Mobile Identity Management
Outline

• Ideas
• Motivation
• Architecture
• Implementation notes
• Discussion
Motivation 1

• The mobile phone has become a highly personal device:
  - Phonebook
  - E-mail
  - Music, videos
  - Landmarks
  - Payment-related information
  - Personal files
Motivation 2

• Electronic identity documents:
  – Identity cards
  – Biometric passports
  – SIM-based identification

• Security/privacy improvements over the old documents?
Motivation 3

"Alko scenario"

Reveal yourself to prove your age.

Why?

Mikäpaperit kelpaavat?

Motivation 4

• Privacy-enhancing technologies:
  – State of public research is reasonably mature
  – Real life?
Use Cases

• Operators
  – Offering Secure Mobile Identity Services for 3rd parties
  – Subscriber services, authentication & authorization
  – Internal use, employee authentication

• Banks, financial transaction processors
  – Authentication to web bank
  – Signing on-line payments, card transactions, cash withdrawals (ATM), documents, agreements (stock exchange, loans, mortgage, insurance...)
  – Internal use, employee authentication
Idea 1

• Mobile phone as an identity token:
  – Officially recognised PKI-SIM cards available in Finland, Estonia, …
  – Mobile network operators have the central role in current implementations.
Idea 2

• A proof of a certain attribute...

...shown by a mobile phone?
Idea 3

• The mobile phone as a contactless multi-application smart card

  – Such cards have been available since 2001, but are still hard to find in the real life

  – Post-issuance downloading of applets usually disabled (mostly due to security reasons)

  – A second try with mobile phones?

• Can it be made open?
Credentials on mobile phones

• Three options for a storage place:
  – Unprotected memory
    • Suitable for non-critical applications only
  – Security environments
    • See e.g. Nokia OnBoard Credentials
    • Fully open
    • Certification issues
  – SIM card
    • Can be easily moved to another phone
    • Property of the MNO — any solutions?
PKI-SIM: Current implementation

Mobile Identification service manages identification and signature transactions (MSS) between service provider and end user.

Service Provider connects service applications into MSS (Mobile Signature Service) interface.

Mobile Operator

Application/Service

Certificate Authority

Population Registration Centre

PRC issues citizen certificates and publishes revocation lists.

End User

Operator delivers PKI-SIM cards to end users. End users register certificates on police.

Figure by Pekka Rauhala, HST group
Access to SIM

• The SIM card is owned by the operator
  – Access to SAT applets
  – Mobile user authentication (GAA)
  – Installation of new applets over-the-air
• Other service providers can use it
  – A contract with the operator is needed
  – The operator charges for services
  – Only online use
Access to SIM

• JSR-177 Security and Trust Services, SATSA:
  – Access to SIM-based applets from Java ME
  – Exchange of APDU messages

– Supported by
  • Nokia Series 40 since 3rd Edition FP 2
  • Nokia Series 60 since 3rd Edition
  • Certain Sony Ericsson, BenQ, Motorola models
Near Field Communication

• A short-range communication technology. Three modes of operation:

  – Reader/writer mode for tags and smart cards
  – Tag emulation mode
  – Peer-to-peer mode (up to 424 kbit/s)

Nokia 3220
Nokia 5140i
Nokia 6131 NFC
BenQ T80

(with NFC shells only)
Near Field Communication

• Potentially, bright future:

  – ABI Research: 20% of phones will have NFC by year 2012.

  – Recently, ETSI has defined an interface between SIM and NFC.

  – Proximity payments already offered by Visa and MasterCard.
Near Field Communication

• Potentially, some problems:
  – Tampering with tags used in NFC services (Collin Mulliner, EUSecWest 2008)

  – Attacks are similar to those based on manipulating with PIN entry devices (PEDs) in chip payments (Drimer, Murdoch)

• Protection against maliciously modified tags/terminals?

  – Authenticate arriving requests, require user's informed consent.
What are Mobile Signatures?

- PKI-based identity on a SIM card
- Secret keys in tamper proof storage
- Keys protected by PIN codes
- Certificates and revocation lists in a directory
- For authentication and digital signatures
- For mobile and web services
Urgent need!

• Industry has a demand to know the user and get his approval for actions.
  – We must be sure that the user is who he claims to be.
  – We must get user’s approval in a way that user cannot claim afterwards that it did not happen.

