Carnegie Mellon

Electronic Commerce and Payments

Marvin Sirbu

Department of Engineering and Public Policy

and

Graduate School of Industrial Administration

Carnegie Mellon University

Pittsburgh, Pa USA

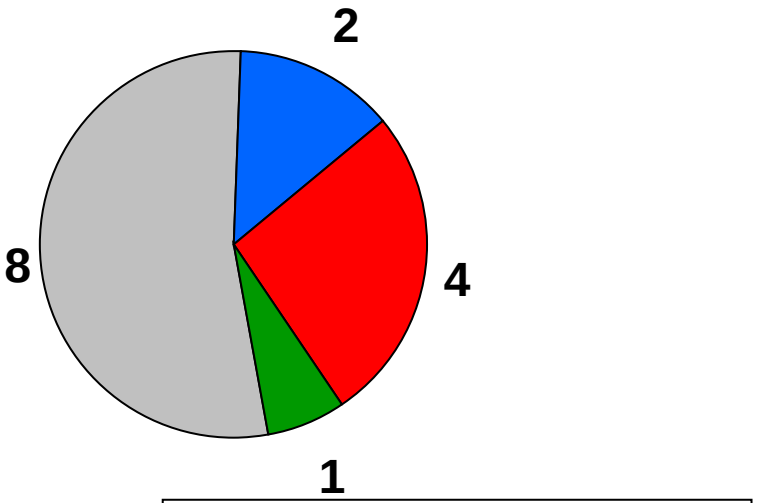
http://www.netbill.com

© 1997 Marvin A. Sirbu

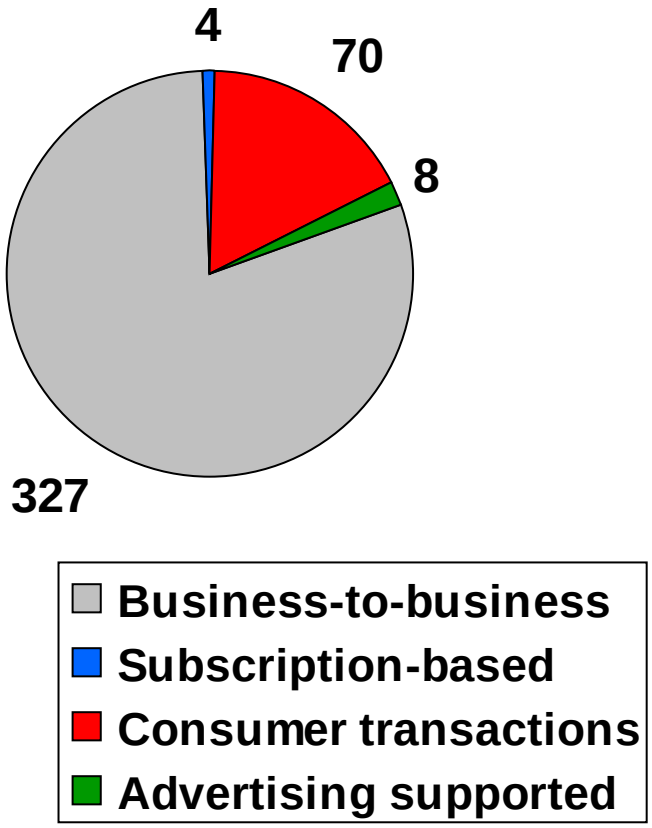
Carnegie Mellon

Internet Commerce Estimates

1997
$15 billion



2002
$409 billion



Source: Infoworld 9/8/97, p. 68

© 1997 Marvin A. Sirbu

Carnegie Mellon

Electronic Commerce

- **Many phases to a commercial transaction**
  - learning about what goods are available
  - finding potential suppliers
  - negotiating price
  - ordering goods
  - goods delivery
  - payment
  - after sales support

© 1997 Marvin A. Sirbu

Carnegie Mellon

Internet Support for Commerce

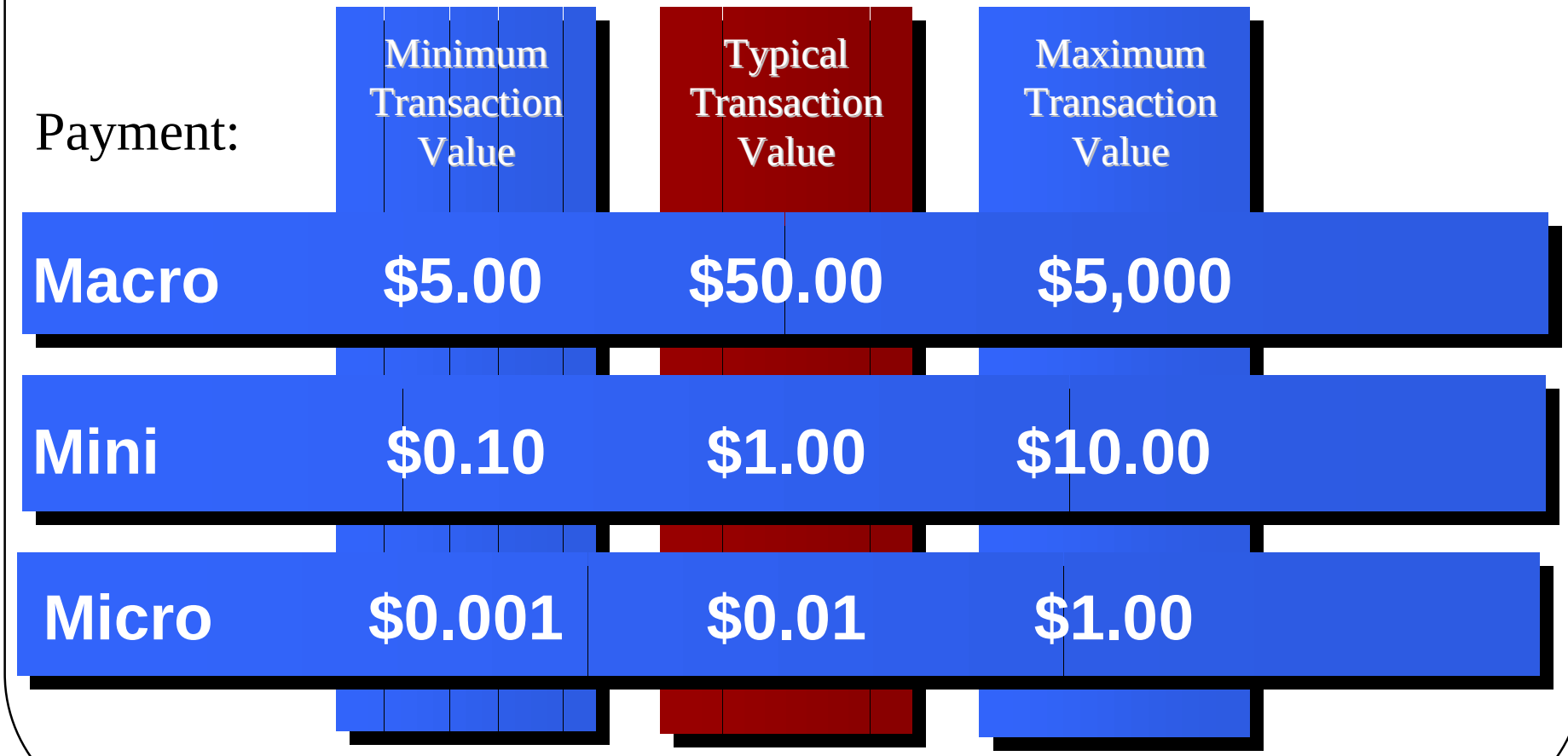
- **The Internet supports all phases**

product learning	bboards, newswire services WWW
finding suppliers	Search engines, Nets Inc.
negotiating price	email, EDI, auctions, NetBill
ordering goods	WWW, email
goods delivery	direct delivery of "soft" goods
payment	multiple methods
after sales support	WWW, email, shared whiteboards

© 1997 Marvin A. Sirbu

Carnegie Mellon

Internet Payment Transaction Ranges



Source: Digital Equipment Corporation

© 1997 Marvin A. Sirbu

Carnegie Mellon

Electronic Information Market Structures

Market Structure	Paper Analog	Electronic Market
Publisher pays	Mail order catalogs	WWW catalogs
Advertiser pays	Free weekly paper	Search engines, ‘zines
Club pays	Corporate library	Site license
Personal subscription	Professional magazine	WSJ, ESPN
Pay per item	Books, newstand sales	Cybercoin, GlobeID, NetBill
Time-based payments	Rental library	CompuServe
Mixed ads + per item	Newspapers	AOL

© 1997 Marvin A. Sirbu

Carnegie Mellon

Advertising on the Web

- **Current payments range from $10-$20/thousand "impressions"**
  - 1¢ to 2¢ each
- **Advertising to support low value information**
  - no transaction processing overhead
- **Third party agencies will place ads on small web sites**
  - *e.g.* DoubleClick.net

© 1997 Marvin A. Sirbu

Carnegie Mellon

Payment Systems

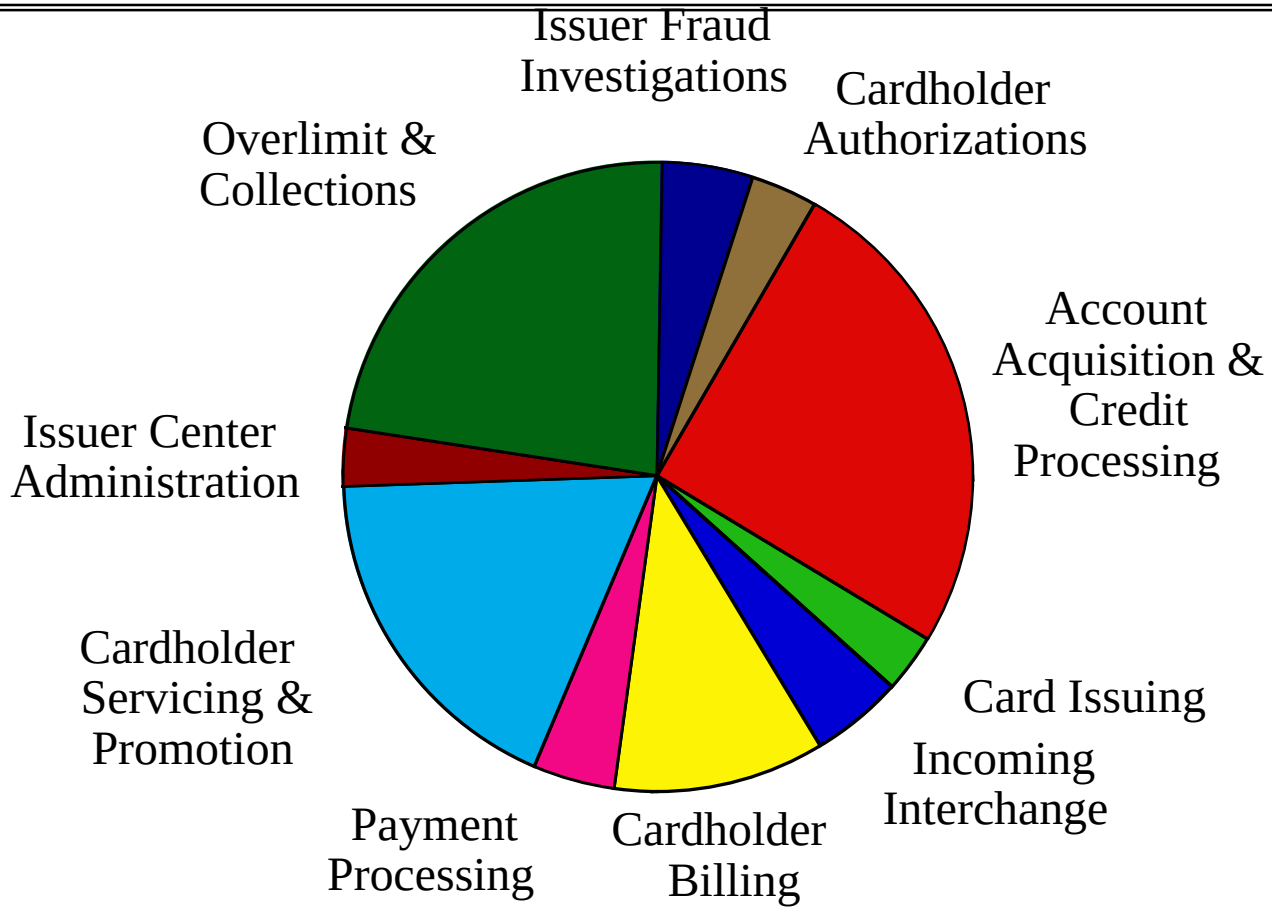
There are two kinds of money

- **Token money: tokens which represent value**
  - tokens can be exchanged for goods
- **Notational money: ledger entries in Demand Deposit Accounts**
  - money is transferred between accounts upon instruction
    - *e.g.* by a check
  - clearing required if accounts are at different institutions
  - accounts may have negative balances
    - *e.g.* credit card accounts

