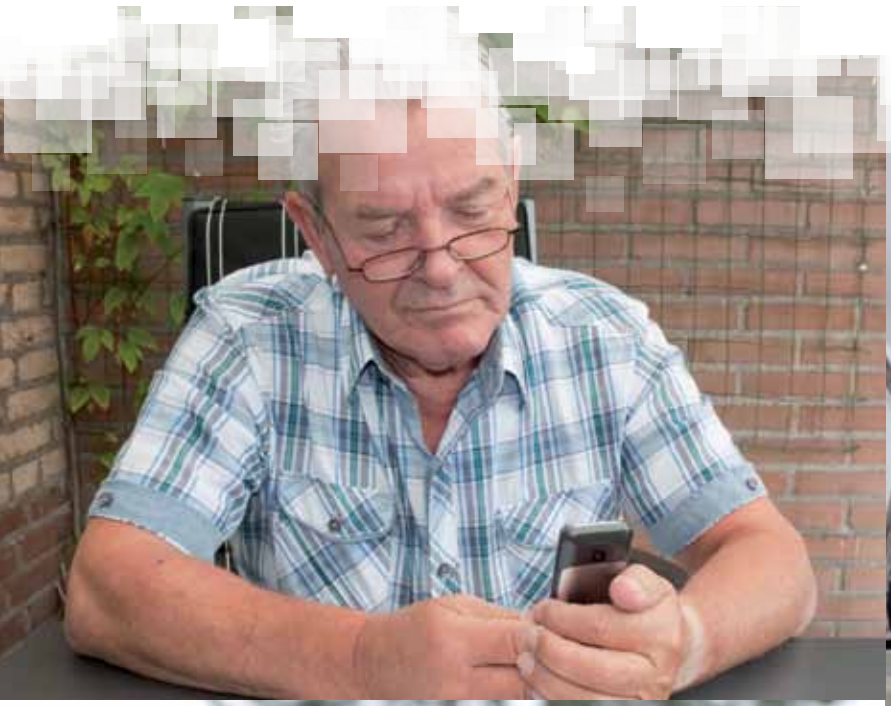
Mobile Identity

Finnish Mobile ID

A Lesson in Interoperability

Author: Alix Murphy



With special thanks to:

Pekka Turpeinen, Telia Sonera
Janne Jutila, Elisa
Perttu Hörkkö, Elisa
Lasse Leppänen, DNA

Antti Suokas, If Insurance
Esa Kerttula, Proftel Ltd.
Jari Kinnunen, HMV
Juha Mitrunen, Valimo
Kai Koskela, Osuus Bank Ltd.
Kimmo Mäkinen, State Treasury of Finland
Pekka Jelekäinen, Finnish Population Register Centre
Reijo Svento, FiCom
Tuomo Pyhala, S-Bank Ltd.

Contents

I Executive Summary

Identity is a core enabler for a wide range of services, especially payments, banking, government services and effectively all services requiring strong authentication of the user. As the underlying complexity of digital services grows, and digital fraud escalates, identity is increasingly being recognised as key to ensuring secure, validated communications and transactions across a wide range of sectors. At the same time, users around the world are demanding faster access to services via mobile, making the mobile medium an indispensable channel for providing secure and convenient access to services across many verticals.

Finland is a market in which mobile operators understood the importance of identity comparatively early, and have worked collaboratively in order to offer a mobile identity service that allows the user to strongly authenticate themselves across a broad variety of services.

Finland is an advanced market: mobile penetration is amongst the highest in the world, with over 90% of the population (of 5.4 million people)[1] having a mobile device, and on average, each subscriber having two SIM cards; the three main operators have all launched 4G / LTE networks and corresponding services. Approaching 90% of the population is already connected to the Internet.

The three leading mobile operators – TeliaSonera, DNA and Elisa, have launched Mobile ID ("Mobiilivarmenne" in Finnish), an identity service offered a shared, common platform for the authentication of users to third party service providers, irrespective of the network operator to which they subscribe.

Uniquely, the three operators have formed a "circle of trust" – an agreement under which the operators accept digital identities created by each other, and allow those identities to effectively "roam" on their network and make use of agreements that each individual operator has with third party service providers.

In spite of substantial government support and a commercially appealing service for both consumers and service providers, the mobile identity service continues to experience some challenges in reaching scale, mostly as a result of the "chicken and egg" problem – subscribers resist taking up mobile identity services until they are integrated by a broad range of third party service providers for everyday use, and - while many service providers have welcomed the advent of mobile identity services – some continue to resist integration until a large percentage of operators' customers have adopted the service. In particular, banks have been slow to adopt the new operator-driven Mobile ID solution due to a number of reasons.

Nonetheless, Finland offers a compelling glimpse of the future: mobile identity services are not only mature in their own right, but also offer consumers access to a compelling and growing range of services.

This case study explores the challenges that mobile operators have faced in deploying mobile identity management services in the Finnish market, and details the innovative approaches that the three operators took to overcome them.

1 Population Register Centre. 31 August 2012

Operator Profiles

TeliaSonera

TeliaSonera is Europe's fifth-largest operator, with subsidiary operators located in 16 countries across the continent and beyond, including Denmark, Norway, Russia, Spain, Sweden, Turkey, and Georgia.

Founded in the 1853, TeliaSonera is a pioneer of the telecom industry and is proud to be one of the early inventors of mobile communications and founders of GSM. In May 2011, TeliaSonera united the company under one common symbol and identity representing a total of 180 million total subscriptions (Q3, 2012).

"International strength combined with local excellence is what makes us truly unique - and provides a world class customer experience, all the way from the Nordic countries to Nepal. This combination has brought groundbreaking 4G, a world class fibre network, and introduced 3G at Mount Everest."

Elisa

Elisa is Finland's largest telecommunications and ICT service company, serving approximately 2.2 million consumers, companies and public administration organisations across the country. Elisa prides itself on being the market leader in mobile subscriptions, while offering a comprehensive 3G and 4G network in Finland. The company also offers international services in partnership with Vodafone and Telenor.

With a vision statement that clearly defines the company's goal to extend its ICT services into a broader range of day-to-day consumer and business transactions, such as digital TV and broadband, home security, and enterprise conferencing services, Elisa aims to position itself as "More than a network and the brand of excellence".

DNA

DNA Ltd is a Finnish telecommunications company providing high-quality, state-of-the-art voice, data, and television services to private customers and corporations. DNA's 3G network covering now five million Finns is continuing to expand, and 4G networks are actively (continuously) being introduced to new population centres (areas). In 2012, DNA recorded a turnover of EUR 769 million and an operating profit of EUR 56 million. DNA has more than three million mobile and fixed-line network customers. DNA and WELHO are registered trademarks of DNA Oy. For more information, please visit www.dna.fi.

