Chapter 14

by

David G. Messerschmitt

Electronic payments

by

David G. Messerschmitt
Electronic payments: the players

- Consumer
- Merchant
- Financial institutions

Physical tokens representing value

Some forms of spending money

- Credit
- Debit
- Check
- Cash

- Loan
- Demand deposit
- Cash reserves
Questions about value tokens

- Who will back the value?
- How is fraud, counterfeiting, etc. prevented?
- Will value restored if lost or stolen?
- Is it subject to regulation?
- Who pays for the system?
- Is it traced?

Policy dilemmas

- Multiplicity of incompatible payment systems?
- Tracing and auditing:
  - Criminal prosecution
  - Taxation
  vs
  - Personal privacy
Some privacy initiatives

- Open Profiling Standard
- TRUSTe
- Anonymous digital cash

Electronic credit and debit

- Standard authentication, confidentiality, and non-repudiation techniques can be used
  - Asymmetric encryption and certificates
- Framework must take into account different institutions involved
- Example: Secure Electronic Transactions (SET) of Visa/Mastercard
Participants

- Consumer (cardholder)
- Merchant
- Acquirer: financial institution acting as transaction clearinghouse for merchant
- Issuer: financial institution that issued consumer credit/debit card
- Association: Visa or Mastercard

SET chain of trust

SET Root
Association
Acquirer
Merchant
Issuer
Cardholder
(self-signed, included in all software)
SET order/payment protocol

<table>
<thead>
<tr>
<th>Consumer</th>
<th>Merchant</th>
<th>Acquirer</th>
<th>Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>initiate</td>
<td>purchase</td>
<td>authorize</td>
<td>authorize</td>
</tr>
<tr>
<td></td>
<td></td>
<td>capture</td>
<td>capture</td>
</tr>
</tbody>
</table>

Smartcard

Card that contains encapsulated electronics and can be used for various forms of electronic commerce (and other things)
Prepaid smartcard options

- **Memory card**
  - Memory plus password/PIN protection
- **Shared-secret**
  - Mutual authentication of any terminal sharing the secret
- **Signature-carrying**
  - Carries signatures created by institution
- **Signature-creating**
  - Hardware to create signature based on secret key

Smartcard merits

- **Memory**
  - Closed system: single institution
  - No authentication of terminal
- **Shared-secret**
  - Requires encapsulated module in terminal, one to carry each card secret
  - One secret per institution implies that all cards of that institution can be compromised
Smartcard merits (con’t)

• Signature
  – Terminals need only public keys
  – Easy to handle multiple institutions
• All but signature-carrying have unique card identity, and hence institutions can invade privacy by linking transactions

Hard vs. digital cash
Digital cash

Since digital cash is represented by data, it is easily replicated. How do we prevent:

• Counterfeiting?
• Multiple spending?

What is a digital cash token?

- Unique identifier
- Value attribute
- Bank digital signature

Prevents counterfeiting
Prevents spending more than once
Financial institution perspective

Consumer’s demand deposit
- Vault cash
- Branch ATM
- Digital branch

Withdrawal

Currency in wallet
- Payment
- Merchant
- Deposit

Currency in smartcard

Merchant’s demand deposit

Digital cash liability

May return as more digital cash

Digital cash must be deposited

Hard currency
- Consumer wallet
- Merchant
- Spend

Digital cash
- Consumer smartcard
- Merchant
- Deposit

Withdraw as new digital cash
Possible characteristics of digital cash

- **Anonymity of consumer**
  - Merchant knows who paid, but that information is not inherent to the digital cash itself
  - Financial institution knows what merchant deposited

- **Attribution of cheating**
  - Double spending

- **Authorized traces**

Spending anonymity

Withdrawal and deposit are traceable, but can we break the chain somewhere?
Supplements

by

David G. Messerschmitt

Message digest

• MD is a fixed length (128 or 160 bit) summary of message
  • One way: message cannot be recovered from MD
  • Collision-free: computationally infeasible to find a message corresponding to a given MD
Digital signature based on a message digest

![Diagram of digital signature process]

1. **Message** -> **MD** -> **Encrypt secret key**
2. **Signature generation**
3. **Decrypt public key** -> **MD** -> **Compare**
4. **Signature checking**

---

Dual signature

![Diagram of dual signature process]

- **Consumer**
  - Offer
  - MD
  - Dual signature
- **Merchant**
  - MD
  - Payment authorization
- **Acquirer**
  - MD
  - Acquirer can verify binding of offer and authorization, does not see offer
  - Merchant can verify binding of offer and authorization, does not see authorization

Understanding Networked Applications 25 A First Course
Spending anonymity

Create $$, including identifier

Repeat n times

Cut and choose one

Blind signature

If the consumer’s software creates the digital cash, and the bank signs it blindly, the bank will not see the identifier. The cut and choose protocol assures the bank the $$ is proper.

Blind signature analogy

Token

Carbon

Put token and carbon in envelope

Present to bank for embossing

Remove token from envelope

Consumer gets bank to sign cash token without observing contents
Cut and choose protocol

Although the bank can’t see what it is signing, with the cut and choose the incentive for the consumer is to generate legitimate instances of digital cash.