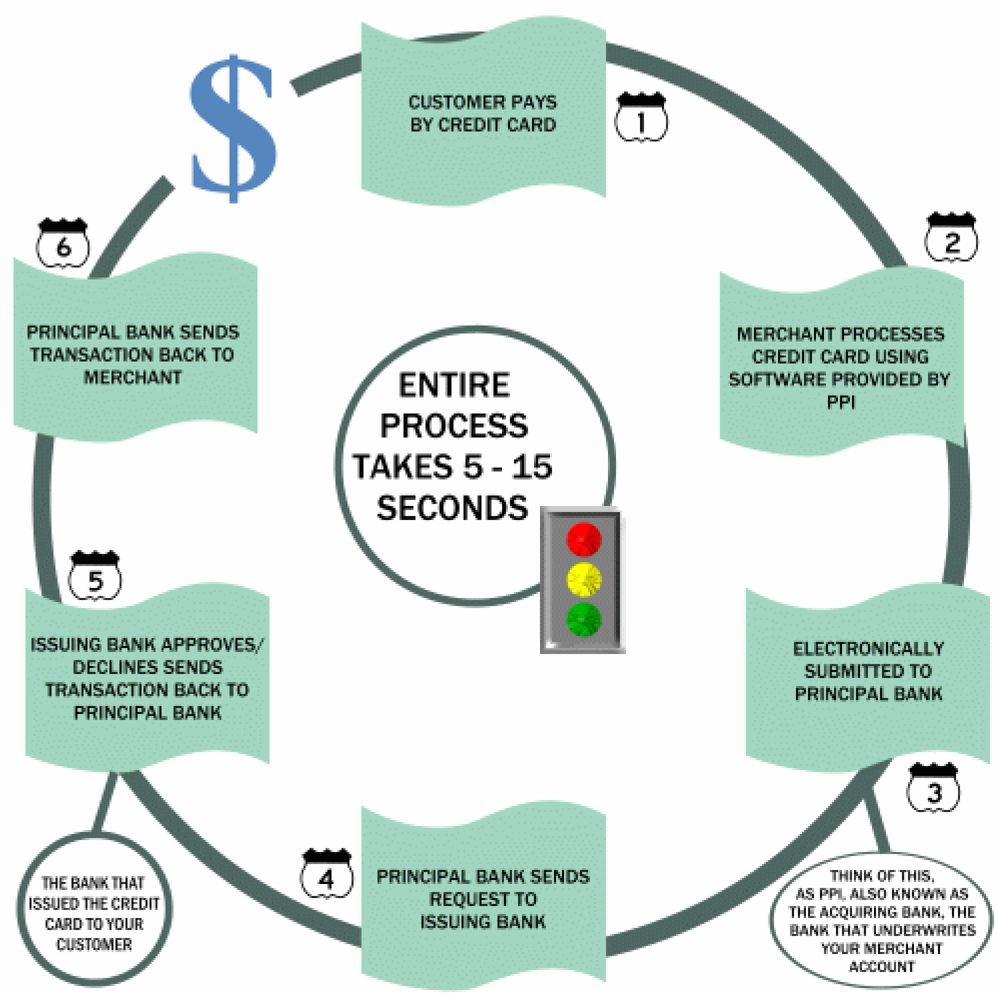
Setting Up Merchant Account

- Merchant bank
  - Also called acquiring bank
  - Does business with merchants that want to accept payment cards
  - Merchant receives account where they deposit card sales totals
  - Value of sales slips is credited to merchant’s account

Processing Payment Cards Online

- Can be done automatically by software packaged with electronic commerce software
- Can contract with third party to handle payment card processing
  - Can also pick, pack, and ship products to the customer
  - Allows merchant to focus on web presence and supply availability

Credit Card Processing



1 CUSTOMER PAYS BY CREDIT CARD

2 MERCHANT PROCESSES CREDIT CARD USING SOFTWARE PROVIDED BY PPI

3 ELECTRONICALLY SUBMITTED TO PRINCIPAL BANK

THINK OF THIS, AS PPI, ALSO KNOWN AS THE ACQUIRING BANK, THE BANK THAT UNDERWRITES YOUR MERCHANT ACCOUNT

4 PRINCIPAL BANK SENDS REQUEST TO ISSUING BANK

5 ISSUING BANK APPROVES/ DECLINES SENDS TRANSACTION BACK TO PRINCIPAL BANK

THE BANK THAT ISSUED THE CREDIT CARD TO YOUR CUSTOMER

6 PRINCIPAL BANK SENDS TRANSACTION BACK TO MERCHANT

ENTIRE PROCESS TAKES 5 - 15 SECONDS

SOURCE: PAYMENT PROCESSING INC.