© 1997 Marvin A. Sirbu

Carnegie Mellon

Financial Transaction System-Cost Structure



© 1997 Marvin A. Sirbu

Carnegie Mellon

Payment System Costs

- **Dispute resolution costs**
  - non delivery (Internet is unreliable)
  - processing refunds
- **Credit risk**
  - losses due to overdrawn debit (credit) account vs costs of real time verification
- **Record keeping costs**
  - statements
- **Communication and processing costs**
  - number of messages
  - cryptographic processing
  - privacy protection
- **Costs of availability**
  - realtime versus deferrable communications

© 1997 Marvin A. Sirbu

Carnegie Mellon

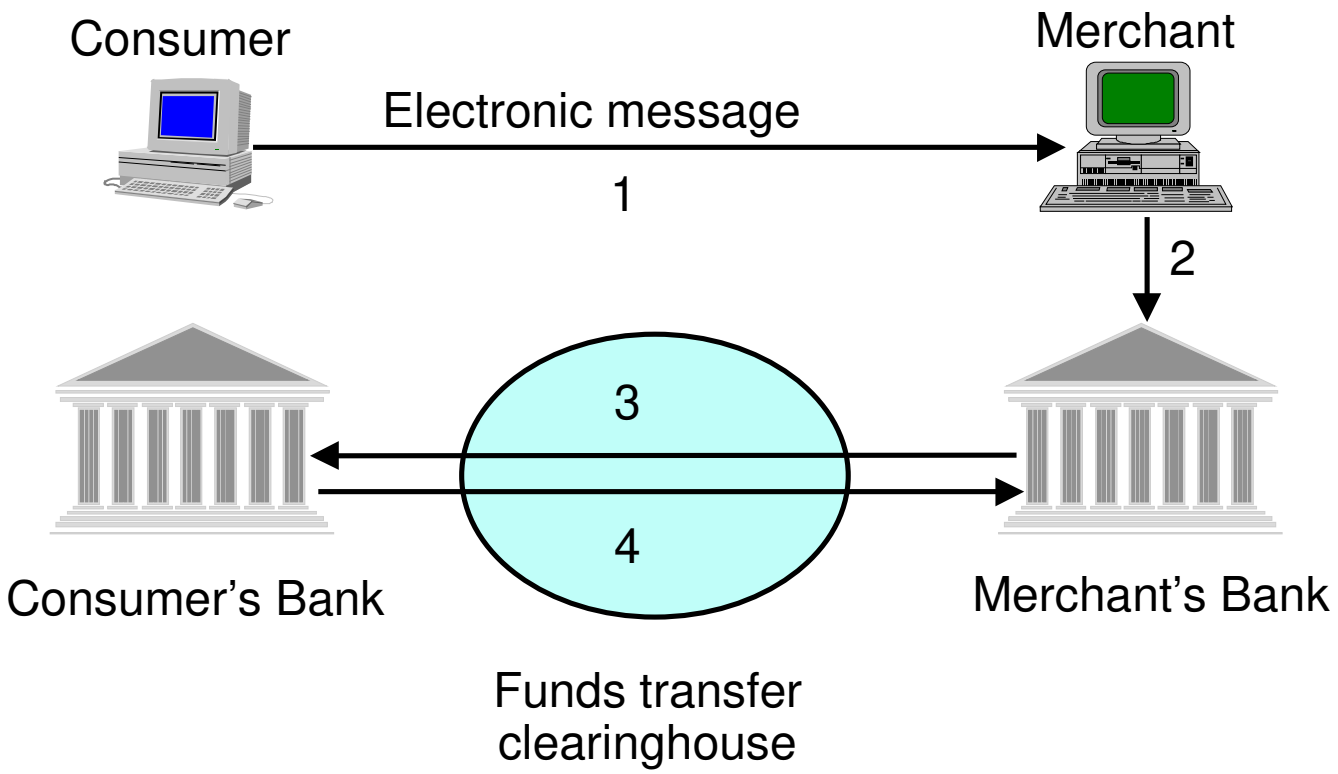
Transaction costs: key issues

- **Exception handling costs dominate normal processing costs**
  - high reliability, accuracy are critical
  - automated complaint handling tools are critical

© 1997 Marvin A. Sirbu

Carnegie Mellon

Risk Management in Electronic Payment



© 1997 Marvin A. Sirbu

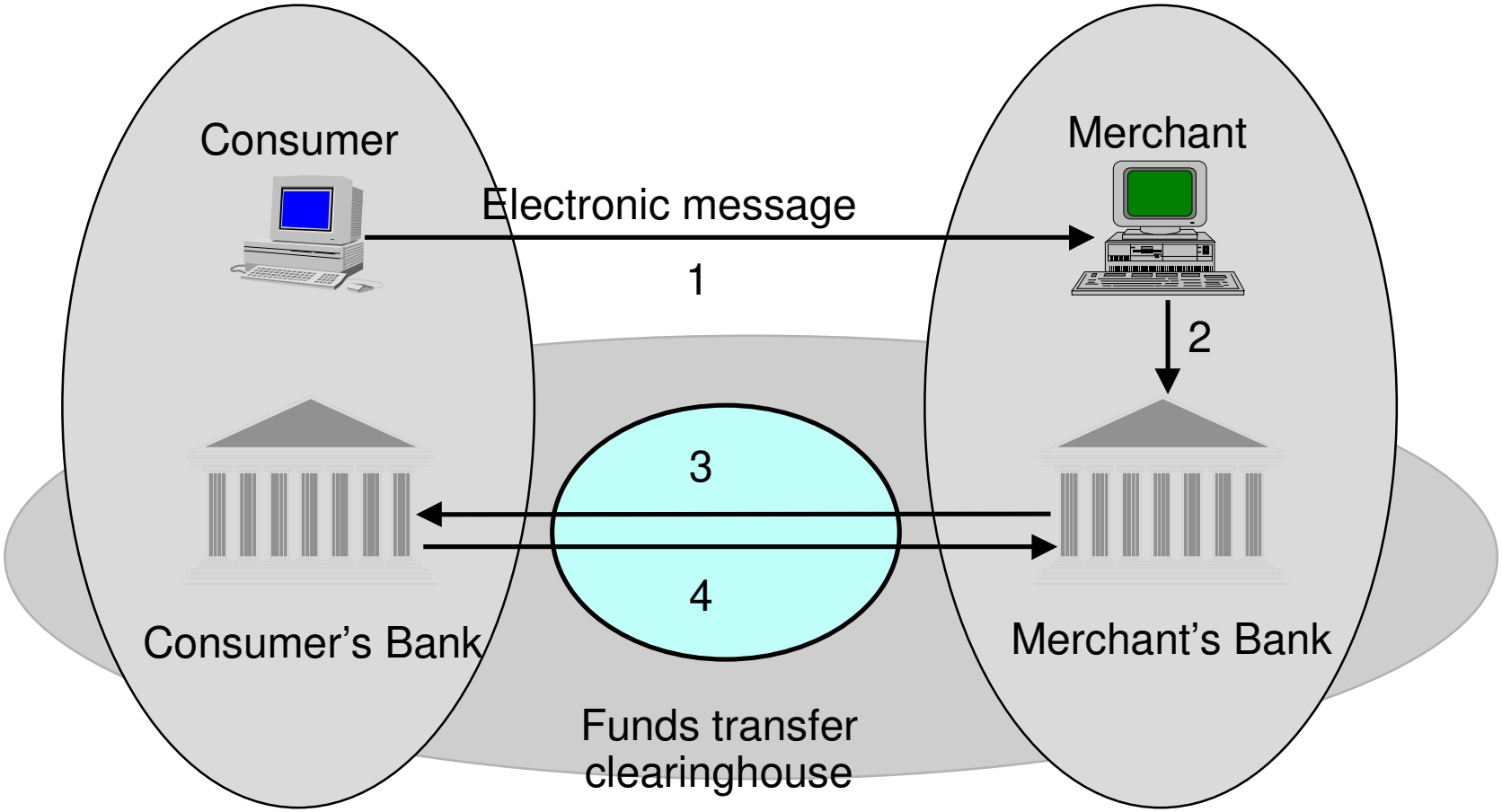
Carnegie Mellon

Risk Management Issues in Electronic Payment

- When is a transaction final?
- What recourse is available if goods are faulty or not delivered?
- When are funds available to merchant?
- When are funds received from consumer?
- Who vouches for identity of customer?
- Who vouches for identity of merchant?
- Who vouches for banks to each other?

© 1997 Marvin A. Sirbu

Domains of Trust



© 1997 Marvin A. Sirbu

Carnegie Mellon

Domains of Trust: Credit Cards

- **Consumer<==C bank**
  - Consumer's Bank trusts consumer to pay credit card debt
  - Consumer trusts bank to stop payment if merchandise bad
- **Merchant <==> Merchant's acquirer bank**
  - Merchant trusts bank will pay on properly authorized transactions
  - Bank trusts merchant will not submit phony invoices
- **Consumer's Bank <==>Card Association<==>Merchant's Bank**
  - Merchant trusts Consumer's bank to settle
  - Consumer's bank trusts merchant's bank to make good merchant's commitment

© 1997 Marvin A. Sirbu

Carnegie Mellon

Examples

- **Credit Cards**
  - Merchant bank guarantees to merchant payment for approved transactions
  - Consumer bank guarantees to merchant bank payment for approved transactions
  - Merchant bank guarantees to customer's bank a refund if goods not delivered
- **Checks**
  - Merchant bank guarantees to merchant contingent on funds from consumer's bank
  - Consumer bank guarantees to merchant bank payment contingent on funds available
  - Merchant bank makes no guarantees to customer's bank of refund if goods not delivered

