Mobile ID
usnadňuje život jak uživatelům tak poskytovatelům služeb!

Smart Cards & Devices Forum 2012

Jan Němec
Gemalto
Květen 2012
Valimo Mobile ID Solution
Mobile ID Makes Things Easier…

… both for end users and service providers!

- Allows you to forget all passwords, bank codes and IDs
- Enables strong authentication and legally binding signatures for all web and mobile services
- Based on digital signatures created in the SIM card (2048bit RSA keypair)

---

**End User**
- Mobile phone based signing
- Mobile ID application on the SIM card

**Operator or Trust Center**
- Mobile Signature Service

**Bank or other service provider**
- Online or mobile services

---

Smart Cards & Devices Forum 2012
What is a Mobile Signature?

• Equivalent of your own handwritten signature

• Created by typing secret code (Signing PIN) into the security application in the phone (SIM)

• Signature and authentication is validated by a trusted third party

• Security similar to using a smart card
Trends in Mobile Authentication

• Deloitte TMT Predictions 2011: More smart phones than PCs sold today
  • 375M smart phones + 50M tablets vs. 350M PCs

• Mobile Internet services require increasingly stronger identification
  • Cloud computing, services and storage: username + password currently
  • Service centric authentication is not sustainable: too many identities
  • OTP not secure anymore, e.g. Zeus malware in mobile phones
  • Printed password lists, separate tokens are cumbersome to use, therefore not an option for 'mobile life'

• User centric authentication and identification
  • Enables multiple service providers to use same authentication and identification method
  • Same look and feel, same user experience
  • Identities can be centrally managed and revoked if needed
  • ID must combine strong security and simple use - ideally usable always and everywhere
Mobile phone as a convergence point

Authentication Request
The Service Provider SP is requesting authentication - Proceed?

Cancel  OK
Mobile ID for the financial institutes, examples

Account request
Please sign your new account request at the Bank of Utopia now.

Cancel  OK

Register your ID
You have initiated a registration process for your ID, proceed?

Cancel  OK

Signing request
Signature request from iPhone app called Gemalto mBanking, Proceed?

Cancel  OK

Encrypt
You are about to encrypt your e-mail, Proceed?

Cancel  OK
Mobile ID for the user

**Signing request**
Signature request from Service Provider Remote, proceed?
- Cancel
- OK

**Decrypt**
You have received an encrypted e-mail, Decrypt?
- Cancel
- OK

**Encrypt**
You are about to encrypt your e-mail, Proceed?
- Cancel
- OK

**Decrypt your webmail**
You have received an encrypted webmail, decrypt?
- Cancel
- OK

**Pairing**
You are about to pair your device with your computer, Proceed?
- Cancel
- OK

**Signing request**
Signature request from your computer "MyComp", Proceed?
- Cancel
- OK
Mobile ID for the government, examples

**Signature request**
The local application "Sign this PDF" is requesting signing, proceed?
- Cancel
- OK

**Signature request**
You have submitted an eGovernment report to the eGov portal, sign it now?
- Cancel
- OK

**Confirm your vote**
I hereby confirm my vote for the candidate John Smith.
- Cancel
- OK

**Signature request**
You have submitted your tax report, would you like to sign it?
- Cancel
- OK

**Encrypt**
You are about to encrypt your e-mail, Proceed?
- Cancel
- OK
Identity in the secure element - military grade security

Nothing to see here – the ID and credentials are in the mobile phone, the plot fails

User might be fooled to a wrong site, but as transactions are confirmed and signed through the mobile channel, the plot fails
Mobile ID and Security

- Based on two channel, two factor mobile authentication
  - Separating the data channel from the authentication channel (Internet vs phone)
  - Protects service providers and their Mobile ID users from phishing and identification theft attacks

- Using mobile Public Key Infrastructure (PKI) model
  - With unique private key(s) stored in a tamper-resistant area of the SIM card
  - The user has to enter a personal, secret PIN code in order to use the Mobile ID
  - Legally binding signatures in all the markets where Mobile ID has been deployed

- When using Mobile ID the user only signs what is actually shown on the screen of the mobile
  - Can be sure not to authenticate or authorize something else at the same time
  - Makes it easy for the end-user to trust the service provider
The User Experience

Authentication – login to online bank, user receives a request to authenticate

Introductory screen shown to user

User enters Authentication PIN; signed response sent to Valimo Mobile ID platform for verification

Signature verified; user receives confirmation and is granted access to the service

Signing – authorize a transaction

Introductory screen shown to user

User sees the transaction details

User enters Signature PIN; signed data sent for verification and returned to the online bank