II Finnish Environment

A. High usage of online services:

Finland has one of the **highest internet penetration** rates in the world, with around 88% of the population having access to online services via mobile, fixed broadband, or both. Accordingly, having an online presence is considered a necessity by most Finnish businesses, as online shopping, e-banking and other online services are the norm for Finnish consumers. Remarkably, well over 60% of Finnish adults, aged 30-45, regularly buy goods and services online.[2]

Many online services require some form of authentication of the user's identity, whether for login access or for secure payment or other authorisations. While simple username and password login combinations are still widely used by service providers, those requiring higher levels of security need to have a **strong authentication** solution that can efficiently authenticate the identity data of customers, while maintaining ease of use.

B. Prevalence of existing Bank ID solutions:

The Finnish Bank ID (or "TUPAS" as it is called in Finland) is a strong customer authentication process administered by all banks in Finland, which uses a combination of a PIN code and a One-Time Password (OTP) from a paper list which must be carried by the user at all times. Launched by the first banks 20 years ago, the Bank ID solution was perceived to provide satisfactory levels of security for online transactions and was swiftly taken up by third party service providers for authentication to their own services. There are currently around 3 million Bank ID subscribers in Finland, and Bank IDs can be used across a broad range of services and segments (not just banking), including e-commerce and government services.

Nevertheless, despite the high penetration of Bank IDs, the solution is coming under increased scrutiny as consumer demand for mobility grows and as stories of fraud and security breaches come increasingly into the public eye.

C. The Finnish Citizen ID card:

The third method of online identity verification and authentication used in Finland is the **National Citizen ID card**. However, despite being the first national eID card in the world, few people in Finland have a card or use it beyond its function as a travel document (the card is primarily used as an alternative to the passport for traveling within the EU). The Finnish eID card costs around €50 and is valid for 5 years. Authentication methods using the card have been adopted by fewer than 10 government services and very few private online service providers – primarily due to the high up-front costs associated with rolling out card readers at each office and point of sale.

Ultimately, the National Citizen ID card does not meet the needs of consumers wishing to access services remotely – either online or over their mobile phone - as it requires the person to be present at the point of sale. According to the Finnish Population Register Centre, which is the state Certificate Authority responsible for the Citizen ID certificates, a total of only 400,000 eID certificates were in circulation by end-2012.

D. Increasing fraud and security breaches:

There is a growing perception that the one-time-password system used by the banks is **vulnerable to fraud and theft**. Incidences of hacking, spam and phishing attacks are growing at a substantial rate, while criminals are becoming more sophisticated in their methods. The paper and plastic cards containing the One-Time-Password codes (which must be carried around by users) are increasingly seen as an antiquated method which is neither sufficiently secure nor user-friendly.

As the value and attendant risk of online activities grows, with consumers executing higher value transactions on the internet, service providers became increasingly keen to find new, more sophisticated means of creating and deploying digital identities for consumers.

What is "strong authentication"?

The term "strong authentication" or "multi-factor authentication" typically refers to a process of authentication which uses two or more different forms of identity verification. In strong electronic identification, the identification device and its user can ultimately be connected to the person's true identity. Most commonly, multi-factor authentication will include a combination of the following factors, or "proofs":

- something known, like a password,
- something possessed, like your ATM card, and
- something unique about an individual's appearance or person, like a fingerprint.

Using strong authentication provides more protection for sensitive information than a simple username and password can provide. When offered by an entity which is trusted to have gone through a strong registration process with the consumer (i.e. an operator which has registered the customer in person using their legally issued identity credentials, such as a passport), strong authentication provides the authenticating party (typically a service provider wanting to authenticate the identity of a customer) with the assurance that the individual is "known" and eligible to use the service.

Strong authentication is increasingly being recognised as a necessary security measure to ensure protection of sensitive consumer information, especially when conducting financial and other high-value transactions online. The European Central Bank recently published an document outlining a plan to require "strong authentication" on all web-based payment transactions by 2016. This potentially means that existing username-password –solutions would no longer be allowed as verification methods for transactions due to the inherent weakness in security in simple username-password methods.

2 TNS Gallup, March 2012
3 Finnish Ministry of the Environment – National Telecommuting Day 2012

E. Consumer demand for mobility:

Finland's SIM card penetration rose above 100% in Q4 2005, and smartphone penetration continued to increase rapidly (today it is already above 46%). These trends have implied a greater demand for a broad array of consumer and public services to be available via mobile. Working from home is also relatively common among Finnish employees (over 34% of employees work at least occasionally at home and 14% telecommute), making the demand for mobility even more material.[3]

Add to this the fact that Finland enjoys near 100% mobile coverage throughout the country (despite being both the eighth largest country in Europe and the most sparsely populated country in the European Union) and the opportunity for a mobile identity service seems clear.

These factors demonstrate the need for a more convenient, all-encompassing form of strong authentication in the Finnish market. In the autumn of 2008, a Finnish consortium made up of government and public services authorities, mobile operators and the Finnish Federation for Communications and Teleinformatics (FiCom), came together to develop the terms for such a new authentication and authorization service, in order to better serve the diverse needs of businesses and provide secure authentication for eGovernment services. **The result of these discussions was Mobile ID**.

Consumer demand for Mobile ID in Finland is very high:

According to an online poll undertaken by Elisa in November 2011:

- 53% of those polled wanted to access public services using a strong mobile authentication service, for services such as document signing and even requesting medical test results.
- 61% wanted to use mobile for transaction approvals and order confirmations for online shopping and banking.
- 43% wanted to be able to verify personal information via mobile for expert and professional services.

For more information, please refer to the following sources:

- http://www.mobiilivarmenne.fi/en/faq/
- http://valimo.com/products/government

III Description of the Mobile ID service

A. Vision & principle:

Seen by its proponents as the "solution of the future" for identification, signatures and payment approval, the Mobile ID platform is a secure identity verification tool which allows customers of third party service providers to login and access their accounts in one seamless process. Utilising the secure environment of the SIM and mobile SMS channel for credential storage and transmission, Mobile ID can be used in a wide range of everyday transactions.

Launched as an interoperable solution by the three main Finnish mobile network operators, Elisa, TeliaSonera and DNA, the logic of Mobile ID is simple: a service provider wishing to authenticate and verify their users can display the operators' common Mobile ID portal on their webpage, allowing any Mobile ID subscriber to authenticate themselves using their own GSM number and by simply keying in their user PIN after being prompted to do so by a flash-SMS message. With the trust framework, mentioned earlier, allowing for signature "roaming" between the operators, the user experience is the same regardless of which operator they use. In addition to web-based services, Mobile ID also works in a variety of different channels, including voice, mobile data and video conferencing.