© 1997 Marvin A. Sirbu

Carnegie Mellon

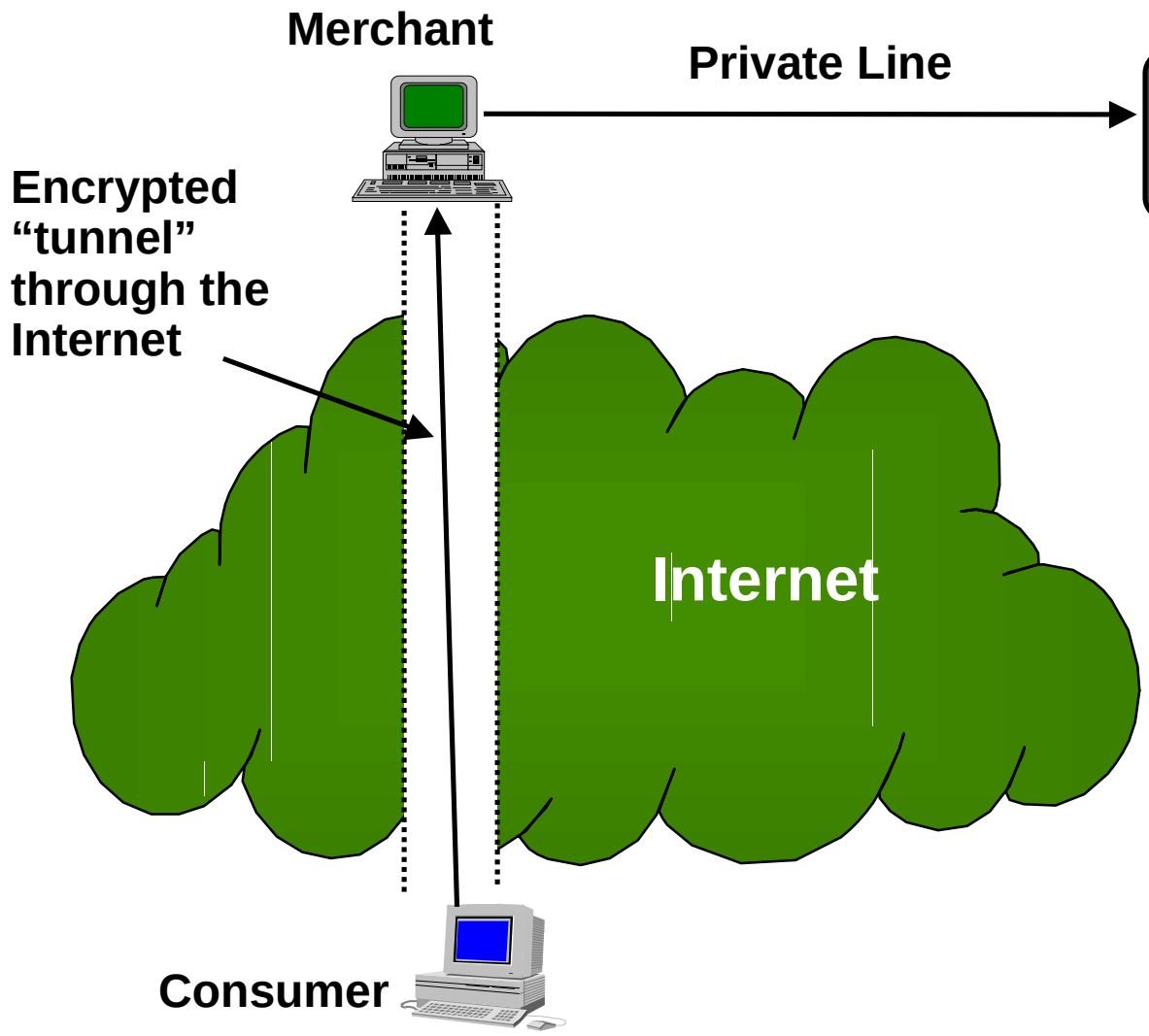
Internet-Based Payment Models

- **Secure transmission of credit card information**
- **Digital cash**
- **Digital checks**
- **Centralized online aggregation account**

© 1997 Marvin A. Sirbu

Carnegie Mellon

Credit Card Info Sent Direct to Merchant (Netscape Model)

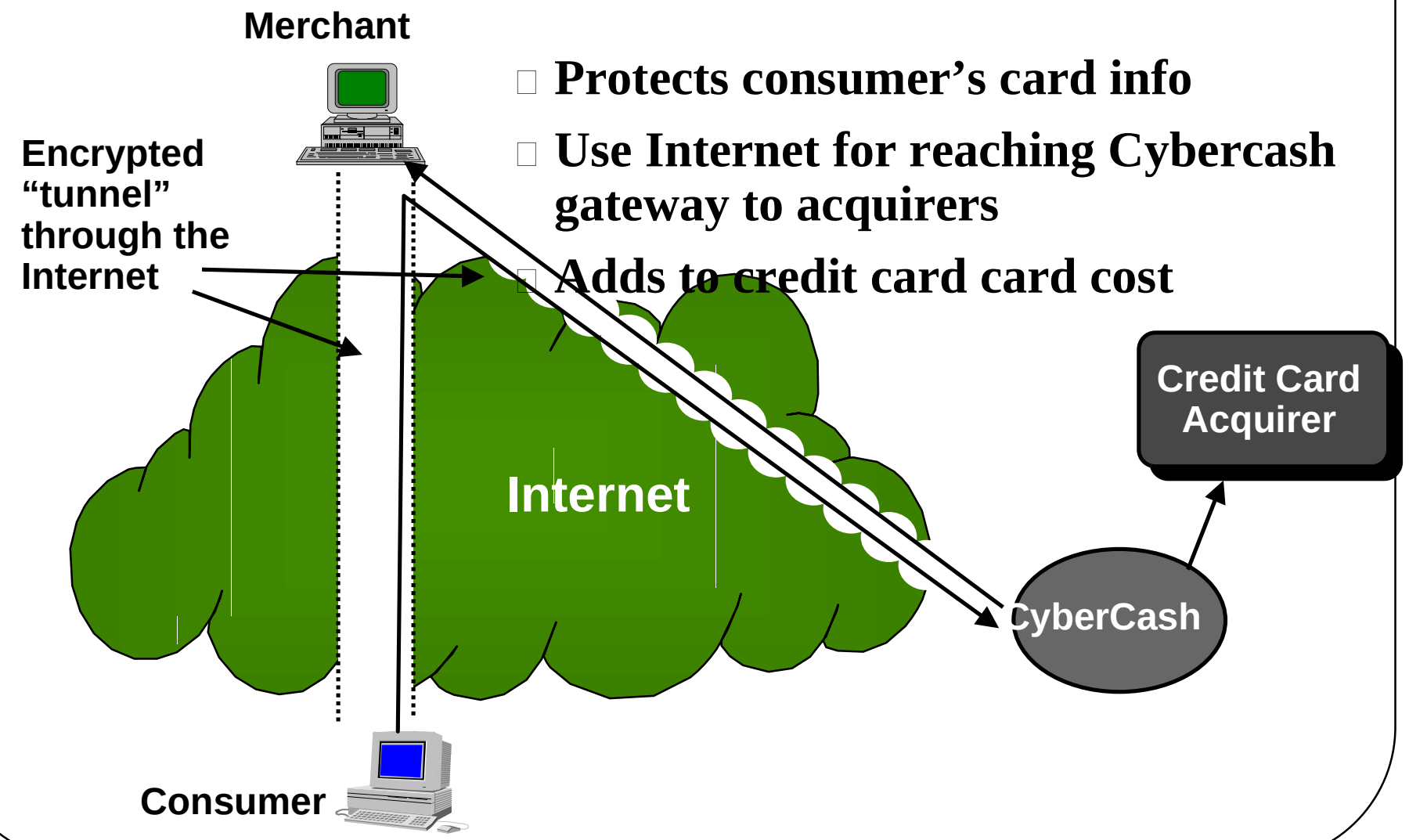


- Consumer sends card # direct to merchant
- Similar to today's phone order
- Must trust merchant with card info
- High transaction costs

© 1997 Marvin A. Sirbu

Carnegie Mellon

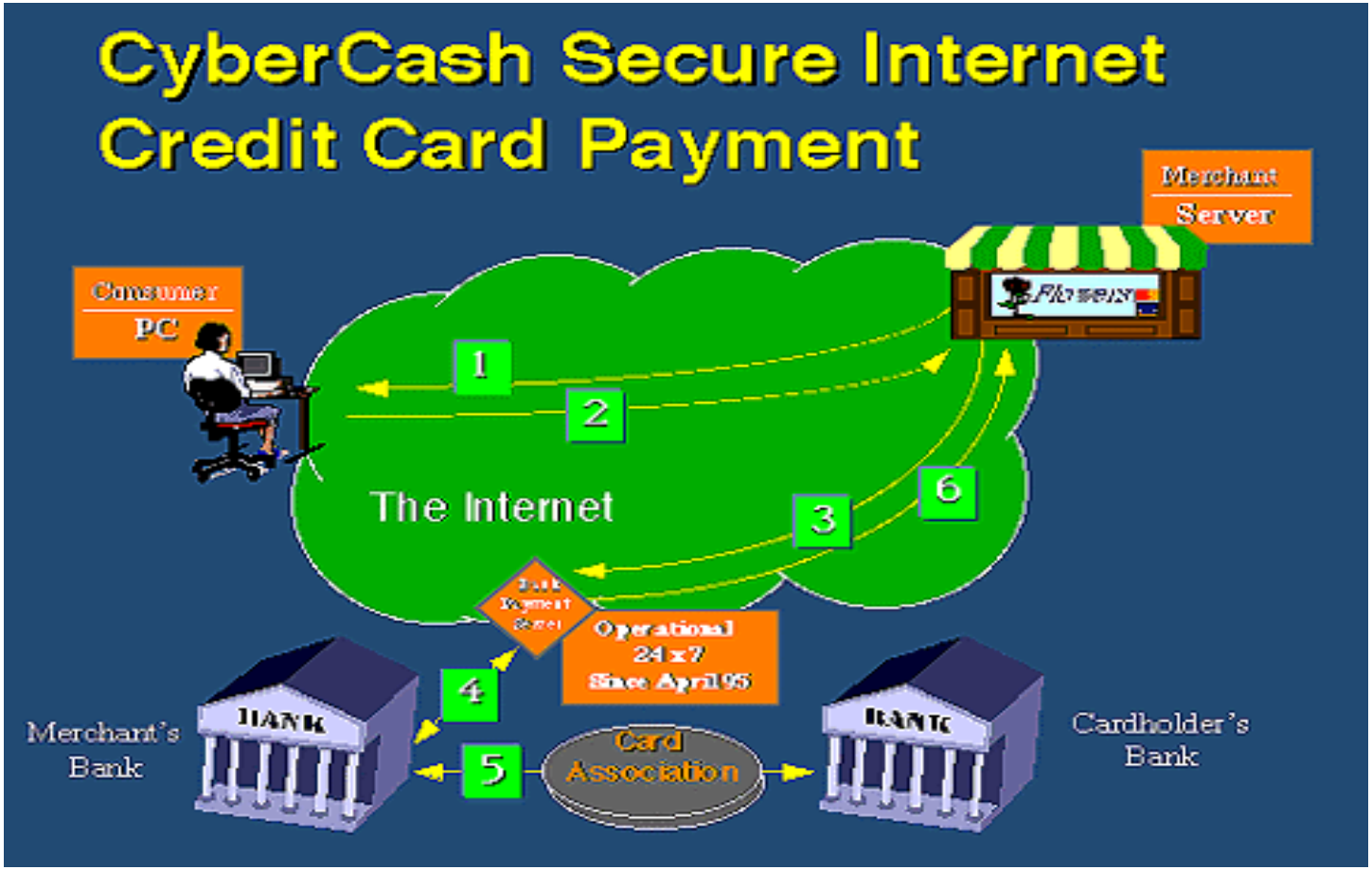
Third Party Intermediary Model (CyberCash)



- Protects consumer's card info
- Use Internet for reaching Cybercash gateway to acquirers
- Adds to credit card card cost

© 1997 Marvin A. Sirbu

CyberCash Credit Card Transactions



copyright CyberCash, Inc.

