When eID becomes Mobile for a whole nation

Valimo Mobile ID just makes adopting an electronic citizen identity easier for everyone

FINANCIAL SERVICES & RETAIL
ENTERPRISE
GOVERNMENT > CASE STUDY
TELECOMMUNICATIONS
TRANSPORT
When eID becomes Mobile for a whole nation

Valimo Mobile ID just makes adopting an electronic citizen identity easier for everyone

eID in Finland: Nordic pioneers

The Finnish eID card, introduced in 1999, was the first ever national eID scheme in the world.

The card allows citizens to carry out secure transactions with public authorities, businesses and other service providers via the Internet, based on public key infrastructure (PKI). Today, the card itself is widely used as the national ID and health card in Finland, but now citizens are also looking for the same level of services in mobile.

eBanking rapidly gaining ground

At the same period, the Finnish banks were pioneering eBanking. They started offering all their services online with One-Time-Password lists (OTP). These OTP lists quickly reached most of the adult population and were considered secure enough and became the most popular method for online authentication.

For more than ten years, the bank OTP lists have been providing reasonable security levels to do business through a wealth of online services including banking, shopping and eGovernment services. But the once secure system (OTP) has been under attack for the past few years.

Source: www.itviikko.fi

Mobile phone technology and Finland: love at first sight!

One thing that depicts an average Finnish person is the love for mobile phone technology. The number of SIM penetration in Finland went over 100% years ago and Finns are always hungry to use the latest mobile phone technology. No surprise Mobile PKI raised Finnish interest before everyone else.

Mobile PKI offers a very strong security framework for all parties. The security related operations are done in the SIM card, a tamper resistant environment, making it almost impossible to misuse the users identity. Software that tries to steal the identity of the user or sniff out passwords or other credentials cannot penetrate the SIM security. Authentication and signature information travels through the SMS and back-end channels to the service provider and is verified by the operator, so even if the user is attacked at the browser level, or the computer is infected, it does not matter. The data never goes through the Internet channel. To be successful, the attacker should also gain access to the mobile operator network to attack/infect the encrypted SMS messages.

A Finnish consortium offering a centralized authentication and authorization portal for eGovernment services, realized quite early that a
flexible and independent method of authentication was of importance.

Mobile PKI was seen as a great alternative for strong and flexible user authentication and electronic signature services. The government services saw the opportunity because of the high rate of transactions of many on-line services and the need for a cost-effective way of strong authentication.

The mobile network operators also seized the opportunity to build new services and generate new revenue streams using the mobile PKI technology. From early on, the major Finnish telecoms operators decided to create a national specification based on the ETSI Mobile Signature standards, the international standardization that defined the mobile PKI.

FiCom, the Finnish Federation for Communications and Teleinformatics, a co-operation organisation for the ICT industry in Finland has produced the Mobile Signature Service recommendation for Finland together with the Finnish mobile operators DNA Finland, Elisa and TeliaSonera, and mobile signature service experts. Although localized ecosystem and technical models were adopted in Finland, the Finnish mobile PKI can work seamlessly with other ETSI MSS compliant implementations.

The four rules of success

The parties involved in the mobile PKI efforts were determined to learn from the eID lessons and take into account that many Finns still clung to the bank issued OTPs.

The Finnish mobile network operators focused on four rules when launching the Mobile ID:

1. > Launch the solution with attractive services.
2. > Make it easy to get.
3. > Market the solution to the end users.
4. > Make sure it is easy to use.

The current Mobile ID approach in Finland is successfully leveraging these four guidelines:

- Authentication is simple as 1-2-3. When you need to authenticate, just type your PIN code that protects the private key into your mobile phone and press OK. That’s it. The PKI software and the Valimo back-end will take care of the rest.

Replacing the bank authentication

The Finnish bank authentication scheme started to penetrate the country at large for almost each and every service requiring strong authentication. From the legal perspective in Finland, the bank OTP list is considered a strong authentication mechanism. This situation is very unique in Europe.

As the bank OTP list penetration reaches 100% of online banking users in Finland, it is a challenge to any new authentication scheme. The new replacing scheme has to fulfill the same promise: to be the de-facto authentication method for all citizens in Finland. The bank OTP lists are not just paper lists, behind is also a protocol developed and maintained by the consortium of Finnish banks. Therefore the new method must be able to easily replace the protocol or offer a way to integrate the new method with minimal effort, preferably without any changes in the services themselves.

To combat the growing attacks, the banks need an alternative method of authenticating the user. Replacing paper based one-time-passwords with electronic one-time-passwords can help mitigating the risk, but eventually the banks need to provide a secure, mobile, and convenient way for the users to securely access the financial services. The other major issue is availability. Every on-line banking user should be able to switch to the new method with relative ease. As the Valimo Mobile ID is based on SIM Toolkit technology, it works in 99% of the mobile phones.
How did mobile PKI get implemented in Finland?