• Needs to support mass-market.
Key Stakeholders

• Bank
  – Internet Bank & ePayment Services
  – Customer base
• Mobile Operator
  – Network Infrastructure
  – Subscribers
• Government
  – More and more public services moving to Web. Strong authentication a must!
• Consumer
  – User of the value added services
Valimo

Need & Key Drivers
Banks
VISA & Mastercard fraud figures

- 40 million credit cards hacked in 2005
  - Breach at 3rd party payment processor affects 22 million VISA cards and 14 million MasterCards

- 70% of the losses caused by use of counterfeit cards

- e-Commerce is the next target

Source: Jani Kallio, Security Manager, Luottokunta Eurocard Oy, Finland
Online fraud figures in UK

- 2004 frauds £5 million
- 2005 £30 million
- 2006 EMV launched, POS card frauds going rapidly down, Online services on target
- Latest news (BBC1 Nov. 7th): Online frauds already doubled comparing to 2005
- What it will be at the end of 2006?

Source: FSA & BBC, UK
Net users want banks to do something

“What could your bank do to boost your confidence in online banking security?”

- Guarantee to replace losses that result from fraud: 48%
- Help me understand how to secure myself against these risks: 26%
- Introduce new, more secure, log-on technologies: 25%
- Nothing -- I trust my bank and have confidence in its security measures: 24%
- Nothing -- there’s no way I would trust online banking: 20%

Source: Forrester UK Internet User Monitor, Q2 2005
Base: British Net users
# Online Banking Security Concerns

The reasons why holdouts don’t bank online vary by country

“Why have you never used online banking?”

<table>
<thead>
<tr>
<th>Reason</th>
<th>DE</th>
<th>ES</th>
<th>FR</th>
<th>IT</th>
<th>NL</th>
<th>SE</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>I prefer/am happy with branch banking</td>
<td>56%</td>
<td>50%</td>
<td>43%</td>
<td>54%</td>
<td>24%</td>
<td>28%</td>
<td>53%</td>
</tr>
<tr>
<td>I prefer/am happy with cash machines</td>
<td>36%</td>
<td>24%</td>
<td>31%</td>
<td>26%</td>
<td>49%</td>
<td>39%</td>
<td>39%</td>
</tr>
<tr>
<td>I am worried about security</td>
<td>42%</td>
<td>42%</td>
<td>33%</td>
<td>31%</td>
<td>39%</td>
<td>39%</td>
<td>42%</td>
</tr>
<tr>
<td>I don’t see the need for it</td>
<td>31%</td>
<td>38%</td>
<td>20%</td>
<td>19%</td>
<td>29%</td>
<td>40%</td>
<td>32%</td>
</tr>
<tr>
<td>I worry about “phishing”/fraud/identity theft</td>
<td>44%</td>
<td>39%</td>
<td>26%</td>
<td>20%</td>
<td>36%</td>
<td>22%</td>
<td>35%</td>
</tr>
<tr>
<td>I don’t know enough about it</td>
<td>6%</td>
<td>31%</td>
<td>16%</td>
<td>17%</td>
<td>26%</td>
<td>20%</td>
<td>14%</td>
</tr>
<tr>
<td>It’s too complicated</td>
<td>6%</td>
<td>8%</td>
<td>9%</td>
<td>8%</td>
<td>13%</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Because there is no human help</td>
<td>4%</td>
<td>8%</td>
<td>16%</td>
<td>9%</td>
<td>6%</td>
<td>4%</td>
<td>25%</td>
</tr>
<tr>
<td>I have already automated all my payments</td>
<td>14%</td>
<td>1%</td>
<td>6%</td>
<td>5%</td>
<td>20%</td>
<td>13%</td>
<td>8%</td>
</tr>
<tr>
<td>I prefer/am happy with telephone banking</td>
<td>4%</td>
<td>2%</td>
<td>7%</td>
<td>2%</td>
<td>16%</td>
<td>17%</td>
<td>16%</td>
</tr>
<tr>
<td>All other reasons</td>
<td>25%</td>
<td>34%</td>
<td>41%</td>
<td>41%</td>
<td>42%</td>
<td>48%</td>
<td>33%</td>
</tr>
</tbody>
</table>

Base: European online consumers who have never banked online (multiple responses accepted)

Source: Forrester’s European Consumer Technology Adoption Study Q2 2005 Survey
Key Drivers, Banks