Carnegie Mellon

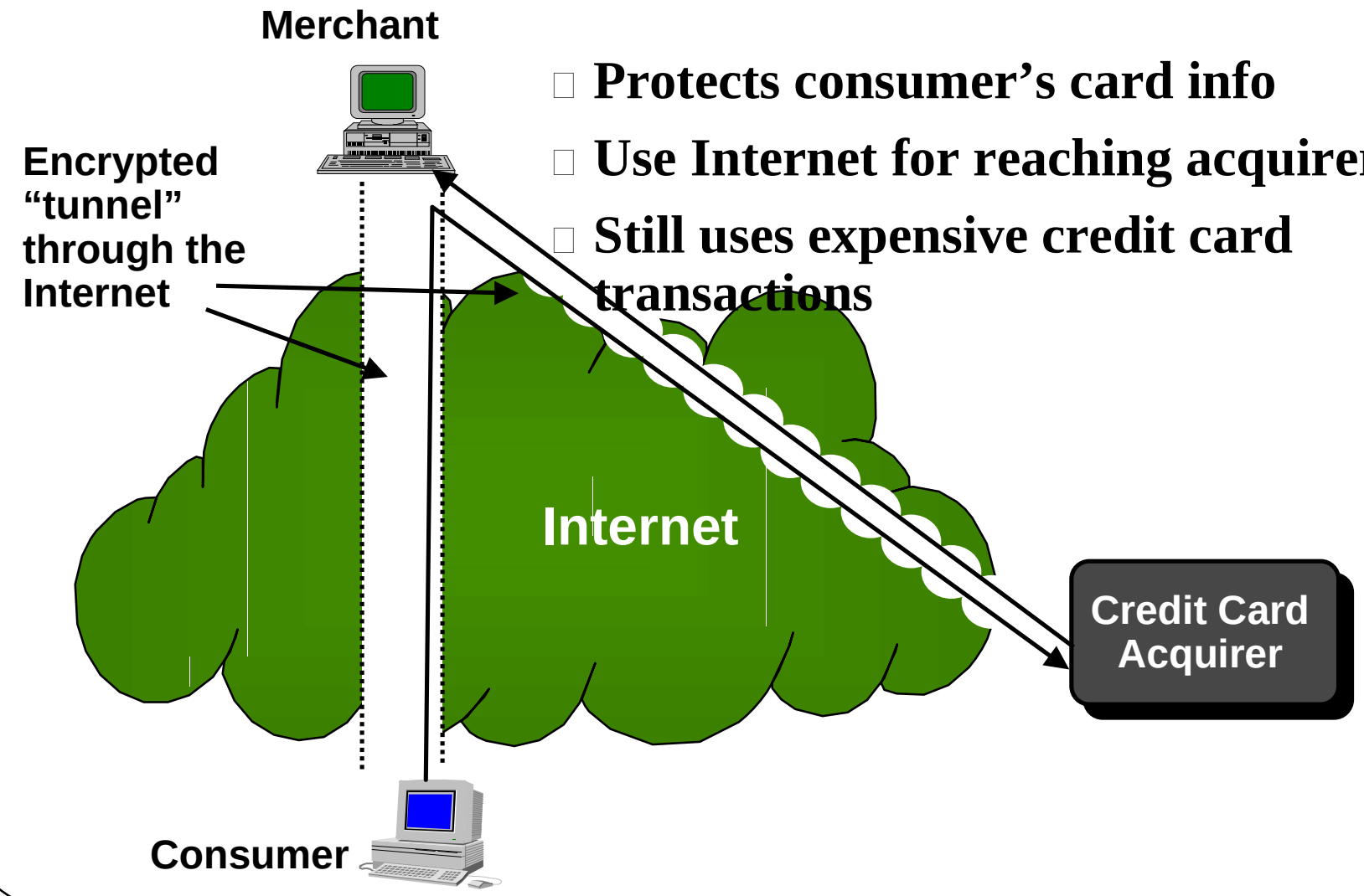
Cybercash Protocol

- Both consumer and merchant have public key pairs.
- Cybercash gateway maintains list of public keys of consumers and merchants
- Consumer uses her private key to sign payment authorization and hash of transaction description
- Merchant uses his private key to sign invoice
- Cybercash verifies both signatures before communicating with bank.
- Impossible for merchant to forge consumer's signature

© 1997 Marvin A. Sirbu

Carnegie Mellon

Credit Card Acquirer On the Net (SET)



- Protects consumer's card info
- Use Internet for reaching acquirer
- Still uses expensive credit card transactions

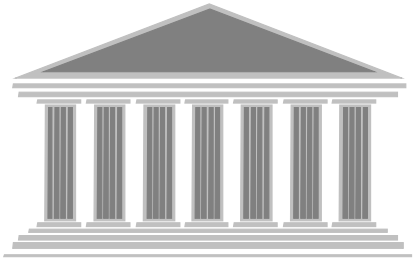
© 1997 Marvin A. Sirbu

SET Protocol

Consumer

Merchant

1. Request Transaction
2. Acknowledge request
3. Purchase Order
4. Purchase Order Verification
7. Status query
8. Purchase status information
5. Customer payment data
6. Verify customer data
9. Request Payment
10. Verify Payment



Merchant Acquirer Bank

© 1997 Marvin A. Sirbu

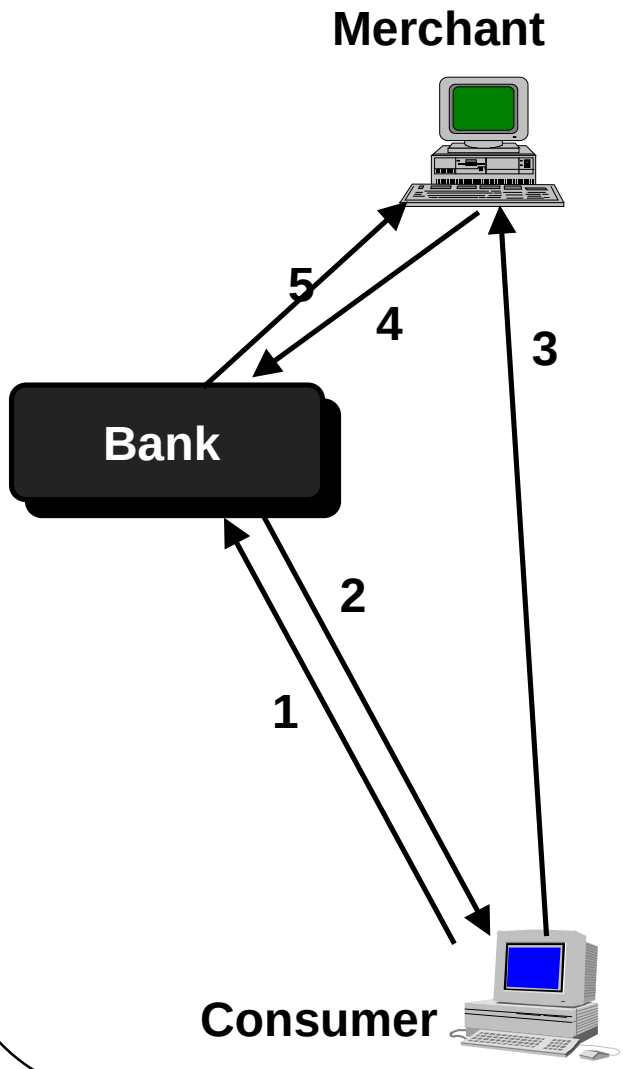
Carnegie Mellon

Why Has SET Been Delayed?

- **Visa and MasterCard initiated separate protocol efforts**
- **SET is complex**
  - reflects complex credit card association operating rules
  - distinct national features
  - much complexity is in Public Key Infrastructure portions
- **Difficulties in allocating economic costs and benefits**
  - Savings due to reduced fraud accrue to acquirer banks
  - Costs borne by card issuers, merchants, consumers

© 1997 Marvin A. Sirbu

Digicash Model



1- Consumer asks Bank for Digicash

2- Bank sends Digicash bits to consumer

3- Consumer sends Digicash to merchant in payment

4- Merchant checks that Digicash has not been double spent

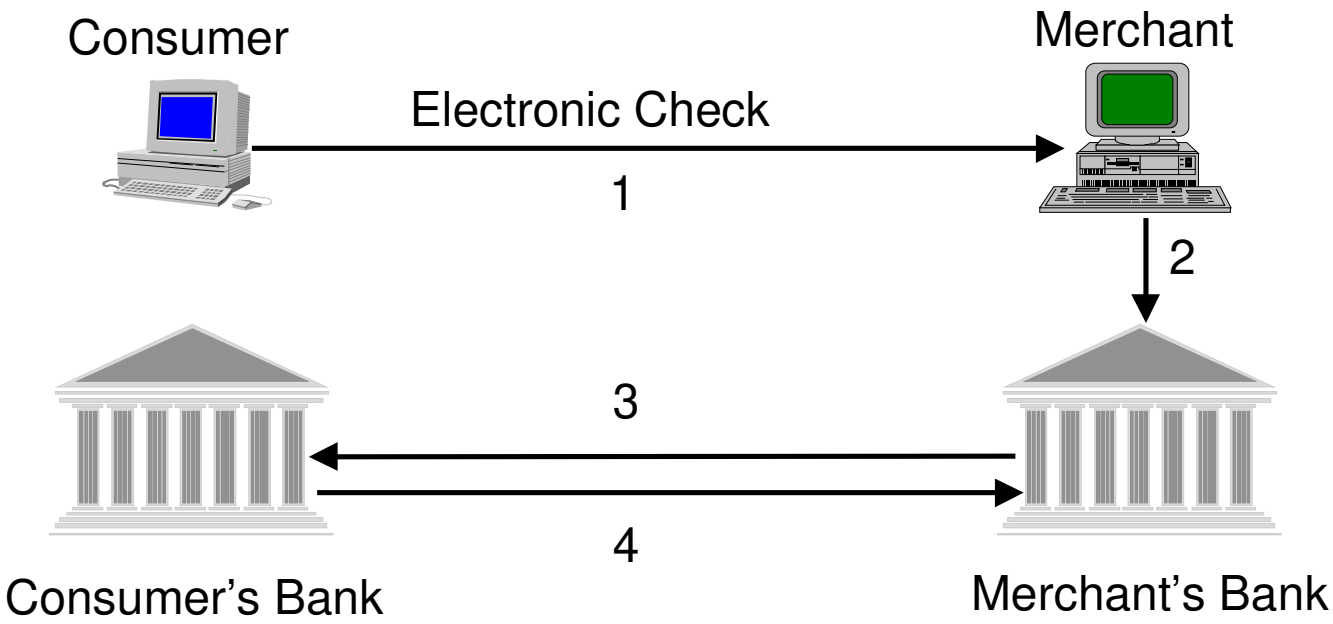
5- Bank verifies that Digicash is valid

- **Advantages**
  - Privacy, Scalability
- **Disadvantages**
  - Complexity
    - Detecting double spending
    - Robustness against failure
  - Accountability