"The Finnish Bank ID revolutionised online services by enabling secure e-business portals. It is now time for the next step in the evolution". (Elisa)

"Mobile ID is a convenient, cost effective and secure enabler for totally new mobile services". (TeliaSonera)

In March 2010, as Elisa, TeliaSonera and DNA came together to negotiate the trust network agreement and develop an interoperable platform for Mobile ID, the mobile operators defined and remained faithful to **four basic principles**, by which Mobile ID would be differentiated from all previous and existing solutions:

i. **Ease and flexibility of use** – By focusing on the principle that the consumer drives demand, user friendliness was of utmost importance to the design and deployment of Mobile ID. With a single user PIN to remember and no paper cards to carry, no extra hardware or software is required. Mobile ID works on 99% of mobile phones (both feature and smartphones) and can be used anywhere with a mobile signal, even from abroad as SMS roams internationally.

   Aside from mobility, the service also needed to be easy to acquire and the registration process made as seamless as possible. PKI-ready SIMs were already widely in use in the Finnish market: to activate the SIM for the Mobile ID service the user can either visit an operator store (a process which takes just a few minutes) or use an online portal. Another added benefit to the Mobile ID is its operability on all channels, including SMS, voice-call, face-to-face service channels.

ii. **Security** – The Mobile ID needed to be at least as secure as, if not more secure than, all existing authentication solutions.

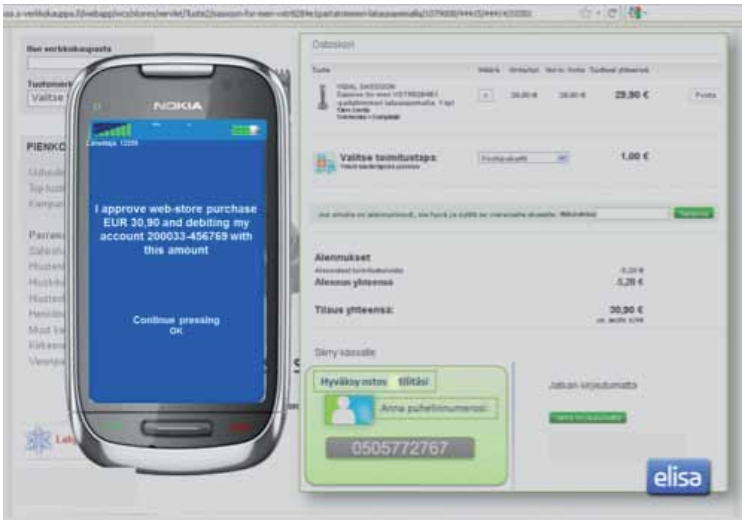
The SIM-based mobile PKI system underpinning the Mobile ID service offers a strong security proposition for all parties. All security-related operations are encrypted within the SIM-card, and all resulting messages are encrypted SMS-messages, while the GSM-number acts as the trigger for the Mobile ID transaction. The combination of two-factor authentication over two separate communication channels (IP and GSM) makes tampering or corrupting the transaction inherently more difficult than in most other solutions.

Mobile ID also uses *spam prevention codes* and *event (transaction) IDs* in order to protect the user from being disturbed by unwanted spam requests – a growing concern in Finland. With the event ID, the user is able to know when accepting a signature request exactly which event the signature request is related.

The European cross-border authentication framework for electronic identification (STORK) has developed a 4-stage classification for the security in authentication tools. According to this system, Finland's legacy Bank ID framework meets the requirements of Level 2, whereas Mobile ID is considered to meet the security requirements of Level 3 due to the inherent security of the SIM-based PKI-system.

Additional security comes from the user-experience: Mobile ID is inherently intuitive to use for the consumer, as inputting PIN-numbers into a phone is already an established routine.

Payment authorisation demo slide (by permission of Elisa)



Furthermore, studies prove that consumers notice losing their phone faster than losing other important possessions like their wallet. When a consumer reports their lost phone to their operator, Mobile ID ceases functioning in real-time, whereas it can take anywhere up to a week or more to cancel all one's cards in a stolen wallet.

iii. **Legal framework** – Two new changes to Finnish legislation governing identification and electronic certificate frameworks were instrumental in enabling the Mobile ID service to be launched:

a. **Act on Strong Identification & Electronic Signature** (effective from 1.9.2009):

i. Under earlier legislation, the registration and issuance of strong identification could only be performed by the Finnish Police authority. The change made it possible for private sector businesses with the relevant level of security and authorisation to also act as issuers of strong identification tokens and services.

ii. The act clarified that an electronic signature, if performed with an authorized strong identification method, was to be considered legally equivalent to a "wet signature."

iii. The law allowed for the issuing of new eID credentials based on other previous strong eID credentials. This made it possible to issue Mobile ID over the internet to customers already in possession of a Bank ID, provided that the parties can agree on pricing and sharing of risk.

b. **Population Information Act 2009** (effective from 1.3.2010):

i. The Finnish Population Register Centre (VRK), which holds national population data for the country and is the only state Certificate Authority in Finland, was originally the only entity with the power to issue the "Finnish Unique Identifier" (SATU) to an individual. Due to the change, all authorised strong ID providers, including mobile operators, could issue eID credentials with the "Finnish Unique Identifier." This enabled registration for the Mobile ID to take place in the operators' stores, without

the customer having to go to the police department to undertake the registration process.

ii. The legislation also clarified the fact that a person can have only one identity, but several certificates, such as a passport, driving licence, mobile ID certificate, Bank ID, etc.

iv. **Interoperability** – The unique feature which differentiates Finland's Mobile ID from many other similar schemes is the cooperative framework – or "Circle of Trust" – between the three main Finnish operators, Elisa, TeliaSonera and DNA. This trust agreement established an open four-corner business model and allowed for the roaming of Mobile ID requests between operator platforms. The business model does not suffer from competitive legislation challenges, as it is highly competitive both towards service providers and consumers.

As a result, a subscriber to Elisa, for example, can use Mobile ID to access service providers that have agreements only with TeliaSonera or DNA. Not only does this add value for consumers, it provides substantial benefits to third party service providers, since they only have to establish a single agreement with a single operator to be able to access all subscribers who make use of the Mobile ID service in Finland. In essence, service providers are federated across the three operators; the individual operators trust one another (a) to undertake the strong registration process with rigour and complete compliance, and to carry the legal responsibility for correct registration, and (b) they trust each other's agreements with third party service providers to be strategically logical and commercially viable (and attractive to subscribers). Each operator is responsible for ensuring that its customers follow the approved Mobile ID policies and guidelines.

Mobile ID: an evolved solution

Mobile ID is the result of a multi-year project involving entities from a wide cross-section of industries in Finland. Discussions around the possibilities for supporting the service began in 2005 and 2006 as the new Government came to office with a strong commitment to strengthening Finland's e-services ecosystem. Under this platform, the Information Society Programme Board saw to it that the Mobile ID was brought to the top of the agenda.