There are governing standards for mobile PKI, which are created and maintained by ETSI. The most important standards are ETSI TS 102 204 for service provider integration, and ETSI TS 102 207 for the roaming and ETSI TR 102 203.

Having a single nationwide standard made the implementation of the environment easier for all participating operators.

Components of the new Mobile ID system

The mobile PKI infrastructure is the same for all operators – i.e. all operators chose the same kind of approach. For some of them, the deciding factor was the completeness of the product offering. Valimo Wireless Mobile ID was able to offer all the necessary parts for both to the client side and the server side to create an end-to-end turn-key mobile PKI for the MNO and the end user. The ability to adapt to different processes, especially in registration, was easily achieved through productized APIs. This feature was a clear asset for the operators.

The components provided by Valimo that form the mobile PKI infrastructure in Finland are:

- **Valimo Signature Server (VSS)**: an ETSI MSS standard-compliant Mobile Signature Service Provider (MSSP) platform offering the core server functionality needed in Mobile ID. It enables mobile signature and strong authentication services for service providers and end-users. The server handles the signature requesting and response processes, communication with Mobile ID clients in the mobile phones, signature validation and transaction management covering the whole signature transaction lifecycle.

- **Valimo Registration Server (VRS)**: implements the different user registration and deployment processes of Mobile ID. The processes can follow either existing ones or new ones created by the RA and CA. The server supports different types of operational environments and offers interfacing tools that simplify the integration of RA and CA systems.

- **Valimo Messaging Server (VMS)**: This carrier grade messaging solution handles the communication between the mobile signing application in the user’s mobile phone and the back-end servers. It connects to the MNO’s SMS-Center. Messages to and from the Mobile ID client in the SIM card, e.g. the VMAC application, are encrypted to ensure transport security and privacy.

- **Valimo MSS SDK**: In order for the service providers to utilize the Valimo Mobile ID service quickly Valimo Wireless provides an integration kit that can ease the integration effort considerably. New on-line services can be integrated to the Mobile ID service in just a matter of hours using this SDK.

- **Valimo Mobile Authentication Client VMAC**: is a signing (PKI) application stored on the SIM card in a tamper resistant hardware environment. Together with the user-specific private keys, it enables the mobile phone subscriber to receive digital signing requests and by entering the correct PIN code to produce the signed response. Digital signatures use the RSA algorithm with either 1024bit or 2048bit key-length. All messages sent through the MNO network also encrypted.

The VMAC offers a generic mobile signature client solution, which is:

- end-user friendly
  - available from any major SIM/USIM vendors
  - OTA platform vendor independent

In the following picture a normal use case of mobile PKI is depicted.

- The user wishes to use an on-line service, and needs to authenticate
- The Service Provider has an agreement with Mobile Operator 2 for the Mobile ID
- The user types his/her phone number into the login screen of the on-line service
- Mobile Operator 2 recognizes the user as an Mobile Operator 1 user, and forwards the authentication request to Mobile Operator 1 (signature roaming)
- The user receives the authentication request and inputs his/her authentication PIN (typically 4 digits) and the SIM application signs the authentication request if the PIN code is correct
- The result is sent back to Mobile Operator 2 (as verified) and the user is granted access to the service.

The result is a roaming signature among the operators. All users from all operators in the country can use the service because of the roaming digital signature. The revenue for the MNO comes from their own customers and from competitors.

The user's actions in this strong authentication case (2 factors, 2 channels) are limited to two:

1. Input the phone number
2. Input the PIN
Simplified registration process

With the legislation, it is now possible for the user to walk into any operator shop and register his/her digital identity on the spot. The user presents his/her ID document (passport, driving licence, ID card) to the shop clerk when requesting a Mobile ID. Thanks to well trained staff, the actual registration process takes only a few minutes and the certificate is valid for five years.

The user has two actions to do for strong authentication:

1. Input the phone number
2. Input the PIN
Using on-line registration to obtain the Mobile ID is even more convenient. In this case, the user can authenticate online using the bank issued OTP credentials. The registration service then uses this information and other information sources to verify the identity before issuing the credentials. The online procedure has been made possible as there will be hundreds of thousands PKI enabling SIM cards in the market after the major rollout, just waiting to be Mobile ID activated.

The big change compared to the previous process, is that the Finnish Population Registration Centre is no longer responsible for the end-user certificates in mobile phones, nor has the liability. Now the MNOs just request a special electronic identity string called SATU (basically electronic ID string, unique to each citizen) from the population registration center during the certificate enrollment process.