© 1997 Marvin A. Sirbu

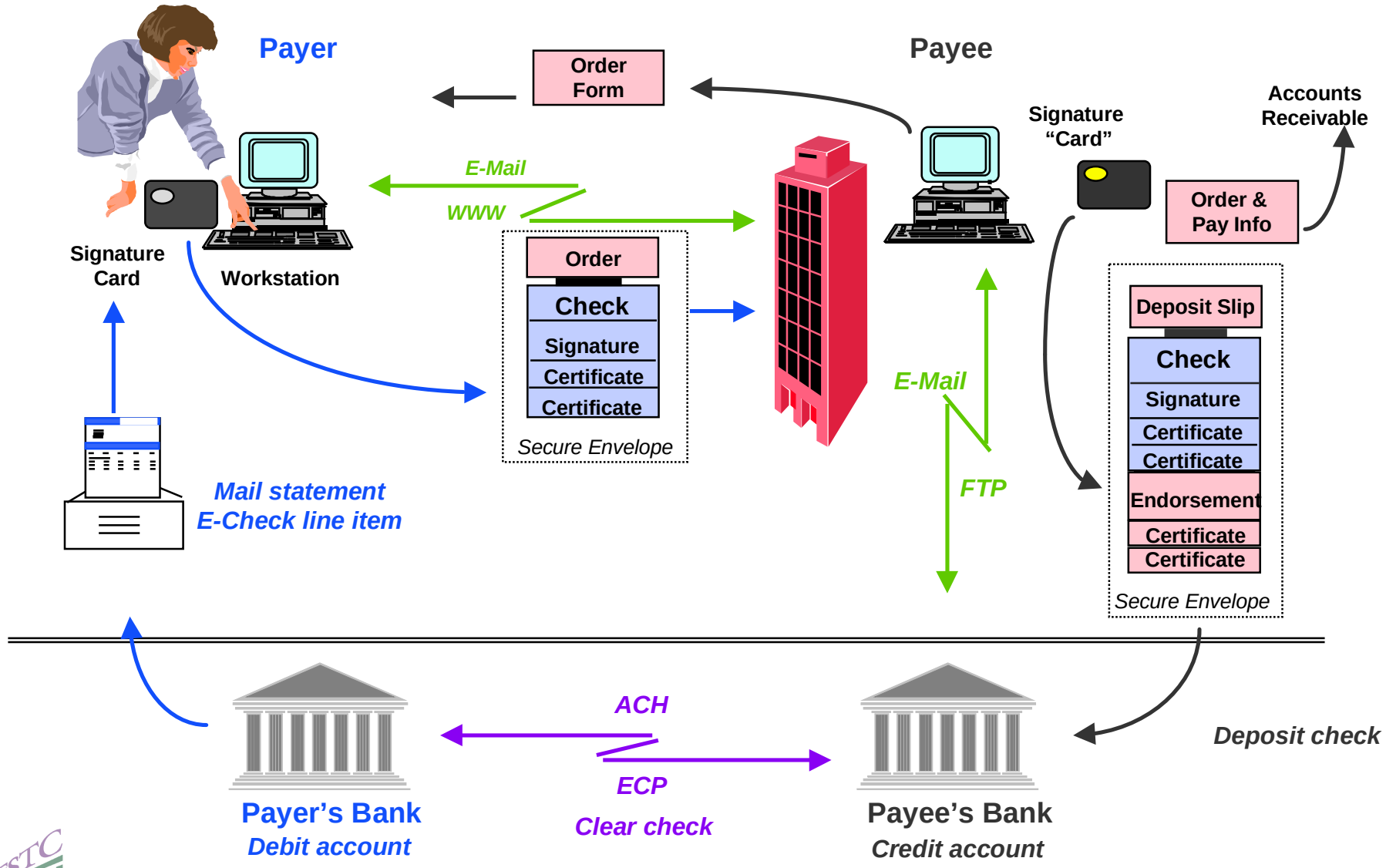
Approach: Digital Checks

- Consumers issue signed drafts on online bank accounts
- Merchants may do online or delayed clearing
- Clear through existing bank systems, *e.g.* ACH
- May attach remittance information



© 1997 Marvin A. Sirbu

Electronic Check Concept



© 1995 Financial Services Technology Consortium

Carnegie Mellon

FSTC Electronic Check

- **Electronic Checkbook:**
  - PCMCIA, Smart Card, PIN protected
  - Key storage
  - Signature and transaction logging
- **Digital signatures: signing and endorsing**
- **Digital certificates: authenticate payor, payor bank and bank account**

© 1997 Marvin A. Sirbu

Carnegie Mellon

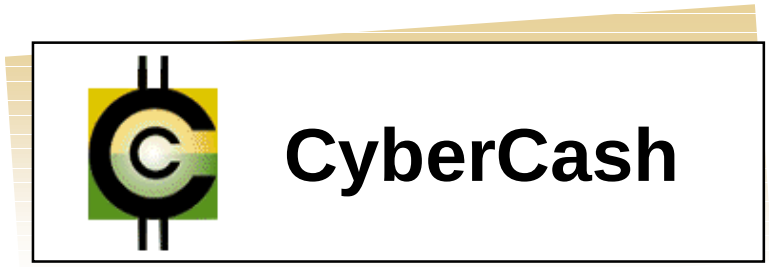
Approach: Online Aggregation Accounts

- **Funds transfer between accounts at a central server**
  - All accounts at the central server
  - Prepaid or postpaid consumer accounts
- **Advantages**
  - Low transaction overhead cost
- **Disadvantages**
  - Scalability: server may become a bottleneck
  - Requires arrangement with accounting server
- **Example: NetBill, AOL, CyberCoin, Globe ID**

© 1997 Marvin A. Sirbu

CyberCash

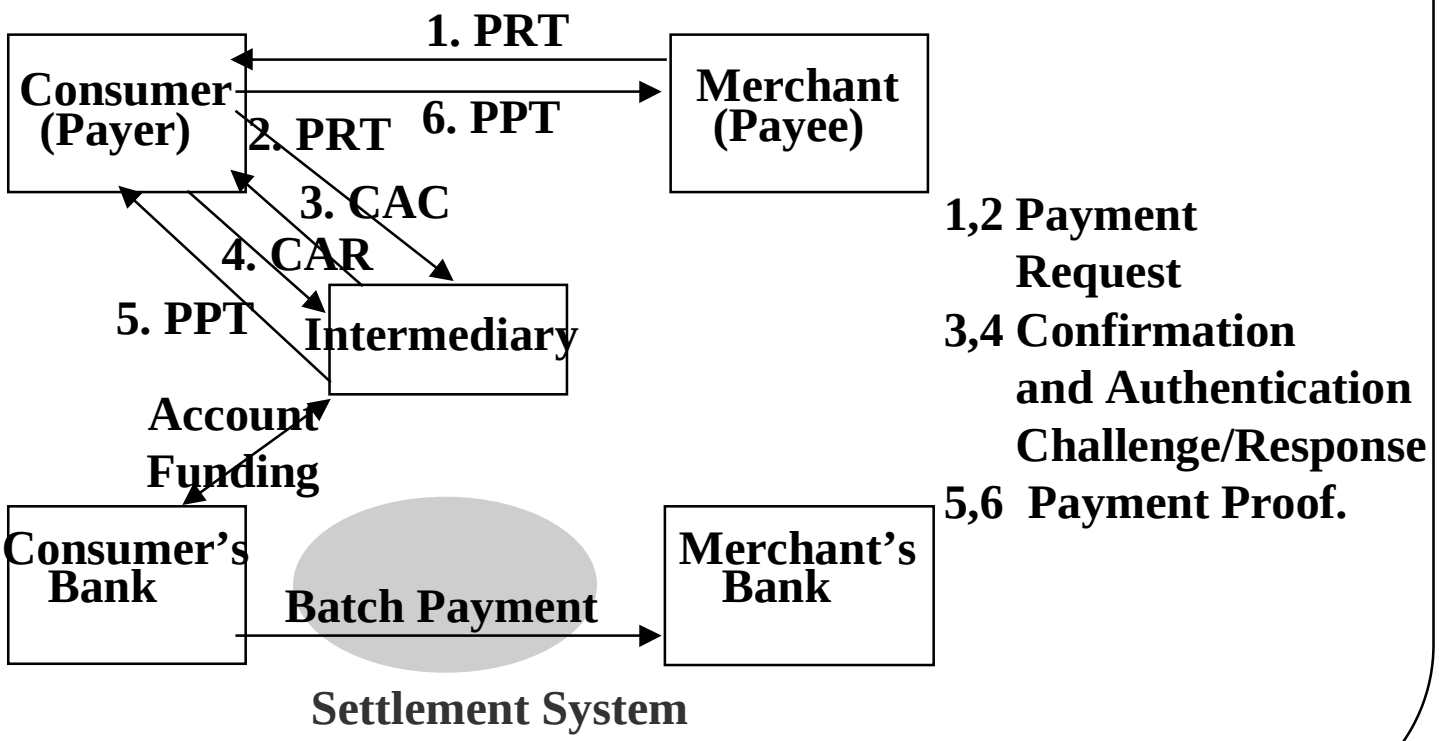
- **CyberCoin:**
  - Announced 9/30/96
- **Transactions:**
  - Values down to 25 cents
  - Cost down to 8 cents
- **Other Attributes:**
  - US only for now
  - Centralized detection of double spending
  - All transaction clear through CyberCash
- **Also focused on credit cards and checks**



© 1997 Marvin A. Sirbu

GlobeID

- Uses Technology from GC Tech
- Online accounting server



© 1997 Marvin A. Sirbu

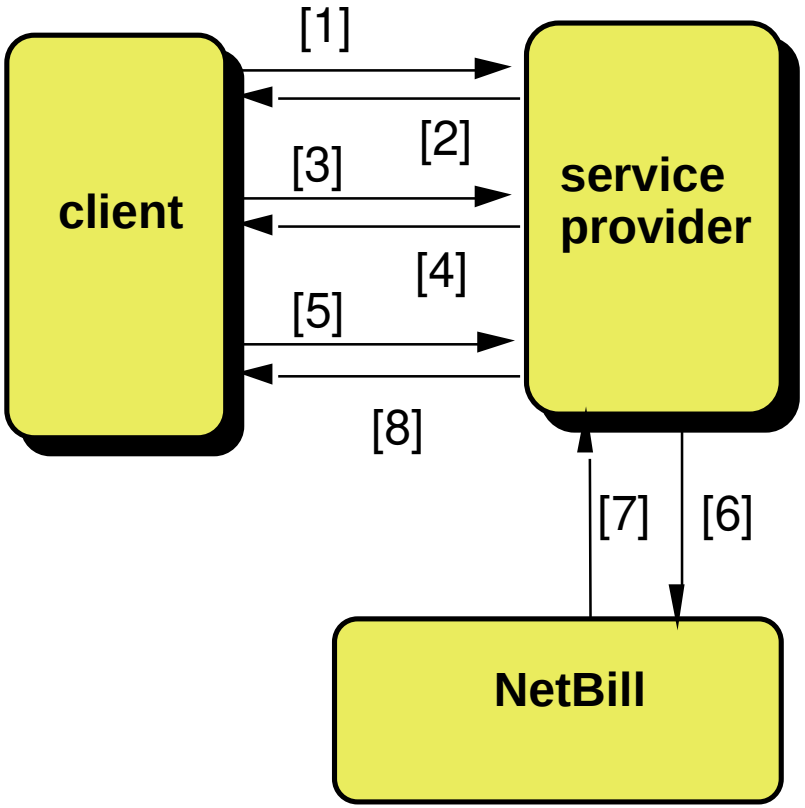
Carnegie Mellon

NetBill

- **NetBill maintains accounts for both consumers and merchants**
  - microtransactions clear through online account server
  - fund accounts through credit cards or electronic checks
- **Atomic transactions**
  - money atomic
  - goods atomic
  - non repudiation
  - uses strong cryptography
- **Support for Flexible Pricing, Access Control**
  - site licenses
  - subscriptions
  - pay per view
- **Automated support operations**

Carnegie Mellon

NetBill Protocol



1. Client Requests a Price Quote
2. Service Provider Makes an Offer
3. Client Accepts Offer
4. Goods delivered encrypted
5. Receipt acknowledged
6. Transaction submitted
7. Transaction approved
8. Key delivered

© 1997 Marvin A. Sirbu

Carnegie Mellon

Strong Service Guarantees

- **Money atomic: money cannot be lost or created due to machine or network failure**
  - digicash coins can be lost
- **Goods atomic: Customer is guaranteed to be charged if and only if information goods are delivered successfully**
  - Uses certified delivery
- **Non repudiation:**
  - Merchant can prove what the consumer ordered
  - Consumer can prove what the merchant delivered