"When I first came to the discussions, I was surprised at how many ministries and civil servants were interested in this issue. Not only the Ministries of Justice and Communications were at the table, but also public service authorities on the fiscal side – in total, around eight different authorities. Then I understood what an important advancement this would be for Finnish citizens." (Reijo Svento, FiCom Director).

Mobile ID in its current form is the third generation of an evolving service. In 1999, Smartrust, a Sonera owned company, launched a SIM-card based mobile signature service for document signing in businesses. The first mobile certificate in the world was launched by the Population Register Centre that year, in a pilot for use in mobile banking. Though these early iterations were formative and ground-breaking, they were also a little too early, as appropriate infrastructure (such as capable handsets and SIM cards, as well as legislation and regulations) was not sufficiently widely deployed, and consumers were just beginning to understand the possibilities that the Internet represented. As a consequence, though many technical "firsts" were achieved, the services did not achieve mass-market appeal.

"The short answer is that it was too early. There wasn't the right legislation, no trust circle, no 4-cornered business model among the providers to make it scalable for reaching the mass-market. Finland has always been keen to develop new things, especially in the mobile world, so mobile identity was considered straightforward. But the market wasn't ready." (Esa Kerttula, Prof-Tel Ltd.).

Other smaller pilots have occurred since then, but the second real attempt was in 2005 when operators tried to launch a Mobile ID similar to the one today.

"At that point, the registration process was too difficult: because the authorities thought that Mobile ID was similar to your passport or driving license: the law at that time stated that only the police department could issue the strong identification. So, customers needed to go to the police station to get a Mobile ID. In the end, the process was too difficult, so it failed." (Antti Suokas, If Insurance).

With the third time, the Mobile Operators believe they have the process right. Better coordination, clarified legislation, new mobile signature service standards, and a greater number of service providers interested in the possibilities that Mobile ID offers have all come together to create an environment that is ripe for the success of the Mobile ID.

"From the end-user perspective, the service hasn't changed much. It's the same device, the same SIM card, the same SIM application toolkit, the same MSS channel. The difference is registration, and the service provider side of the equation. Now that operators can undertake registration themselves, it's become a straightforward and easy process. Also, because of the circle of trust – and the fact that third party service providers can gain access to all three operators' subscribers via a single agreement and a single technical platform, there's much more traction from companies across the Finnish economy, and government agencies." (Esa Kerttula, Prof-Tel Ltd.).

Another key change that has added to the growing success of the Mobile ID service is pricing. All stakeholders admit that earlier variants of the service were too expensive – seen from the perspective of consumers and third party service providers. Today, due to the Circle of Trust agreement which encourages competition among the operators to sign up service provider partners, as well as stronger interest from online service providers who recognise the key strategic value of the Mobile ID in reaching a larger customer base, the pricing offered by the operators is now more accurate. In these early stages, Mobile ID is offered as a free service to subscribers, while third party service providers are charged for the service on a per-transaction bases, with prices stratified based on the frequency, volume and value of the transactions being made. Most importantly, however, the price offered to third party service is around a third of that currently being charged by banks for use of their Bank IDs.

B. How it works:

How Mobile ID works: the consumer journey

When a user needs to authenticate their identity while using an on-line service:

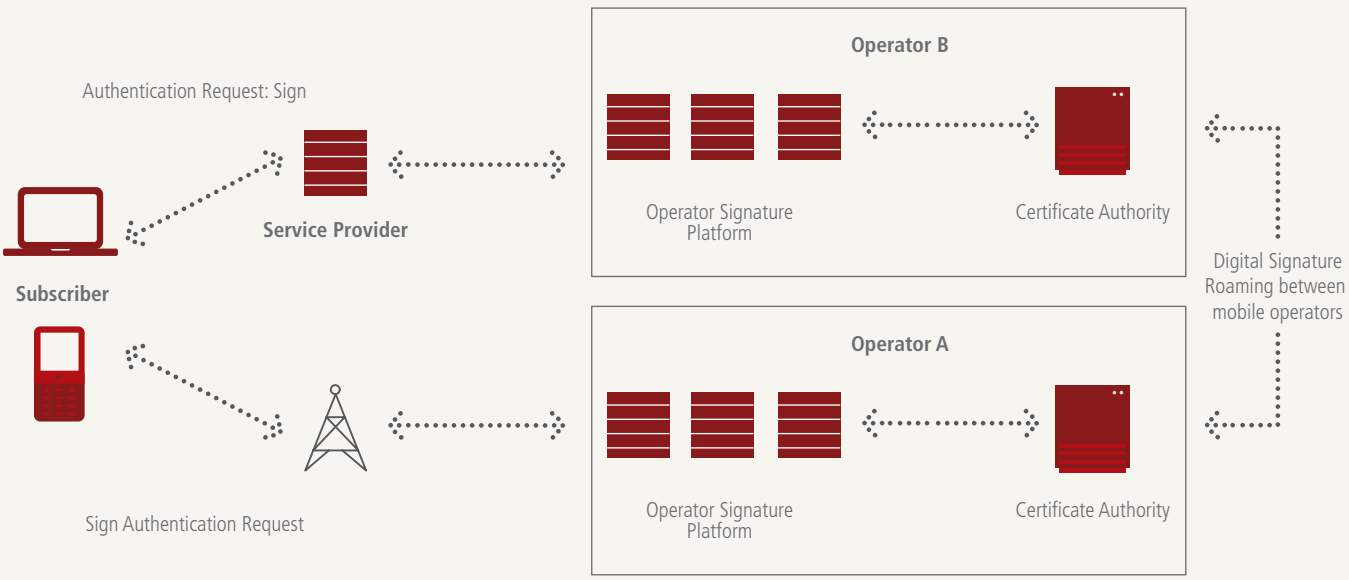
- The user recognises the Mobilivarmenne (Mobile ID) symbol as the interoperable mobile-based tool they wish to use, and clicks on the icon, which brings them to a login screen.
- The user types their phone number (which in this example corresponds to Operator A) into the login screen in the on-line service provider site. The number is transmitted over the IP channel while the response comes back to the user over theGSM channel).
- The Service Provider has an agreement for the Mobile ID with Mobile Operator B.
- Mobile Operator B recognizes the user as an Mobile Operator A subscriber and so forwards the authentication request to Mobile Operator A (signature roaming).
- The user receives the authentication request to their phone and inputs their unique user authentication PIN (4-8 digits). If the PIN code is correct, the SIM application signs the authentication request.
- The result, now verified, is sent back to Mobile Operator A and the user is granted access to the service.

The user's actions in this strong authentication case (2 factors, 2 channels) comprise of:

1. Input the mobile number (on a PC, for example).
2. Input the PIN (on the mobile device).

In the end, all that is required of the user is the physical possession of a phone and PIN-code.