For the service provider

A typical service provider scenario involves an entity who wishes to share their services, sell products or offer on-line access to account information. The common factor is that they wish to protect the user against identity theft and also mitigate the risk of fraud within their own services.

Mobile PKI technology offers a very good value proposition in this due to the two-factor and two-channel authentication and EU digital signature directive compliant electronic signing. The service provider receives an SDK from the mobile network operator, which is then used to implement the ETSI TS 102 204 interface between the service provider and the Valimo Mobile ID. This interface enables the service provider to ask for authentication of the user and request electronic signatures from the user. Through the Software Development Kit (SDK) the service provider can integrate their services within hours to the Valimo Mobile ID infrastructure.

For the mobile network operator

There are a few choices on how to implement the back-end operations and assign roles. Typical roles in the mobile PKI are:

- Certification Authority (CA), who issues the certificates
- Trust Center also known as MSSP (Mobile Signature Service Provider), which will provide the whole mobile PKI service
- Registration Authority (RA) responsible for managing the user registration for certificate issuance on behalf of the CA
- the Mobile Network operator, who provides the communication channel between the MSSP, the RA and the end user
- The Service Provider that offers the end user services relying on the mobile PKI service for authentication and signing

These roles can be managed by different companies, or can be combined in various ways. The main benefit of using the Valimo Mobile ID is that for every role, there is the off-the-shelf product that implements the required use cases.

In Finland, each operator decided to implement their own mobile PKI infrastructure end-to-end. Each operator has their own certification authority, back end services for signature life cycle management, verification, roaming and message delivery, their own SMS Center, and service provider customers. It was also decided early on that the infrastructure

Through the Software Development Kit (SDK) the service provider can integrate their services within hours to the Valimo Mobile ID infrastructure for the benefits of users.

Mobile PKI interoperability: it’s easy and it works!
must support roaming digital signatures. Users can then use all the services, even if they are not connected to their own MNO network.

With this approach, operators can all sign up service providers, and according to the MNOs the competition is fierce. This will serve all operator interests as they need to push the credentials to the end users and attract them to use the services. If one operator signs a service provider, all operators benefit.

This approach gives the MNO complete control over the mobile PKI technology. They do not have to rely on third parties nor buy the service from competition. With the control, the importance of SIMs grows. By delivering PKI SIMs to the market before the actual launch of the mobile PKI technology, the MNOs are maneuvering to create a more permanent tie-in in their customer relationship. Once the end user has enrolled their credentials from her own operator, the desire to switch diminishes considerably. For the operator, mobile PKI and Valimo Mobile ID are tools to create loyalty within their customer base.

### Benefits for the service provider

One of the biggest advantages for the service provider is cost efficiency. According to the Tax Administration in Finland the cost for a single transaction went from 10€ - 50€ to a level of 0.20€ - 0.50€ per transaction when they adopted on-line services. The cost savings for the service provider, even in a small nation such as Finland, can be huge.

These on-line services are under constant threat. The on-line crime has turned into a highly professional business. The service provider needs to protect its own assets and give users the assurance their information is also protected. User’s trust is key for the service provider.

Today, passwords to protect customers and their data are not enough to create trust with the customer. They may even discourage potential customers, slow down adoption and eventually kill the service. More and more services are going into the cloud, and the normal authentication is username + password. Security breaches in these kinds of services are not even news any longer. Online services that offer alternatives gain competitive advantages over others.

Strong authentication is one way of mitigating some of the risks related to on-line services and Mobile PKI offers one of the strongest and easiest ways to authenticate the end user.

Another aspect in the on-line business is transaction protection.

There are several potential threats when a high-level transaction is made in an on-line service. Mobile PKI when done with Valimo Mobile ID offers two distinctive advantages over other methods:

- Transactions are signed using a method that complies with the EU electronic signature directive and making signatures legally binding
- The transaction and the identity of the user are protected against even the most sophisticated attacks. Pretending to be someone else requires access to both the service and the operator network. This is no easy task to do.

For the Finnish service provider, new on-line services can be delivered in a favorable environment with minimal risks as:

- they will be protected from fraud from the start
- the authentication process is already well accepted among the Finns
Benefits for the mobile network operator

Mobile network operators have to get the best ROI from their investments. They have to create new opportunities and generate revenue. Mobile PKI enables both. One of the issues service providers are struggling with is the mobilization of the user base. Users crave for services that are available 24/7, reachable from almost anywhere and at the same time they need security. Mobile PKI offers both. For the MNO it creates new opportunities in several ways:

• adds value to current services
• can secure new products and services to attract new customers
• can stimulate new business models
• can strengthen customer loyalty

For revenue opportunities the MNO can investigate these different options:

• Negotiate high volume, special priced authentication transactions for eGov, corporate or financial services
• Productize new services and integration options for the end user organizations
• Offer trust center-type of services to other organizations
• Generate transaction revenue in services requiring transaction verification (electronic signing)

Mobile PKI creates a wealth of new opportunities. For the MNO, it means offering new and innovative services to its existing customer base, targeting completely new customer segments and use cases where the MNO presence was previously only through subscriber base.