© 1997 Marvin A. Sirbu

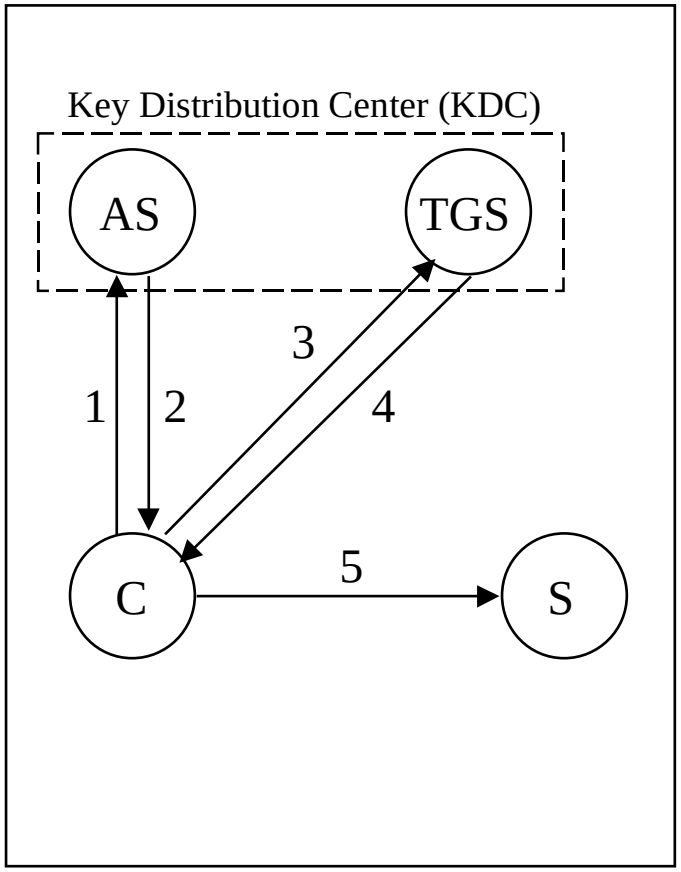
Carnegie Mellon

Secure Communication Using PK-Kerberos

- **All NetBill communications protected under Kerberos Session Keys**
  - provides mutual authentication as well as privacy
- **Session Keys issued via public key operations directly between client and server**

Carnegie Mellon

Traditional Kerberos



1. AS-REQ: C, TGS, Ts1
2. AS-REP: $\{K_{c,tgs}, TGS, Ts1\}K_c$, $T_{c,tgs}$
3. TGS-REQ: C, S, Ts2, $T_{c,tgs}$, $\{auth\}K_{c,tgs}$
4. TGS-REP: C, $\{K_{c,s}, S, Ts2\}K_{c,tgs}$, $T_{c,s}$
5. AP-REQ: $T_{c,s}$, $\{C, Ts3\}K_{c,s}$

where

$T_{c,tgs} = TGS, \{K_{c,tgs}, C, T_{auth}\}K_{tgs}$

is the ticket granting ticket;

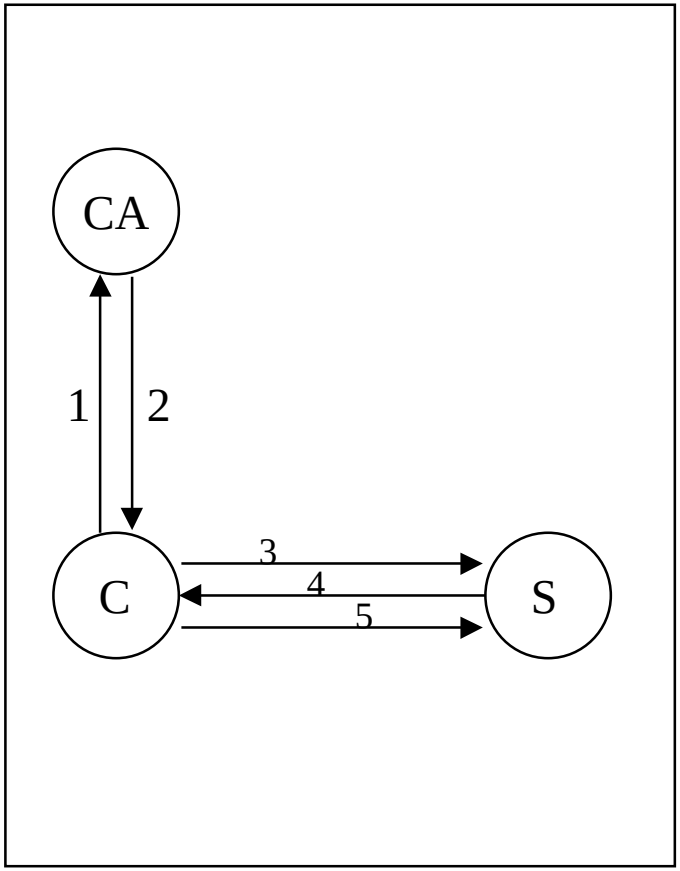
$T_{c,s} = S, \{K_{c,s}, C, T_{auth}\}K_{s,tgs}$

is the service ticket.

© 1997 Marvin A. Sirbu

Carnegie Mellon

Public Key Kerberos



1. SCERT-REQ: S
2. SCERT-REP: scert
3. PKTGS-REQ: S, T_{auth},
   $\{K_r,C,ccert,\{S,T_{auth},K_r,PK_s\}^PK_c\}PK_s$
4. PKTGS-REP: $\{C,S,K_{c,s},T_{auth}\}K_r$, $T_{c,s}$
5. AP-REQ: $T_{c,s}$, $\{C,Ts1\}K_{c,s}$

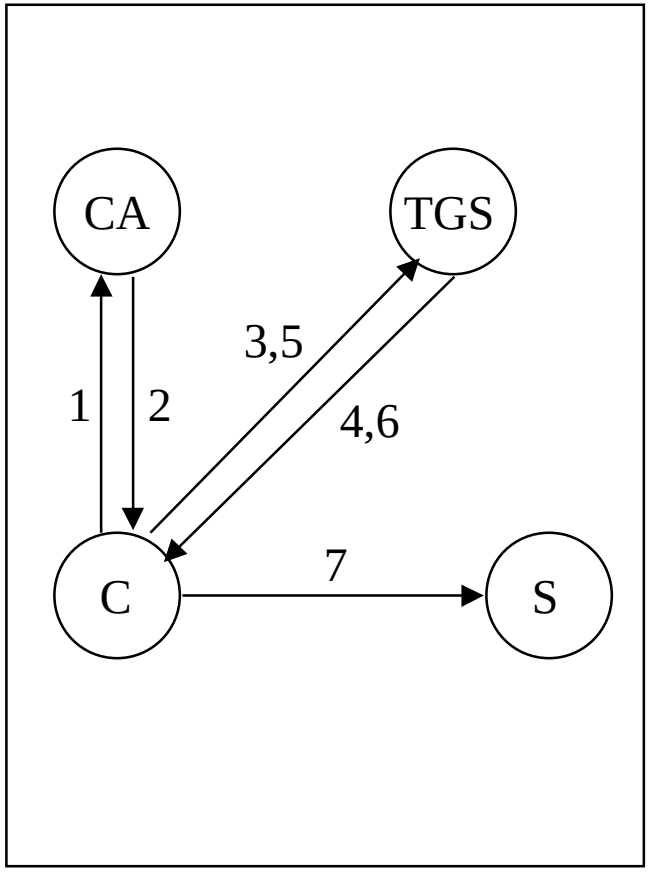
where ticket

$T_{c,s} = S,\{K_{c,s},C,T_{auth}\}K_s$

© 1997 Marvin A. Sirbu

Carnegie Mellon

PK Kerberos (via TGS)



1. SCERT-REQ: TGS
2. SCERT-REP: tgs-cert
3. PKTGS-REQ: TGS, T_{auth},
   $\{K_r,C,ccert,\{TGS,T_{auth},K_r,PK_{tgs}\}\text{^}PK_c\}PK_{tgs}$
4. PKTGS-REP: $\{C,TGS,K_{c,tgs},T_{auth}\}K_r$, $T_{c,tgs}$
5. TGS-REQ: C, S, Ts1, $T_{c,tgs}$, $\{auth\}K_{c,tgs}$
6. TGS-REP: C, $\{K_{cs},S,Ts1\}K_{c,tgs}$, $T_{c,s}$
7. AP-REQ: $T_{c,s}$, $\{C,Ts2\}K_{c,s}$

where

$T_{c,tgs} = TGS,\{K_{c,tgs},C,T_{auth}\}K_{tgs}$
is the ticket granting ticket;

$T_{c,s} = S,\{K_{c,s},C,T_{auth}\}K_{s,tgs}$
is the service ticket.

© 1997 Marvin A. Sirbu

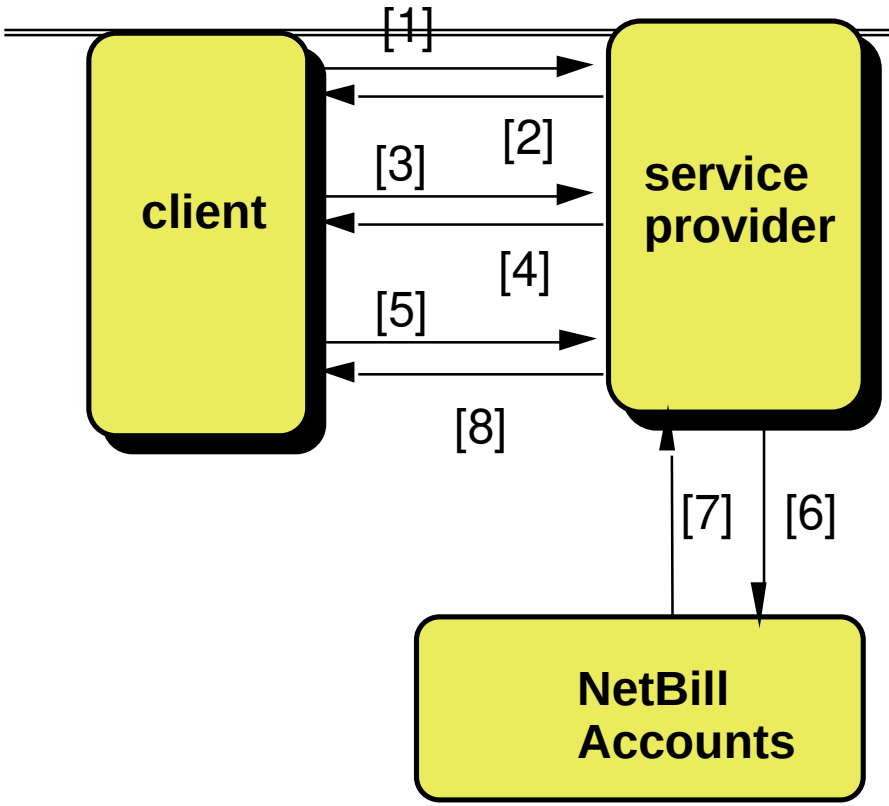
Carnegie Mellon

Improving Privacy in NetBill

- **NetBill runs a TGS which issues session tickets for access to merchants**
- **Session ticket contains a random pseudonym rather than the buyer's real identity**
  - consumer's signature on EPO is encrypted using a Ticket shared between consumer and NetBill. Merchant never knows consumer's true identity
  - impossible for merchant to provide custom quotes, volume discounts, subscriptions
  - A per merchant pseudonym (*e.g.* H{C, M}) allows for these while limiting correlation of purchase data across merchants

© 1997 Marvin A. Sirbu

NetBill Protocol



- **Three Phases:**
- **1-2 Price negotiation**
- **3-4 Goods Delivery**
- **5-8 Payment**