User authentication using signature roaming between Mobile Network Operators



C. Technical solution:

i. The mobile certificate (also referred to as "mobile ID", "cell phone ID", "cell phone certificate") is an electronic personal identity certificate which the SIM cardholder may use to prove their identity within the context of different electronic services or electronic signature situations. The mobile certificate contains the personal details of the SIM card owner and is held in a directory, while with the corresponding private keys are embedded in the SIM of a mobile phone.

   Key elements of Mobile ID certificates:

   – Support both identification and signature services.
   – Used in all cases where the individual must prove their identity in the electronic world, i.e.:

     a. banking, public services etc. ("old" cases)

     b. social networks, gambling etc. ("new" cases)

   – Always uses the same user PIN.
   – Security of 2 channels: activity is over (fixed) Internet channel and identification is over mobile network.

   Services based on similar technology are already used in several countries, including Turkey (bank identification, cash withdrawal from an ATM), Estonia (citizen certificate in extensive use for e-services) and Norway (BankID).

ii. Using a single nationwide standard for mobile PKI greatly facilitated the implementation of Mobile ID. In Finland, a selection of standards established by the international standards body, ETSI, are applied to the Mobile ID service. These include:

   a. ETSI TS 102 204 for service provider integration;

   b. ETSI TS 102 207 for the roaming; and

   c. ETSI TR 102 203 for business and functional requirements.

   In addition to these, the ETSI Mobile Signature Service Provider (MSSP) standard enables signature transmission and authentication across all operators.

iii. The mobile PKI infrastructure used in the Mobile ID is uniform across the three operators. Productised APIs for the service were provided by various technology firms (Valimo Wireless, Methics Inc. and others). The underlying uniformity of APIs enabled the operators to offer an identical experience for service provider clients and correspondingly, end users. The signing PKI application is stored on the SIM card, allowing the user to receive digital signing requests and to produce the signed response by entering their unique user PIN code. The digital signatures use the RSA algorithm with either 1024bit or 2048bit key-length.

For further information on the Certificate Policy or the ETSI MSS standards employed by the Mobile ID solution, please refer to: http://www.mobiilivarmenne.fi/en/documents/

IV Uptake and Scale

A. Adoption by Businesses and Third Party Service Providers:

i. The primary value of the Mobile ID to consumer-facing businesses is the potential of reaching all Finnish mobile subscribers with **one single, seamless integration process for digital authentication and signing.** Historically, any business that wanted to offer electronic or web-based services needing customer authentication needed to sign an agreement with each of Finland's banks independently, in order to use the Bank ID scheme. This meant that, as is often the case, businesses ended up having to execute at least 10 separate agreements and integrations with banks, each with its own fee structure and certificate scheme. Some public service authorities offering multiple services had to execute up to 80 separate agreements with different banks.

   As a consequence of its technical uniformity and commercial simplicity, the Mobile ID service supports the same user-experience across all channels, including internet services, mobile, voice and video, meaning that businesses can ensure full coverage and customer-reach in their segment or vertical. Service providers need only sign an agreement with one operator in order to offer the service to all participating mobile subscribers of the three operators combined.

ii. The availability of the service on **multiple channels** allows service providers to work flexibly with customers on whatever medium they are using. For example, when a customer calls their customer service number wishing to make changes to their agreement, rather than providing their address or the last four digits on their social security number (typical security questions in a voice-based authentication procedure), the user subscriber GSM-number is picked up from the call and a PIN-verification request is send over the SMS channel (the user PIN is never transmitted). With a correct answer, the operator service certifies the caller ID during the call.

iii. Unlike the proprietary authentication systems used by Bank ID, the **competitive dynamics** of Mobile ID mean that the operators compete on partnership with service providers, thus keeping the pricing for the service low and the incentive high to develop and deliver innovative value-adding eServices within a high-security architecture.

iv. The interoperable model provides an **ideal platform for government and public services authorities**, who recognise the need for a cost-effective and user-friendly method of strong user authentication across their e-services platforms. With 200% SIM penetration in Finland, as well as the fact that the service works on 99% of phones, Mobile ID offers the foundations of a nationwide eServices ecosystem, with the potential to address the majority of the Finnish population. In 2012, VETUMA (the eAuthentication and payment service used by federal and municipal Finnish government agencies) activated Mobile ID for all VETUMA clients, meaning that over 140 public organizations were now able to authenticate citizens for access to their service using Mobile ID.

"For the Finnish Government, Mobile ID is the most cost effective way to provide an authentication method to citizens." (Kimmo Mäkinen, Service Manager." State Treasury of Finland).

v. The multi-channel capability of Mobile ID, including voice and video, gives services providers the opportunity to build a wide array of **additional value-adding services in the future**. Studies are currently being conducted on the potential for Mobile ID to be used by medical professionals for signing prescriptions and securely sending essential health records during specialist referrals. By the beginning of 2014, all social sector clerks will be issued with mobile apps for access to records and systems while out of the office. Mobile ID is also being considered for use in checking and verifying information from different healthcare and social sector registers.

B. Challenges to scale

Nevertheless, despite the strong value proposition to Finnish businesses, some challenges remain to obtaining scale among service providers:

i. **Two-sided market** – Like any new service offering, there is a "chicken and egg" challenge to be overcome. Users are unwilling to adopt a new service when relatively few services are appended to it, and, equally, service providers tend to adopt a "wait and see" approach – preferring to deploy the solution when there is a critical mass of subscribers.

   Some forward-looking service providers have recognised the potential that Mobile ID can bring for their future service offerings and have decided to adopt the service. These early pioneers include insurance providers, smaller local banks and government public service authorities.

ii. **Resistance from banks** – As the predominating providers of online authentication for nearly 20 years, banks in Finland are understandably concerned about the entrance of Mobile ID onto the market. The open-four corner business model employed by the operators is also likely to increase competition between banks by enabling consumers to shop electronically between bank offerings. While a number of Finland's banks foresee the value in employing another trusted entity to undertake the costs associated with the strong electronic authentication process, the banks have their own legitimate considerations regarding security and operability which they believe need to be addressed.

   The Finnish banks articulate their concerns in the following manner:

   a. **Security** – Banks view their Bank ID solution as a "gateway" into participating banks' internal systems and to the assets held by their customers. As such, the security of that system is of utmost importance. Banks have therefore been understandably keen to rigorously check and recheck the security of the Mobile ID solution, to ensure that it is as secure as

their own, trusted solution – and to further ensure that it provides additional value (in terms of functionality and usability) for bank customers.

A key dimension of this security question is the process of customer registration, as this is the point at which trust is laid down between the registering party, the authenticating party and the customer. For banks and service providers alike, there is significant financial and reputational collateral riding on the trust established at this point: and all parties need to be certain that the registration process is applied uniformly, rigorously and without compromise by mobile operators.

