Telecom Forum 98

Timo Rinne
Development Manager
Helsinki Telephone Corporation
timo.rinne@hpy.fi

Electronic Money

Server

Billing

Internet Banking

Customer

Billing

Bank

ECommerce

Company

ECommerce
Classification of Network Payments

- Amount of money to be transferred
  - micro, small and big payments
- The moment of payment transaction
  - beforehand, simultaneously, afterwards
- Classification by traditional payment methods
  - credit cards, electronic cash, electronic cheques, account transfers, electronic invoices, smart cards, other methods
- National / international payment

Network Payments in Finland

<table>
<thead>
<tr>
<th>Co-operative organization or company</th>
<th>Amount of money to be transferred</th>
<th>The moment of payment transaction</th>
<th>National / international</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Card payments SET</td>
<td>VISA/Mastercard Luottokunta</td>
<td>Small and big</td>
<td>Afterwards</td>
</tr>
<tr>
<td>Account transfers</td>
<td>Merita Osuuspankki</td>
<td>Small and big payments</td>
<td>Beforehand</td>
</tr>
<tr>
<td>Solo Kultaraha</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital cash</td>
<td>IBM Digital INA Finland</td>
<td>Micro payments</td>
<td>Afterwards</td>
</tr>
<tr>
<td>MiniPay</td>
<td></td>
<td></td>
<td>Before/after</td>
</tr>
<tr>
<td>Millicent</td>
<td></td>
<td></td>
<td>Before/after</td>
</tr>
<tr>
<td>Money-Penny</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart cards with a purse Avant</td>
<td>Automatia</td>
<td>Micro, small and big payments</td>
<td>Beforehand</td>
</tr>
</tbody>
</table>
Value Chain of E-commerce

- Content production
- From product to service
- Transmission
- Access
- Client systems

Payment operator
Server hosting
Access provider

provisions of payments
service
traffic

TELCO/ISP

Electronic Identity, what is it?
Electronic Identity

- A way for an entity to prove who it really is -> AUTHENTICATION
- Reliable authentication is necessary for telecommunications:
  - access control
  - authorization
  - billing

Driving Forces of Electronic Identity

- Electronic commerce
- Internet services
- Secure protocols (SSH, IPSEC)
- Routing protocols
- Wireless communications
- Legislation
  - The Law of Privacy in Telecommunications in Finland 1998-99
- General requirements for information security
What should a telco do?

- A telco or an ISP should provide electric identity for its clients and for all entities in its network
- Electric identity is an important part of the telecommunications infrastructure
- Reliable electric identity requires certificates
- Certificates can be issued by a telco itself or they can be supplied by some other third parties
- So, should a telco or an ISP establish its own CA services?

Telco/ISP as a CA

- Future CAs will be established by the governments, financial institutes and telcos
- Why telcos and ISPs???
  - To supply services with higher quality
  - To supply certificates as a part of the infrastructure
  - CA services can be integrated easily in a telco’s business processes and traditional services
Internet Certificate Services

Certificate Authority
- certificate issuing and re-issuing
- manages revocation requests
- 24/7 operation
- VERY good security

Directory
- stores certificates and CRLs
- 24/7 operation
- HA environment

User
- generates RSA key pair
- certificate requests
- revocation requests
- holds the secret key (in a hard drive)

CA services - smart cards

Certificate Authority
- certificate issuing and re-issuing
- manages revocation requests
- 24/7 operation
- VERY good security

Directory
- storing certificate and CRLs
- 24/7 operation
- HA environment

User
- certificate requests
- revocation requests
- holds the secret key (in a smart card)

Registration Authority
- user identification
- certificate requests
- CA’s interface to the users

Card Factory
- generates RSA key pair
- smart card personalisation
- smart card logistics
- VERY good security
Internet Certificate Services

- **Pros**
  - inexpensive to the users
  - minimum investments
  - automatic operation, minimum number of personnel
  - existing infrastructure supports Internet Certificate Services
  - client applications exist already

- **Cons**
  - low grade of security
  - smart cards will penetrate to the market anyway
  - life cycle only few years

Certificate Services - Smart Cards

- **Pros**
  - high grade of security
  - multiple services on the same card
  - dynamic services can be developed with mobile code
  - can be integrated on mobile equipment
  - technology for today and to the future

- **Cons**
  - expensive to the users
  - requires investments
  - requires personnel
  - logistic chain is very complex to set up
  - client side is not ready yet
Conclusions

- Telcos and ISPs can act as many roles in E-commerce
- Electronic commerce requires strong authentication and good security
- Using certificates is an generic way to do the job
- Certificates will be (they already are) important part of the telecommunication infrastructure
- Telco or ISP should set up its own CA services
- Internet Certificate Services can be deployed right now
- Smart cards are about to penetrate to the market as soon as client side gets ready and the prices come down