- **Inclusion of price negotiation phase permits flexible pricing**

- **A "subscription" means the price is zero**
  - could skip steps 6,7

© 1997 Marvin A. Sirbu

Carnegie Mellon

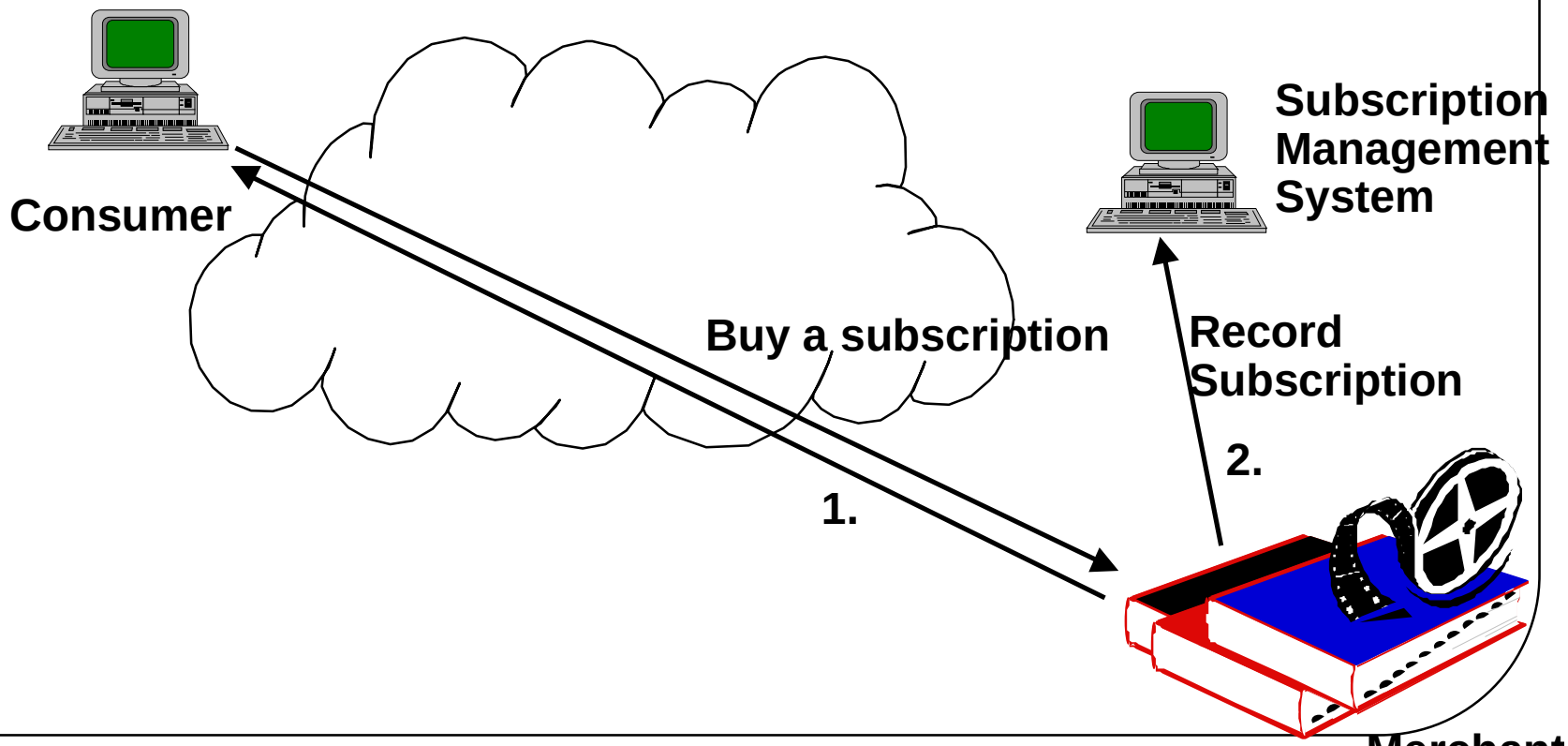
Flexible Pricing Examples

- ***Ex Post* choice of pay per use or subscription**
  - pricing module would log count of individual articles purchased by user in subscription database
  - when count exceeds threshold, price drops to zero for remainder of subscription interval
- ***Volume Discount***
  - pricing module would log count of individual articles purchased by user
  - when count exceeds threshold, price drops by discount percentage
- ***Cross selling***
  - buying an article from IEEE Transactions entitles user to one hour free subscription to IEEE Proceedings
  - side effect of running goods access CGI for Transaction article is to record subscription to Proceedings

© 1997 Marvin A. Sirbu

Subscription Management System

- Consumer buys a subscription
- Subscription info is logged at SMS database



© 1997 Marvin A. Sirbu

Carnegie Mellon

Two Methods to Support Subscriptions

1. **Pricing module does lookup of user in subscription database on each goods request**
   - if user is a subscriber, quoted price is zero

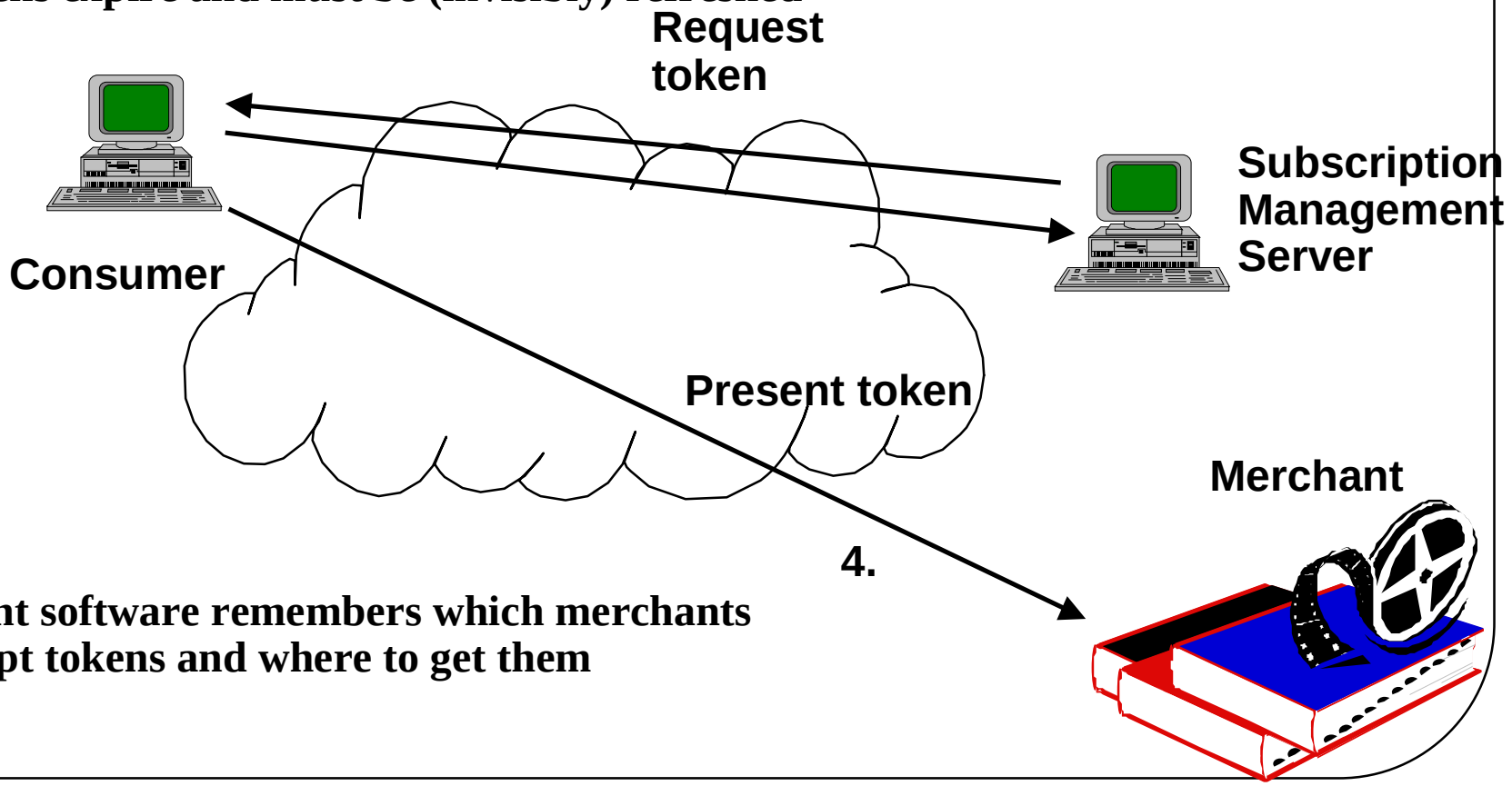
2. **Client obtains and caches a "token" (cookie, credential)**
   - token presented with each request for price quote
   - token identifies holder as subscriber
   - price can be calculated without database lookup

- **NetBill supports both methods.**

© 1997 Marvin A. Sirbu

Subscription Management System

- Subscriber requests token from SMS
- Subscriber presents token when requesting goods to show she is a subscriber
- Tokens expire and must be (invisibly) refreshed



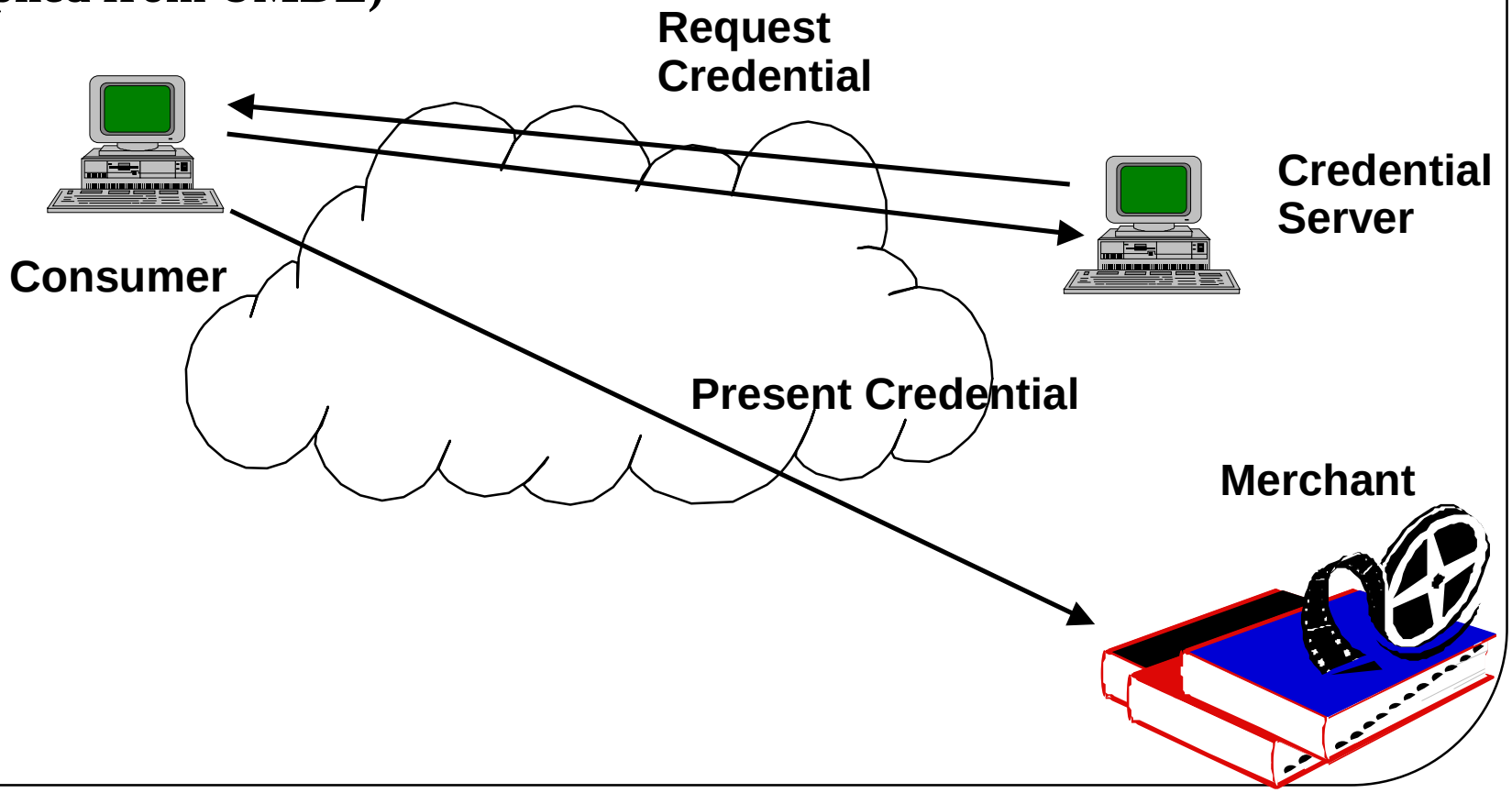
- Client software remembers which merchants accept tokens and where to get them