Additionally, the majority of banks have their own certificate standards, formats and policies internally. Conferring trust onto mobile certificates is a lengthy and complex process. Secure certificates sit at the heart of strong authentication processes, and a great deal of thought goes into the design, storage and use of certificates for different use cases. Accordingly, being prepared to migrate to the use of a third party's certificates (in this case the mobile operators) requires a great deal of investigation and negotiation – particularly for banks, whose online / digital activities tend to have a comparatively high level of risk appended to them.

In fact, the registration process for Mobile ID customers is exactly the same as that for Bank ID customers, and is administered by professionals with the same training in trust issuance and compliance as those providing ID documents in the public sector (e.g. the police department). Under Finnish law, Mobile ID has been deemed to offer an equivalent security level to that of the Bank ID.

The Finnish Communications Regulatory Authority (FICORA) has the authority to give permission for companies to issue Mobile IDs, but very closely oversees and scrutinises their activities.

"We've worked together for many years and our colleagues in the mobile operators now understand the high level of risk and subsequent security that we require. We've had good relations with the three main operators but our industry background is different – it does of course take some time to overcome these differences"
- (Kai Koskela, SVP of Private Consumer Banking at Osuuspankki, the largest consumer bank in Finland).

b. **Regional banks** – For Finnish banks, the Mobile ID proposition offers a logical extension or "addition" to their Bank ID: the ability to authenticate customers over the phone is of great value. However, regional banks operating in Finland with headquarters based in Sweden and Denmark may have a different set of priorities. These banks express the need to have streamlined solutions across all markets, making adoption of Mobile ID more challenging. These banks also have other Bank ID solutions in operation in other countries in the Nordic region, for example.

c. **B2B clients** – The primary use case for Mobile ID is on the B2C side: for consumer facing business to verify their customers securely. However, for clients wishing to use the tool in B2B transactions and verifications, the challenge lies in enabling corporate representation using Mobile ID: in this case, the customer is a company, not an individual. While the certification process is no more complex for a business entity, the challenge emerges when multiple users with different roles in a single company need to use Mobile ID. The process is further complicated when an individual with access to the Mobile ID certificate wishes to leave the company, or transfer roles. These questions are among those currently being addressed by the Finnish mobile operators.

d. **Two-sided market** – Even for those banks wanting to offer the Mobile ID solution for access to their own banking systems, or to integrate the service with their Bank ID on other third party websites, the investment required for this transition requires a level of market penetration among other service providers that has not yet been reached. For those banks on the verge of accepting the Mobile ID solution, one factor informing their resistance is the notion of "going it alone" without the other banks.

e. **Revenue** – Each bank has its own pricing structure for charging service providers for the use of its Bank ID service. These pricing structures are based on the costs to the bank for maintenance of the service, the cost of the certificates, and the pricing structure charged to consumers (i.e. most banks charge customers on a monthly subscription basis, but charge service providers per transaction).

Additionally, because some services are high value but low volume, or vice versa, the values per transaction are differentiated depending on the volume used (i.e. from €0.05 and €0.10 per transaction for "high-volume, low value" through to €0.30-0.40 per transaction for "low-volume, high-value"). In some cases, the difference in volumes can be from thousands to millions of transactions, depending on the service. As a result, those banks which derive substantial revenues from the Bank ID service are less willing than others to support the Mobile ID service's entry into the market.

Nonetheless, as this case study went to press, a consortium of Finnish banks were in discussion with FiCom and the Finnish mobile operators in order to negotiate a working agreement on the potential use of Mobile ID for online banking access, amongst other things.

A Service Provider's Point of View: If Insurance

Interview with Antti Suokas
(Business Developer, If Insurance)

If entered the project for Mobile ID with Elisa almost 3 years ago, as part of an attempt to adapt to changes that were expected in the insurance market. "In fact, the biggest need we foresaw at the time was in registration for car insurance – there needed to be a way to do the process electronically, to reduce the hassle of processing lots of paper and to eliminate the need for the customer to go in person to the authorities. That's when we heard about the Mobile ID idea."

If's criteria when assessing the Mobile ID: "Good customer service is part of our core business. We needed to find a way to identify customers and to get electronic signatures for consent over the phone, but any solution needed to be hassle-free and easy-to-use for the customer. Usually, when we serve our customers we use some kind of logical identifying questions to ensure that the customer is who they claim to be (usually these are pieces of information that only the customer should know, such as their social security number, details on the insurance they have, etc.). With Mobile ID, we could eliminate this process."

Cost: "Another very important criterion for us is that the cost of the Mobile ID is around one third of cost of equivalent Bank ID. We have over 1.7 million logins per year, so this is a remarkable price reduction. Also, like many service providers in Finland, we have to enter into separate agreements with each of the banks. This creates a lot of work for us. We built our business case for Mobile ID on various assumptions on the penetration of Mobile ID and the level of savings we could make, and it worked out in every scenario."

Being ahead of the market: "We were the second company in Finland to start using Mobile ID. We wanted to show that we were front-runners in the market and to be the first big, mass-market consumer-facing company to be using it (the other company at the time was a small scale start-up company providing electronic signatures for business contracts between companies). It's a strategic move that we are still proud of."

"When we originally started to look into Mobile ID, we saw it as a potential replacement for Bank ID. But now we recognise it as a complementary tool to improve the user experience, especially in terms of adding new services. I think other service providers are seeing this as well: now there are more than 200 service providers using Mobile ID."

Launching the service: "Before we launched Mobile ID to our consumers, we wanted to test out the service. Our first target group was our own personnel. We thought that once our own people were familiar with it, it would be much easier for them to promote and give support to our customers. In fact, this was extremely useful as we found out the questions that customers would be asking about it. The feedback: "They loved how easy it was to use! Basically, the main questions were 'So now I can use this with our (IF Insurance) services, but where else?'"

"Other initial concerns related to the security of the tool, as well as questions related to the actual process for obtaining a Mobile ID. For example, the Mobile ID needs a PKI enabled SIM, so those people with older SIMs needed to switch over to new ones. People were worried that they would lose all their contact information. Luckily, the operators had started to introduce the new SIMs a few years ago, so this wasn't a problem for most people."

"Now, we try to actively promote Mobile ID to our customers as much as possible. But we do this in the same way that we promote our other services: as part of our service portfolio. On our main login screen we have a description of mobile ID and tell people that they need to contact their operator in order to get one. Our basic message to consumers: "It's the way of future; start using it already!"

Plans for the future: "One of the most important additional functions we want to enable with Mobile ID is signing documents and obtaining approval signatures from customers over the phone. If you could do this over SMS – even while you are speaking on the phone to the customer service representative – the whole process could be completed in one single session. Additionally, unlike the Bank ID which only provides the name and customer number, with Mobile ID we could add a lot more information to the customer profile, such as the address, basic credit checks (all with the customer consent, of course.) Mobile ID offers a whole range of opportunities that Bank ID doesn't."