Payment Processing Services

- Internetsecure
  - Provides secure credit card payment services
  - Supports payments with Visa and MasterCard
  - Provides risk management and fraud detection, and ensures all proper security for credit card transactions is maintained
  - Ensures all transactions are properly credited to merchant’s account

Payment Processing Services

- Tellan
  - Provides PCAuthorize for smaller commerce sites and WebAuthorize for larger enterprise-class merchant sites
  - Both systems capture credit card information from the merchant’s form and connect directly to the bank network using dial-up or private, leased lines
  - Bank network receives credit information, performs credit authorization, and deposits the money in the merchant’s bank account
  - The merchant’s web site receives confirmation or rejection of the transaction, which is communicated to the customer

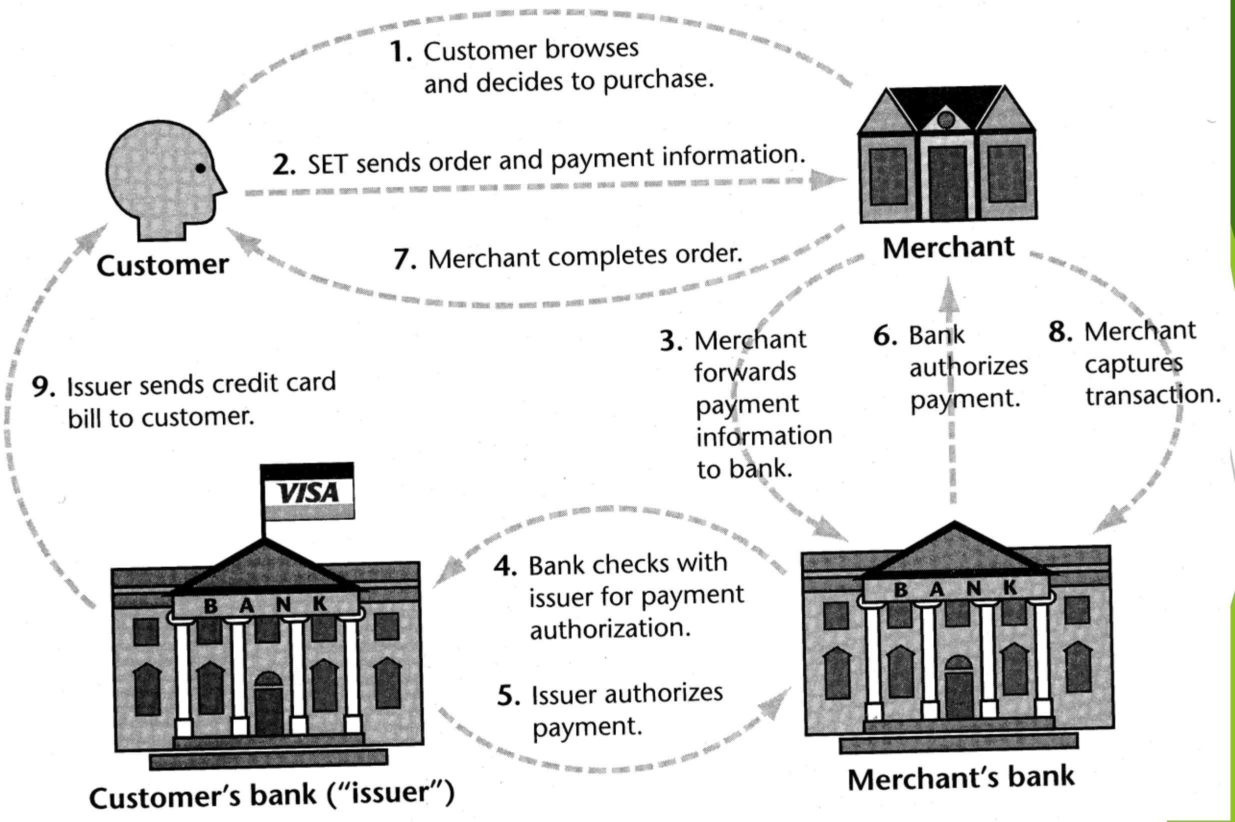
Payment Processing Services

- IC Verify
  - Provides electronic transaction processing for merchants for all major credit and debit cards
  - Also allows check guarantees and verification transactions
  - A CyberCash company
- Authorize.Net
  - Online, real time service that links merchants with issuing banks by simply inserting a small block of HTML code into their transaction page

Secure Electronic Transaction (SET) Protocol

- Jointly designed by MasterCard and Visa with backing of Microsoft, Netscape, IBM, GTE, SAIC, and others
- Designed to provide security for card payments as they travel on the Internet
  - Contrasted with Secure Socket Layers (SSL) protocol, SET validates consumers and merchants in addition to providing secure transmission
- SET specification
  - Uses public key cryptography and digital certificates for validating both consumers and merchants
  - Provides privacy, data integrity, user and merchant authentication, and consumer nonrepudiation