Signature verified, transaction authorised
Valimo Solution Architecture - generic
Security and Encryption

End User

Service Provider

Valimo MSS SDK Integration Library

Operator

Trust Center

Valimo Messaging Server

Valimo Signature Server

Valimo Registration Server

Service Provider e.g. Bank

Customer Database

Registration and Validation

Certificate Authority

Registrar e.g. Retail shop kiosk, bank

SSL

RSA

3GPP TS 23.048

AES

Transaction Database

User Database

AES

Card Database

AES

User Database

Security Client on the SIM card

Security and Encryption
Mobile ID Registration - Process Flow

1. User goes to MNO, proves his identity
2. Background check
3. OK + SATU e-identity
4. Registration request
5. Key generation + registration request
6. Applet generates key pair, user chooses PIN
7. Public key + ICCID returned – PKCS#10
8. Certificate request P#10
9. CA issues the certificate, stores in database
10. Certificate returned
11. VRS stores certificate for signature validation purposes
12. Notification to MNO: registration completed
13. Notification to user: registration completed
Mobile ID Authentication - Process Flow

1. User wants to log in to the website
2. Redirected to MNO Mobile ID service
3. User enters mobile phone number
4. Authentication request (data) sent to User – PKCS#7
5. User responds to request, enters PIN and creates signature using Authentication key
6. Signed data returned
7. VSS verifies signature
8. Authentication response 'OK' returned
9. User logged in
10. Acknowledgment sent to User
Mobile ID Signing - Process Flow

1. User wants to sign a contract
2. Redirected to MNO Mobile ID service
3. User enters mobile phone number
4. Signature request (data/hash) sent to User – PKCS#1
5. User responds to request, enters PIN and creates signature using Signature key
6. Signed data returned
7. VSS verifies signature
8. Signed data and response ‘OK’ returned
9. Signed contract stored and processed
10. User has signed the contract
11. Acknowledgment sent to User
## Valimo Mobile ID vs. Other Authentication Solutions

<table>
<thead>
<tr>
<th></th>
<th>PIN / TAN Password List</th>
<th>One-Time Password (OTP) Token</th>
<th>EMV Card + Reader (OTP Token)</th>
<th>Mobile SMS - OTP</th>
<th>PKI Smart Card + Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😃</td>
</tr>
<tr>
<td>Easy To Use</td>
<td>😃</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>Mobility</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>Low Usage Cost</td>
<td>😃</td>
<td>😃</td>
<td>😃</td>
<td>😃</td>
<td>😃</td>
</tr>
<tr>
<td>Low Maintenance</td>
<td>😞</td>
<td>😞</td>
<td>😃</td>
<td>😃</td>
<td>😃</td>
</tr>
<tr>
<td>All-Purpose Versatility</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😃</td>
</tr>
<tr>
<td>Legal Qualified Signing</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😞</td>
<td>😃</td>
</tr>
</tbody>
</table>

Mobile ID

[![Valimo Mobile ID logo](image)](image)
Mobile ID Use Case Opportunities

- **Banking & Payments**
  - e- & mBanking and Transaction Confirmation
  - Cardless ATM withdrawals
  - Financial inclusion – for the unbanked

- **Online eID**
  - Social network Single Sign-On
  - Enhanced security and convenience to Identity 2.0

- **Citizen eID**
  - 24/7 eGovernment services, digital healthcare

- **Corporate use**
  - Legally binding digital signatures, e.g. PDF and email
  - Corporate VPN
  - Streamlined workflows - electronic document management and digital signatures

- **e- & mCommerce:**
  - Secure credit card transaction confirmations
  - Safe Person-to person transactions
  - Age verification
Valimo Mobile ID

Case Finland – Complementing the national citizen eID with Mobile ID
Facts about Finland

- Population: 5.4 million
- Mobile phone subscriptions: 8.9 million
- Households with a mobile phone: 99%
- Smart phone coverage: 38% and rising rapidly

Mobile Network Operators:
- Elisa: 39%
- Sonera: 36%
- DNA: 26%

Banking and users of Bank ID
- Banking customers: 3 million
- Online transactions per user per year: 100
- Overall number of online transactions/y: 500 million
Electronic Identities in Finland

- Citizen eID card launched in 1999 being the first national eID scheme in the world
  - Close to 400,000 cards issued by the end of 2011
  - Card issuance is voluntary, not issued automatically to all citizens

- Bank issued paper based one-time-passwords issued to all online banking customers
  - 3 million users
  - Government recognizes the Bank ID as a suitable authentication mechanism for eGovernment services