"The challenge we still experience is that many of our customers don't have a Mobile ID yet, so the penetration is still too low to make the investment to build these additional kinds of services. Once the banks join us, I believe the penetration of Mobile ID will grow quite rapidly."

"Facilitating the online registration process for customers will be a major factor. At the moment, only a few banks allow the Bank ID to be used as pre-authentication for online registration to obtain a Mobile ID, otherwise the customer must go in person to their operator to get it. Once the online registration process is solved, it really can't get any easier for the customer. This is the part we are waiting for. But because banks are so resistant to this they are holding back promotion and marketing activities for the whole market."

Message to other service providers: "As with many new products, there's a snowball effect. The tendency in these situations is that companies think they should just wait to see what others in the market do. When I talk to other service providers in Finland I tell them: "We are big in the market. If we believe that we should be doing this, then you should as well. As an insurance company, our business is based on trust, so if we think Mobile ID is secure enough for us then it should be for you, too."

The other message we want to give is that the first step doesn't involve any big risks at all. Our biggest costs were on the pre-study and a few days' work for our IT department, but that's all. The cost structure for Mobile ID is to pay per use, so if people weren't using it then we weren't paying the operator. I try to tell them, "don't wait – just do it and see what happens!"

C. Consumer Uptake

i. The Mobile ID service is currently offered as a free service to individuals, and is viewed by its users as far more convenient and user friendly than existing Bank ID or Citizen ID card authentication solutions. The ability to access secure accounts from anywhere, at any time, without the need to carry a plastic card with OTP codes is very appealing to Finnish consumers. Additionally, anyone who has two bank accounts requires two separate Bank IDs, with two separate PIN codes and plastic OTP code cards.

ii. Nevertheless, low awareness among consumers and slow service provider uptake to date have meant that Mobile ID was not taken up by consumers as quickly as the operators had hoped. One primary reason attributed to this relatively low uptake is the registration process required in order to obtain the Mobile ID. Currently, two methods can be used for registering for a Mobile ID:

a. **In person at the operator store**: The in-store registration process entails collecting the user's personal information, verifying the ID documentation (typically a passport, driver's license or national Citizen ID card) and verifying the customer's subscription to the SIM. The process can be done in any operator store around the country and takes approximately 8 minutes in total.

b. **Online using the Bank ID**: Around 4 Finnish banks currently have agreed to offer their Bank ID as a component of the online pre-registration process for their customers to obtain a Mobile ID. Users who have already gone through a hard registration process with their bank can use the strong authentication process of the Bank ID to verify their customer information on their operator's website. The ability to issue Mobile ID "over-the-air" is based on the fact that most SIMs in the field are Mobile ID capable already. This process only takes 3 minutes and is therefore considered to be far more convenient to the customer.

In the eyes of the three mobile operators, enabling the pre-registration through the Bank ID is a key milestone for facilitating scale and uptake among users.

However, so far, only 4 of the 10 banks in Finland have made an agreement to allow their Bank ID to be used in this way, meaning that the threshold for Bank ID authentication established by the operators has been limited (in Elisa's case, only 50% coverage). As a result, the level of market penetration necessary for investment in public awareness marketing has also been delayed.

iii. The additional limitation to scalability is the **uptake of daily, high-value services**, especially in internet-banking and payment approvals. Reaching high volumes for services used by consumers (compared to those used less frequently, such as insurance and government services) is important for maintaining scalability for the operators, as well as increasing awareness and user-familiarity with the service.

"For consumers, these (high volume) services are interesting enough to go through the first authentication threshold and encourage them to obtain the Mobile ID." (Elisa).

"I'll never go back to plastic cards" (user of the Mobile ID service).

For further information on the Mobile ID as presented to customers, please see:

http://www.mobiilivarmenne.fi/en/faq/

Official Mobilivarmenne website

What?	Where?	Why?	Who is it for?
The mobile certificate is your digital ID in your mobile phone. With it, you can prove your identity and use electronic signatures in different electronic services.	With the mobile Certificate, you can prove your identity online or during a phone call in an easy way. It is compatible with online services that require identification and will also be compatible with bank services in the future.	The mobile certificate is absolutely secure. It functions with an access code which only you know. With the mobile Certificate you can take care of electronic business in a convenient way from start to finish.	The mobile certificate is compatible with all Finns' mobile phones, and you can easily have it activated by your operator.

V Economics

A. Business model

i. In establishing a "Circle of Trust" between the three operators, the Mobile ID offers a significant advantage over other existing solutions. The model is service-provider driven: the service provider has an agreement with a single operator, under which the payment structure and revenue generation is derived.

ii. **Pricing structure**:
The three operators compete on pricing packages to service providers. For example, Elisa's pricing is standardized for all service providers, with volume-discounts for high-volume service providers. For consumers, Mobile ID will remain free until penetration levels have grown sufficiently.

According to Elisa, this aspect of their business-mode was publicly stated from the start of Mobile ID. Today, Mobile ID is packaged as a value-adding service to the user's mobile subscription.

B. Roadmap to commercialisation & sustainability

i. There is still some disagreement as to the form that future revenue models for Mobile ID should take. Some believe that once the service reaches 25% penetration of end users, operators can start charging consumers via billing or a subscription-based payment scheme. Others, however, believe that the solution should not cost anything for the end-user and that total cost should fall on the service provider, at least the mass-market segments. When it comes to enterprise subscription to the Mobile ID, there may be some ability to charge enterprises for use of the service.

Elisa: Bringing the Mobile ID to market

The strong authentication market is small but rapidly growing. In Finland we see approximately 30% growth annually. Commercially, the most important emphasis will be on value-adding services, such as mobile purchases, remote payments over the internet and mobile (potentially, this includes NFC-based physical payments in the near future), as well as a multitude of eServices requiring approval or signature from the consumer. Mobile ID will be a key enabler in these and many others. In this way, we see the Mobile ID as a "control and value-capture" point.

We saw market-entry as a "chicken-and-egg" situation: no users means no services, which means no reason for users to join and the same for service providers. But this is often the case in the telecoms arena. So, we started enticing the service provider side with the aim of having enough services to implement Mobile ID across multiple industries, and also focused on trying to attract high-involvement services. After approximately 12 months, Mobile ID was usable in most internet-based services where the Bank IDs were historically used for strong authentication.

What's important to recognise is that high-involvement services can be of two sorts: existing ones such as Internet banking, and new-ones where Bank IDs are not feasible. These latter services are typically services that rely on mobile phones and applications, such as mobile-based purchase and payment approval. Both require new service design which, from the point of decision to the point of public launch, can take on average 12 months or more to develop. Thus, these services are only now entering the market.