© 1997 Marvin A. Sirbu

Carnegie Mellon

Site Licenses and Third Party Discounts

- Supported using same technology (“Credentials”)
- Credential server operated by unrelated entity (e.g. CMU for goods supplied from UMDL)



© 1997 Marvin A. Sirbu

Carnegie Mellon

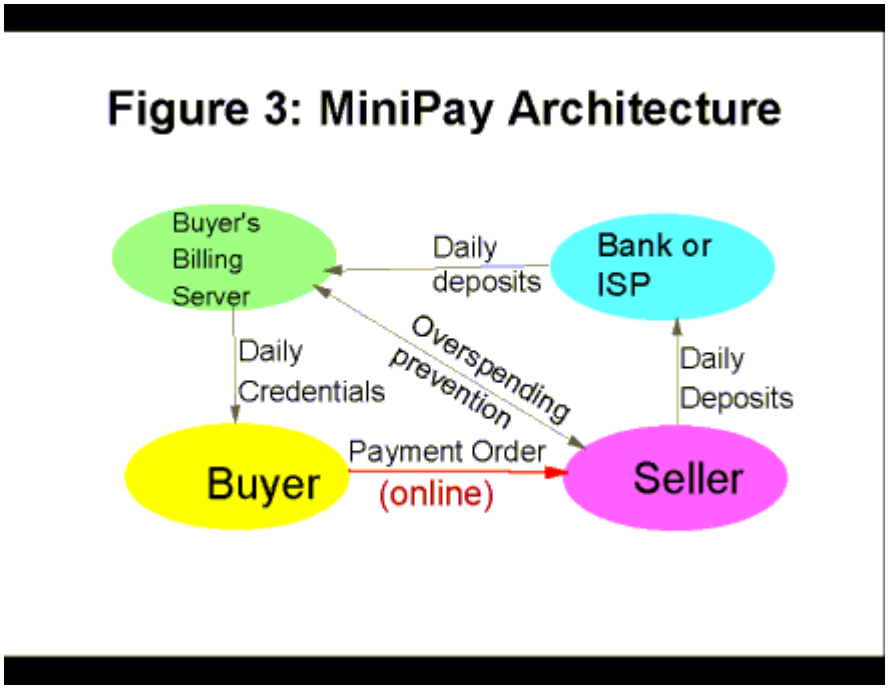
Credential Examples

- **Server at UMDL provides digital library content to CMU via site license**
  - CMU maintains credential database of who is a student entitled to library content under site license
- **IEEE arranges discount for its members when buying IEEE publications from Stanford digital library**
  - IEEE maintains credential database of members
- **Optimized protocol for zero priced (*e.g.* site licensed) goods**
  - skip interaction with NetBill server: 8 steps ==> 6 steps
  - If willing to give up certified delivery ==> 2 steps

© 1997 Marvin A. Sirbu

Trading Off Risk and Computation

- Agora from Bell Labs
- Mini-Pay from IBM



Carnegie Mellon

Lessons Learned

- Subscriptions versus microtransactions
- Wallet software
- Local State versus machine portability
- Selling goods versus selling keys
- Authentication issues

© 1997 Marvin A. Sirbu

Carnegie Mellon

Subscriptions versus Micropayments

- **Most information providers on the net are selling content via subscriptions**
  - consumer budget certainty
  - attractive to intensive information consumers
  - minimal impact on producer surplus
- **Does not require overhead of per item payments**
  - must authenticate consumer as subscription owner
    - potential for password sharing
  - negligible latency overhead
- **Subscriptions can be sold using macropayment technologies**
  - *e.g.* credit card

© 1997 Marvin A. Sirbu

Carnegie Mellon

Getting Wallets to Consumers

- **With the exception of entering Credit Card number via SSL, payment systems require consumer to have "wallet" software**
  - consumer resistance to downloading a wallet at point of sale
- **Potential solutions**
  - Wallet bundled with browser
    - Microsoft beginning to bundle wallet framework with browser (O/S)
    - probably requires more standardization before browser vendors will invest
  - crypto API in O/S, JVM or browser may allow lightweight browser download
  - expensive marketing efforts (à la AOL)

© 1997 Marvin A. Sirbu

Carnegie Mellon

CyberCash Agile Wallet

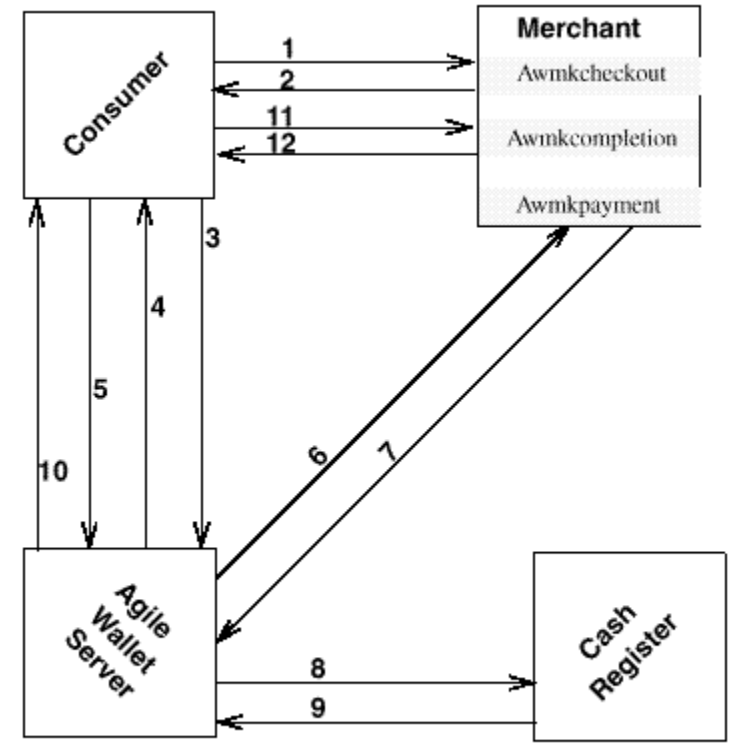


FIGURE 2: REAL-TIME TAX AND SHIPPING WITH THE MCK

Carnegie Mellon

Integrating Wallet Software with Browser

- **Web encourages point and click metaphor**
  - send URL, return content
- **Payment requires extra steps. How to simplify:**
  - selling web page construction
  - browser/wallet integration.
- **Support for streamed content**
- **Support for wide variety of content imaging plugins**

© 1997 Marvin A. Sirbu

Carnegie Mellon

Integrating Wallet Software with Browser: Approaches

- **Support multiple browsers on multiple platforms**
- **Spyglass Software Developer's Interface**
  - now deprecated.
- **Helper App**
  - CyberCash
- **Plugin**
  - Digicash
- **Local Proxy**
  - NetBill, GlobeID, Millicent
- **Java applet**
  - CC InstaBuy
- **Launching the wallet**

© 1997 Marvin A. Sirbu

Carnegie Mellon

Key Management and Multiple Machines

- **Typical commerce protocol assumes consumer has a private key. Where is this key stored?**
- **What happens when consumer uses multiple machines?**
  - Office, home, laptop
  - Public kiosk, University computer cluster
  - PC, Mac, Unix
- **Credit card entered via SSL requires no local state, only a standard browser**
- **Tradeoff of local state, efficiency and security**

© 1997 Marvin A. Sirbu

Carnegie Mellon

Problematic Solutions to Local State Problem

- **Smart cards**
  - long time before ubiquitous readers and software
- **Portable credentials stored on floppy**
  - diskless laptops, PDAs
  - kiosks
  - cross-platform file formats
- **Unique account on each machine**
  - can’t access subscriptions

© 1997 Marvin A. Sirbu

Carnegie Mellon

NetBill's Approach to Portability

- **Key Repository**
  - consumer submits private key, encrypted ("locked") by a key derived from passphrase, to NetBill central key repository
    - NetBill cannot decrypt locked private key
  - To activate wallet, consumer types UserID and passphrase
    - UserID used to request locked private key from Key Rep
    - Private key unlocked on local machine using passphrase
  - Similar option in PK-INIT for Kerberos 5
  - only as strong as consumer's passphrase selection
  - Protocol can be strengthened against dictionary attacks by deriving two orthogonal symmetric keys from passphrase
    - second key stored at NetBill and used to prove possession of passphrase before locked private key is downloaded

© 1997 Marvin A. Sirbu

Carnegie Mellon

NetBill Key Repository Protocol

- **Current Protocol initialization**
  - K_g = g(passphrase)
  - C ==>NB: $K_g\{SK_C\}$ at account creation
    - transmitted over secure channel
- **Retrieving Secret Key**
  - C ==> NB: {Identity}
  - NB ==> C: $K_g\{SK_C\}$
- **Potential attacks**
  - malefactor submits false identity, subjects encrypted private key to dictionary attack at leisure
  - third party can capture encrypted private key in transit

© 1997 Marvin A. Sirbu

Carnegie Mellon

Improved Repository Protocol (not implemented)

- **Initialization**
  - K_g = g(passphrase)
  - K_f = f(passphrase)
    - f and g orthogonal
  - Initially, K_f and $K_g\{SK_c\}$ stored at Key Repository
- **Key Request**
  - C ==> NB: $\{K_R, K_f\{K_g\}, \text{Identity}\}PK_{NB}$
  - NB ==> C: $K_R\{K_f\{K_g\}\}$
- **Consumer proves possession of password before encrypted secret key is sent**
- **Strong random key used to encrypt transmission**

© 1997 Marvin A. Sirbu

Carnegie Mellon

Additional Portability Steps

- **Use of ACAP for storing configuration/preferences information**
  - still requires consumer to specify ACAP server at session initiation
    - equivalent to specifying key repository
  - Preferences can be stored encrypted under private key or passphrase for local decryption
- **Storage of purchased information?**

Carnegie Mellon

Selling Digital Goods versus Selling Keys

- **NetBill assumes goods are stored at server and encrypted on the fly for the purpose of secure delivery**
  - unique key for each purchase
  - goods are up-to-date
- **InfoMarket, InterTrust, have proposed free distribution of goods in encrypted containers (“cryptolopes”). Consumer than purchases key to access container**
  - goods distribution completely separate from purchasing
    - superdistribution, CD-ROM distribution
  - layered access possible
    - different keys to get 300dpi JPEG versus 1200dpi
  - goods could become stale

© 1997 Marvin A. Sirbu

Carnegie Mellon

When to Authenticate Consumer?

- **SET uses unique authentication for payment only**
- **NetBill uses authentication for price setting as well as payment**
  - customized pricing
- **Amazon.com uses authentication for marketing and after sales support**

© 1997 Marvin A. Sirbu

Carnegie Mellon

Authentication Issues

- **Different confidence level needed for different uses**
  - different certificate authorities
- **For subscribed digital goods, subscription identity need not be same as payment identity**
  - I can pay for WSJ with MC or Visa
- **Anonymity and pseudonyms**
- **Computational expense of multiple authentications/ cryptographic operations**
- **Authentication versus non-repudiation (digital signatures)**
  - customized quotes versus non-repudiable quotes

© 1997 Marvin A. Sirbu

Carnegie Mellon

Keys to Future of Electronic Payments

- **Who will vouch for identities?**
  - private certificate authorities?
  - banks?
  - government?
- **What liability will be accepted by various parties?**
  - affected by national regulatory policies
    - in US, financial institutions must take liability
    - consumer doesn't worry about losing credit card
    - should consumer worry about losing private key?

© 1997 Marvin A. Sirbu

Carnegie Mellon

Keys to Future of Electronic Payments

- **Anonymity and Privacy**
  - Easy to keep records of electronic transactions
  - Privacy of transaction to observers (message privacy)
  - Anonymity of participants (pseudonyms, anonymous tokens)
  - Risks of money laundering, illicit money transfers
  - Inability to hold parties accountable

© 1997 Marvin A. Sirbu