The mobile phone is a trusted device that provides anywhere, anytime access to confidential, personal and business content and guarantees integrity and non-repudiation of electronic transactions.
Key Drivers, Banks

- Authentication through different channel than the service
- Makes phishing and Man-in-the-Middle impossible
Open Mobile Identity

• Architecture at a glance:

Security and trust services = SATSA

Java Card applet

J2ME applet

NFC = Near Field Communication

Credentials

Privacy proxy

Phone

Terminal

Computer Display UI
Open Mobile Identity

• The SIM card applet contains:
  – A pseudonym pool: biometric identifiers, customer numbers, strings.

  – Identity profiles. A profile contains
    • A private key, generated on-card
    • A certificate issued to a pseudonym, with corresponding certificate chain
    • Attribute certificates with masked values of attributes; attribute masks
    • Secret keys

  – Profile-loading private key and a corresponding public key certificate
Identity proxy

• Provides a trusted user interface
  – Informs the user about requests
  – Asks for user's consent
  – Communicates with the SIM card applet
  – Communicates with the verifier/payment terminal
  – A signed Java ME applet

– Signature is checked by the phone before any message exchange with SIM is allowed.
Loading an identity profile

Identity issuer

Generate a timestamp $T$

Identity proxy

Generate a keypair $\{K_U, K_R\}$

SIM card

$K_U$ signed and timestamped; profile-loading certificate; [pseudonym]

Construct CertificationRequestInfo block

Construct Certificate Signing Request

CSR; profile-loading certificate, [pseudonym]

Construct identity profile data

Identity profile data

Identity profile data

Store identity profile
Identity proofs and digital signatures

Identity verifier
- Identity profile type; list of attributes; message G to be signed (optional); timestamp $T_{IV}$

Identity proxy
- Identity profile type
- Root certificate
- Verify request signature; Acquire user's consent
- Generate a timestamp $T_{IP}$
- Request data; $T_{IV}$, $T_{IP}$
- Ask and verify PIN, if needed
- Proof data; $\langle G, T_{IV}, T_{IP}\rangle_{KR}$

SIM card
- Identity profile type
Other uses

• Challenge-response protocol
  – Encrypt a nonce with a secret key
  – Mobile phone as an electronic key, proximity scenario

• One-time passwords
  – Encrypt the current time with a secret key
  – Mobile phone as a secure authentication token
Biometric authentication

- Privacy-aware
- Biometric patterns not released to verifiers
- TPM/trusted user interface is needed

479a1 is a proof fingerprint
Implementation issues

• NFC terminals are needed
  – Not many yet, but the situation may change
  – Many electronic ticketing trials
  – Contactless payments with cellphones already work in some places

• For certificate validation, CRL is probably the best option
  – Identity proxy must go online from time to time
eBanking, Authentication

- 2. Bank system sends authentication request to Operator’s authentication service, based on user credentials (account number)
- 3. User enters his authentication PIN
- 4. Access to the bank service is allowed (if PIN is correct and certificate is valid)

Please authenticate yourself to enter the Web Bank Service.

An introductory page is shown to the user.

Enter PIN

The user enters their PIN and the Signature is sent

You are successfully authenticated

The user is given feedback on the result of the signing
What about regulations?

- Supportive legislation in most European countries
- Scandinavia is the leader of the pack
  - Finland is a showcase in pro’s and con’s
- Initiatives in many countries
- Banking & finance are top sponsors
Implementation issues

• SIM as a storage place for profiles:
  – Most SIMs have passed Common Criteria certification
  – High density SIMs provide tens to hundreds of megabytes of Flash memory for profiles
  – Not much RAM is required.
  – 1024-bit RSA signatures in ~200 ms.
  – Software distribution can be done over-the-air (Sirett et al., CARDIS 2006)
Discussion

• **Benefits**
  - A terminal that the user can trust
  + Easy time syncronisation
  + Secure and certified storage for identity info
  + Fast proximity transactions
  + No need for extra hardware tokens
  + Biometrics supported
  + Privacy-aware
  + Open for use by anyone: a public tool

• **Drawbacks**
  - Electronic tickets with stored value not supported
  - Not many NFC terminals
  - Possible opposition by mobile network operators
  - Requires installation of a J2ME applet
  - Pseudonymous, not anonymous