Eventually, what we want to establish is a world where your Mobile ID becomes the eID used everywhere. Estonia has managed to do this with their eID and there is now strong push to do the same in Finland since the benefits are huge. We could eventually provide proprietary IAM (Identity and Access Management) systems for service providers to identify their employees) (e.g. policemen or healthcare care professionals) by offering mobile PKI based solutions for that process. For the time being, however, we think the best approach is to offer our current generic Mobile ID for all and then build on additional identity relevant services that can be adjusted for the particular use case (i.e. allowing for degrees of access relevant to the service).

We are confident that the market will move in our direction. On the consumer side, the main threshold is user familiarity with Mobile ID. Our experience is that after three transactions the consumer feels comfortable with Mobile ID and then becomes an active user. We have ongoing activities to increase usage frequency, but in our view, the current starting-phase user-frequency has been in line with our expectations.

Elisa's business model has been publicly stated from the start: we aim to earn revenue from both service providers and from consumers. We know it will be important to standardize the pricing structure for service providers and we give volume-based discounts for high-volume service providers who use our service. For consumers, Mobile ID will remain free at least until the end of 2013 when the penetration has grown sufficiently and familiarity is well established.

ii. A number of other models are currently being discussed to look at the viability of integrating Mobile ID with existing solutions, or providing support in scaling service adoption by rolling it out among public service authorities. One such model being proposed by some would be for use of Mobile ID in public and e-government services. In this model, the Finnish Government would provide some support for infrastructure development and integration of the services, while each public service authority would sign a service agreement with their customers.

C. Future services enabled by the Mobile ID

i. As mentioned above, current usage of Mobile ID is seen as the "tip of the iceberg" in terms of the services and processes that it could support, across a broad range of industries. Eventually, the operators want to reach a point where Mobile ID becomes the eID used everywhere, for services beyond simple authentication and access, by empowering service providers to build flexible and customer-tailored services based on the strong identity credentials held by the operators.

ii. A number of feasibility studies are currently being undertaken on the potential use of Mobile ID in healthcare (see box below), social services, payments, person-to-person verification (e.g. over voice) as well as options for direct customer care by consumer-facing businesses. One important future use-case for Mobile ID that the operators are examining is over the Near Field Communication (NFC) channel. This would be of particular interest in scenarios where the customer authentication process needs to be quicker than over the mobile or internet channels, such as in-store payments, transport and similar.

Mobile ID in the future: Healthcare prescriptions

Studies into the use of mobile certificates in the healthcare industry have now been underway for several months. For example, a solution for mobile prescription authentications by qualified healthcare providers was also considered during the earlier Mobile ID launch in 2005, but it was not developed due to the low uptake of the service.

The idea is now being taken up again in a feasibility study being commissioned by the Finnish Population Register Centre . Finland has 300,000 healthcare professionals, meaning that enabling Mobile ID to act as a doctor's signature for prescriptions would open up a significant number of high-volume transactions. In this model, the certifying body would be the state certificate authority, the Population Register Centre, which would issue the certificates to doctors and other medical professionals. According to early findings from the study, this service is feasible and will take around eight months to develop the solution.

"Life-changing solutions like this one are now close at hand with the Mobile ID. We at the Population Register Centre know that 95% of the (mobile certificate-based) solution is ready; what it needs now is a strong business model to connect the healthcare sector to the mobile operators.

Similar studies like this one are being conducted across a range of sectors where Mobile ID is perceived to have the potential to vastly improve the conduct of day-to-day activities of both employees and consumers. For example, a number of public and social service authorities are considering Mobile ID as a tool for social workers to use in accessing records while out of the office.

VI Mobile ID – Key Success Factors

A. Interoperability

By establishing a "Circle of Trust" between the three operators, Mobile ID was able to offer a significant advantage over other existing solutions. This unique model of strategic collaboration, whereby the operators present a unified, seamless platform but were still able to compete with each other for revenue on the service provider end, allowed the operators to work together to cover the market and reach scale.

However, the operators have learned that in order to reach the scale and penetration they hoped for, there still remain a number of challenges to be overcome.

B. Reaching high frequency transactions

High volume transactions, such as banking, online payment and e-commerce verifications, will be the key to driving sustainability in terms of revenue and reach. Consumers are more likely to "stick" to Mobile ID if they use it frequently; while service providers are more likely to invest in adopting an authentication service that consumers will use often. Sustainability in the business model for operators is gained from those service providers who process a greater volume of low-cost, high frequency transactions over time.

Once the point of high frequency is reached, the range of additional value-added services which can be built over the top of the Mobile ID is infinite.

C. Gaining acceptance of the banks and new mobile payment service providers

Determining a basis upon which Mobile ID can enter the market and stand compatibly alongside the Bank IDs will be crucial to ensuring the success of the solution. Mobile ID does not need to be viewed as a direct competitor to the existing Bank ID solutions; indeed, there solutions are mutually compatible and can provide a combination of greater convenience and security to the consumer when offered together. Facilitating the online registration process for Mobile ID through the customer's existing Bank IDs, for example, will greatly empower both solutions to better serve the user.

Different solutions to this challenge are currently in discussion, including the concept for a potentially interoperable model for identity authentication between all three solutions (Mobile ID, Bank IDs and the Finnish National Citizen ID card), which would greatly reduce the burden for service providers in terms of system design and integration.

The key learning taken from this situation by the mobile operators is the value gained from listening to the needs of other industry players in the identity market. Ultimately, clear and open discussions with the Finnish banks resulted in the mobile operators being able to develop a more robust solution which meets the security needs of financial service entities, while working with the Finnish legislative authorities to ensure that these specifications were made clear by law.

D. Positive role of government:

i. **Legal clarification**:
Clarification of the legal framework regarding Mobile ID was key to ensuring the successful launch of the solution. By establishing legal justification for the competitive "Circle of Trust" between the operators, and by adjusting the legislation to allow mobile operators to act as issuers of strong identification on the basis of their strong Know-Your-Customer (KYC) processes, the Finnish government paved the way for Mobile ID.

ii. **Unifying role played by FiCom**:
The Finnish Federation for Communications and Teleinformatics (FiCom), Finland's national telecoms representative body, played a crucial role in bringing the mobile operators together to speak with one, unified voice with the Finnish Government and other key industry stakeholders during the establishment of Mobile ID. Through the work of FiCom, the key legislative and technical solutions embodied in the trust agreement were defined among the operators in order to launch a fully interoperable service.

iii. **Role of government in driving service uptake**:
Governments around the world are beginning to recognise the positive benefits of mobile identity for citizen authentication and access to public services. The Finnish Government is developing plans to make all public services fully available online by 2015. By encouraging migration to e-services which require strong authentication solutions, the Government will help to drive uptake by consumers who recognise the value in being able to access services – for activities as diverse as accessing private health or housing records, bidding for housing, receiving benefits, filing taxes – all from their mobile phone.

Mobile
Identity

For further information, please visit www.gsma.com/mobileidentity
or contact the GSMA Mobile Identity team at
mobileidentity@gsma.com