- Corporate ID issued by the Tax Authority (KATSO)
  - Used to authenticate and authorize employees of organizations or representatives to various eGovernment services
Prevailing system crumbling

- The prevailing electronic identity in Finland for over a decade has been the Bank ID
  - Over 99% of online transactions requiring strong user authentication were done with Bank ID
- Unfortunately the Bank ID has become vulnerable
  - Successful attacks against bank accounts happen on weekly basis
- Customers are looking for a new, convenient tool to be used as a universal authentication token
  - As all the banks use the Bank ID and the related protocol (TUPAS), the replacement should be able to cover all banks and government needs
- Through raising smart phone usage customers are becoming familiar using phones in various new situations
  - Not just for voice or text anymore
Mobile ID basics

- Mobile ID is a PKI based signing solution in the SIM card
  - Works in 99% of the phones
  - PKI means legally binding signatures
  - Use cases for authentication and digital signature
- Mobile ID is convenient, yet equivalent in security compared to a smart card
  - Signing tool always with you – the mobile phone
  - Keys generated and stored in the tamper resistant environment meeting the government requirements for strong authentication and signing solution
  - Authentication and signing requires that the user only remembers the PIN codes protecting the authentication and non-repudiation keys
  - No central databases to be hacked
  - User cannot even by mistake reveal the credentials as they remain in the SIM card making identity theft impossible
Mobile ID revolution in Finland

- As an answer to the customer demand both from the government and the end users the three Finnish operators decided to launch a nationwide Mobile ID to the market
  - MNOs form a Circle of Trust (CoT)
  - Service providers need only one agreement with one MNO – but all operator customers can use the services
  - Interoperability between MNOs based on Valimo standard based back-end means roaming digital signatures between operators
  - The market leading operator, Elisa has already deployed over 3 million PKI SIM cards into the market
  - All operators saw an opportunity to new revenue, reduced churn and entry into a new market (Identity and Access Management)

- Government and private sector collaboration
  - Enrolling the Mobile ID is possible without a visit to a government office
  - The end user can acquire the Mobile ID either through the operator shop or online
  - End user can use Mobile ID as general purpose strong ID and signature tool in private and public sector services
Easy to get equals successful adoption

3 ways to get the Mobile ID in Finland

1. Go to the operator shop and register your Mobile ID there
2. Use e.g. Elisa on-line service and register your Mobile ID using your Bank ID as bootstrap authentication (most Elisa customers already have a PKI SIM)
3. As the subscription owner go to the on-line site (1st authentication using your Bank ID) and order a new SIM, which is delivered to your address
   • Register, or have the subscription user register the Mobile ID (e.g. Children)
Success requires services

- Mobile ID launched to the Finnish market Q4 / 2011
- At launch date a handful of service providers had adopted the mobile ID
  - “If” – a major Scandinavian insurance company
  - A few smaller financial companies
- In February the biggest national bank joined Mobile ID raising the number of Mobile ID enabled services by over 300
- April 2012 the government authentication and payment portal “VETUMA” adopted Mobile ID enabling all eGovernment services for Mobile ID adding 120 new service providers

→ 6 months after the launch there are close to 500 public and private sector services supporting Mobile ID
VETUMA portal for eGov services

Select identification method

**Mobile certificate**
Identify yourself using a mobile phone that has a SIM card equipped with mobile certificate.

**Bank identification**
Identify yourself with the identifiers granted by your bank.

**Certificate card**
Identify yourself with a personal ID card containing a chip granted by the police. You also need card reader, equipment and software.

Good to know
Some e-services require electronic identification. Identification is carried out using the Citizen's online authentication and payment service. Citizen's online authentication and payment service is a secure way for identification to various e-services and payments to authorities. Depending on the e-service, possible methods of identification are personal bank identifiers, electronic ID cards, user IDs and mobile identification services. Methods available to you are presented on this page.

About this service  |  File description  |  Feedback
Valimo mobilizes digital IDs. Valimo Mobile ID allows mobile phone users to securely authenticate, digitally sign documents, confirm transactions and payments, simply by entering a self-chosen PIN code. The multipurpose solution combines strong security and ease of use, enabling new service concepts and more efficient processes. Valimo Mobile ID is used in a variety of services throughout the world, including online banking, mobile payments, e/m-commerce applications, governmental services, along with enterprise identity and access management. The two-channel, two-factor authentication method based on Public Key Infrastructure (PKI) produces a legally binding signature regardless of time and place. Valimo Mobile ID solutions are global market leaders in terms of installation base and number of active users. Founded in 2000, Valimo Wireless is headquartered in Vantaa, Finland.
Thank you,

your questions, please?