In Finland, right after the launch, one of the biggest insurance companies already supports mobile ID. Netvisor financial services has adopted the Mobile ID. Some of the Netvisor users access the site several times per day. A microloaning service and a pension fund provide Mobile ID authentication for their users. The Lahti municipality uses Mobile ID to authenticate people accessing several different online services. The National Board of Patents and Registration of Finland allow users to access the services using Mobile ID. Every week new service providers join the mobile PKI revolution and create more value for the stakeholders in the mobile PKI ecosystem. The main beneficiary being the end user.

Source: www.mobiilivarmenne.fi
Benefits for the government

One of the greatest assets of mobile PKI and Valimo Mobile ID is the ability to extend the national eID scheme in the country. Valimo Mobile ID enables governments to put the citizen electronic ID into every pocket that can hold a mobile phone. Complementing the national eID card the mobile PKI SIM card adds the true mobility factor into the eGovernment services. Now citizens can access services from all over the world, the only thing needed is a working SMS connection.

One of the biggest challenges in the market has always been the threshold in user acceptance. If the solution is too complex, the citizens may shy away from it. Using the mobile phone as a signing and authentication device is natural for almost all users, and when it is done Valimo way, using a SIM card one can also see it as the most democratic method of all – it can be available to anyone who has a mobile phone. mobile PKI truly brings power to people’s fingertips!

The Valimo Mobile ID provides also the capability to digitally sign documents. When using the EU directive as an example the Valimo Mobile ID can be used to produce advanced electronic signatures. The signatures created using Valimo Mobile ID are legally binding according to the directive. The way electronic signatures are created and acknowledged by the local legislation differs from country to country. But it is safe to say that the Valimo Mobile ID will most probably comply to local legislation when a legally binding electronic signature is in question.

Benefits for the end user

Extreme mobility is the most obvious benefit for the user. As Valimo Mobile ID is managed in the SIM card on the client side, it can be used with almost any mobile phone out in the market. Mobility is one of the key features that the MNO and service provider also see as a great benefit for the end user. The 3G coverage in Finland is very high and the price of mobile data is very low compared to some other countries. This has resulted in a wide adoption of 3G data packages within the Finnish public, and the result is that people use online services increasingly using mobile methods, either using a smart phone or combining the mobile data with a laptop and working remotely as many Finns appreciate to do.

Accessing on-line services and signing transactions become almost impossible to fake by fraudsters. This is a great illustration of usability and security working hand in hand. The end user has a strong authentication method available in his/her mobile phone. An extremely easy-to-use PIN is required to use the keys stored on the card for authentication or signing. For the Finnish market, this is extremely important as mobile phones have been part of daily lives for many years.

With Valimo Mobile ID, the value of the mobile phone increases even more. On top of games, entertainment, web access or banking applications, it offers electronic identity that travels easily with the user, strong authentication, and consent through secure electronic signature, secure banking access, age verification, and much more.

Valimo Mobile ID can open up a multitude of new possibilities for the benefits of users, mobile operators and service providers. Finland is a tech savvy nation, where innovations quickly go mainstream. In Finland people are demanding users when security is at stake. Valimo Mobile ID is answering these needs today.

Simplicity means success: when you need to authenticate, just type your authentication PIN code and press OK.

Extreme mobility but the Finnish way: working on a lake during a beautiful summer day
Let the users speak!

According to an on-line poll done by Elisa (as of 07/11/2011), here are the top applications where users people want to utilize Mobile ID for:

**61%**: **Banking** - Authentication, transaction approvals, document signing

**61%**: **Online shops** - Registering a customer account, confirmation of the order and payment

**60%**: **Personal customer service** - Verification of identity, payment confirmation

**53%**: **Public services** - Authentication, requesting test results, signing of forms and documents

**48%**: **Post** - Utilizing online and offline services, verification of identity, signing of documents

**43%**: **Library** - Loaning, reserving, and contact information changes

**43%**: **Expert services** - Verification of identity and personal information

**42%**: **Airline check-in** - As an identity document when checking-in

**37%**: **Registering** - Registering an online service

**32%**: **Vacation** - Buying a travel insurance before departure

**27%**: **Social media** - Anonymous authentication (age verification)

**19%**: **Liquor store** - Verification of age


**Good signs ahead.**

---

**VALIMO is your ID On-Line.** 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 multi-purpose 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 Finland and as from February 2010 part of Gemalto Group.
Improving trust: Strong and easy to use security for the user.

For further information, please visit: www.valimo.com