Mobile Payment Protocols

Simon Anikó – BXLADA
Kara Péter András – YBVGB8

Introduction

• Alongside traditional commerce, e-payment rises
• It all revolves around the needs of the customers
• People demand simplicity, haste, customization and mobility
Payment methods

• Forms of payment: cash, check, debit card, credit card, electronic (wireless subset is mobile payment)
• For more information, check the Buttyanian slides

Mobile commerce

• Participants: customers, merchants, banks, mobil service providers, mobil device manufacturers, government
• Types: bank account (needs card+account), electronic cash (converts cash to e-cash), phone bill (prepaid or postpaid)
Aspects of security

- Authentication (who are we?)
- Authorization (are you sure?)
- Confidentiality (don’t tell anyone)
- Integrity (don’t change it)
- Non-repudiation (yes, it was you)

Types of Mobile Payment

- SET protocol
- Role-based 3 domain model
- Virtual POS protocol
- Real Point of Sale
- KSL protocol
- E-Cash model
Architecture

SET protocol

• Secure Electronic Transaction
• Needs credit card and SET installed
• Purchase on SET supported site → SET wallet activates → payment info → crypto functions → request sent → confirmation → funds transferred → delivery of item and the proof of transaction
Role-based 3 domain model

- Multiple roles for one participant (optional)
- Uses GSM security functions
- Registry on wallet server → offline/online purchase → customer auth (GSM) → payment process (interchange network) → item delivery (offline/online) → clearing and settlement (data recording) → (optional) restart/continue

---

Virtual POS protocol

<table>
<thead>
<tr>
<th>Customer</th>
<th>Merchant</th>
<th>Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>associate with cellphone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>request product options</td>
<td></td>
<td>encrypt payment request</td>
</tr>
<tr>
<td>service options list</td>
<td></td>
<td>decrypt</td>
</tr>
<tr>
<td>signed selected product</td>
<td></td>
<td>transfers money from customer’s account to merchant’s account</td>
</tr>
<tr>
<td></td>
<td>verify</td>
<td>signed payment confirmation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>verify</td>
</tr>
</tbody>
</table>
Real Point of Sale

Customer
- associate with cellphone
- request product options
- certM, nM, product list
- (S,nC)kM, certC+(S,nM,nC)kC*
- (P)kM* verify, decrypt
- verify
- (order info)k verify
- response and ID of Bank verify

Merchant
- bank
- Payment Order Message and a signature
- signed response
- verify
- transaction

Bank

Legends:
certX: certification of X
keyX: public key of X
keyX*: private key of X
nX: nonce of X
S: selected items
P: payment request

KSL protocol

Customer
- associate with cellphone
- request transaction date
- (date, idM)k
- (order info)k verify

Merchant
- Payment gateway
- issuer
- (order info)keyP, (date)M* decrypt, verify
- cost, idM
- signed response verify
- signed response

Issuer
- order info, date
- (response)k
- signed response

Legends:
certX: certification of X
idX: identifier of X
keyX: public key of X
keyX*: private key of X
k: symmetric key
E-Cash model

Customer

- associate with cellphone
- request product options
- product list
- (S)k
- (AEPO)k
- verify, calculate sum
- (sum)kC*
- decrypt

Merchant

Legends:
- certX: certification of X
- h: hash
- sum: sum of e-cash
- keyX*: private key of X
- S: selected items
- k: symmetric key by SSL
- AEPO: Agreement of Electronic Payment Order

Payment gateway

- AEPO, (AEPO)h, certM, sum
- (ACK)k
- verify, transaction
- verify

Mobile Payment in Hungary

- T-mobile (Hun. Telecom) (FHB account)
- Purchasing items with cellphone
- Paying bills (general household services)
- Transactions between similar users
- Charging prepaid cellphone
- Procedure: giving identifier, getting confirmation message, accept / decline / ignore (and decide later)
Summary

- Mobile payment protocols provide an easy and secure way for commerce
- Spread and domination is based on the commerce culture of different societies
- Protocols are already implemented, but new ones shall rise too
- It is also available in Hungary