The SET protocol

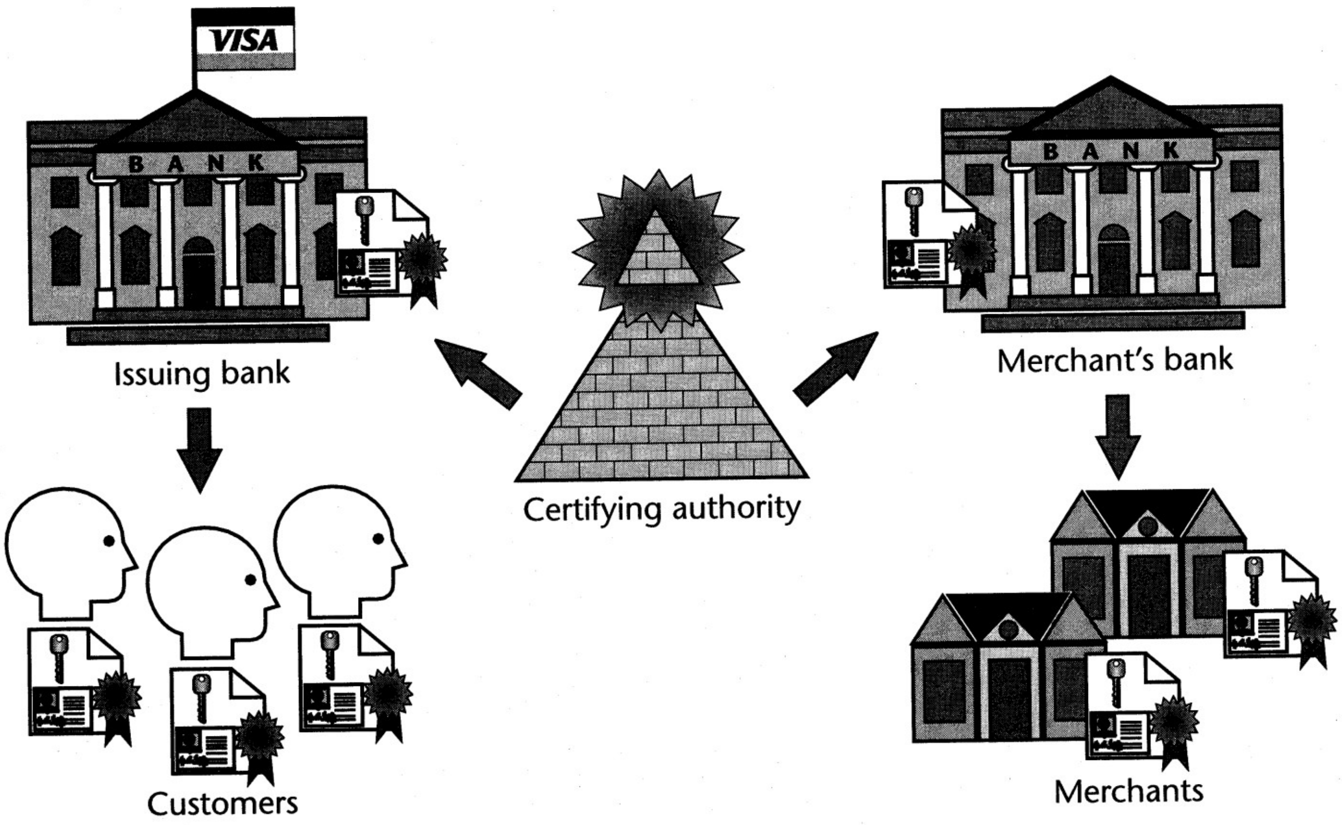

1. Customer browses and decides to purchase.
2. SET sends order and payment information.
7. Merchant completes order.
Customer
Merchant
3. Merchant forwards payment information to bank.
6. Bank authorizes payment.
8. Merchant captures transaction.
9. Issuer sends credit card bill to customer.
VISA
BANK
4. Bank checks with issuer for payment authorization.
5. Issuer authorizes payment.
BANK
Customer's bank ("issuer")
Merchant's bank

The SET protocol coordinates the activities of the customer, merchant, merchant's bank, and card issuer. [Source: Stein]

SET Payment Transactions

- SET-protected payments work like this:
  - Consumer makes purchase by sending encrypted financial information along with digital certificate
  - Merchant's website transfers the information to a payment card processing center while a Certification Authority certifies digital certificate belongs to sender
  - Payment card-processing center routes transaction to credit card issuer for approval
  - Merchant receives approval and credit card is charged
  - Merchant ships merchandise and adds transaction amount for deposit into merchant's account

SET uses a hierarchy of trust



All parties hold certificates signed directly or indirectly by a certifying authority. [Source: Stein]

SET Protocol

- Extremely secure
  - Fraud reduced since all parties are authenticated
  - Requires all parties to have certificates
- So far has received lukewarm reception
- 80 percent of SET activities are in Europe and Asian countries
- Problems with SET
  - Not easy to implement
  - Not as inexpensive as expected
  - Expensive to integrated with legacy applications
  - Not tried and tested, and often not needed
  - Scalability is still in question