



Mobile
Identity

Estonia's Mobile-ID: Driving Today's e-Services Economy





Contents

I Executive Summary	4
Operator Profiles	5
II Estonia: A Digital Society	6
A. Digital Agenda	6
B. ID-cards and digital signature	6
C. Baltic & International cooperation	7
III Estonian Mobile-ID	9
A. Vision & principle	9
B. How it works	9
C. Technical solution	10
IV Uptake and Scale	11
A. Rapidly changing consumer demand	11
B. Businesses increasingly turning to mobile	11
C. Early adoption and promotion by Banks	13
D. Public Sector recognition and promotion	14
E. Clarifying legislation	16
F. Wider availability of Mobile-ID	16
V Challenges	17
A. Awareness	17
B. Cost	18
C. Business model	18
VI Mobile-ID: A vision towards the future	19



I Executive Summary

Estonia is swiftly gaining international recognition as one of the most digitally advanced societies on the planet. Citizens in Estonia can access and conduct a broad range of services and transactions either online or from their mobile, including accessing private health records, declaring taxes and signing legal contracts. Estonia also boasts one of the world's most advanced digital signature systems, with over 80,000 digital signatures made each day. 99.6% of banking transactions in Estonia are now done electronically and, in 2012, 94% of people declared their income electronically. In 2011, the country was the first in the world to allow m-Voting in the national Parliamentary elections. 3% of all votes were conducted via mobile.¹

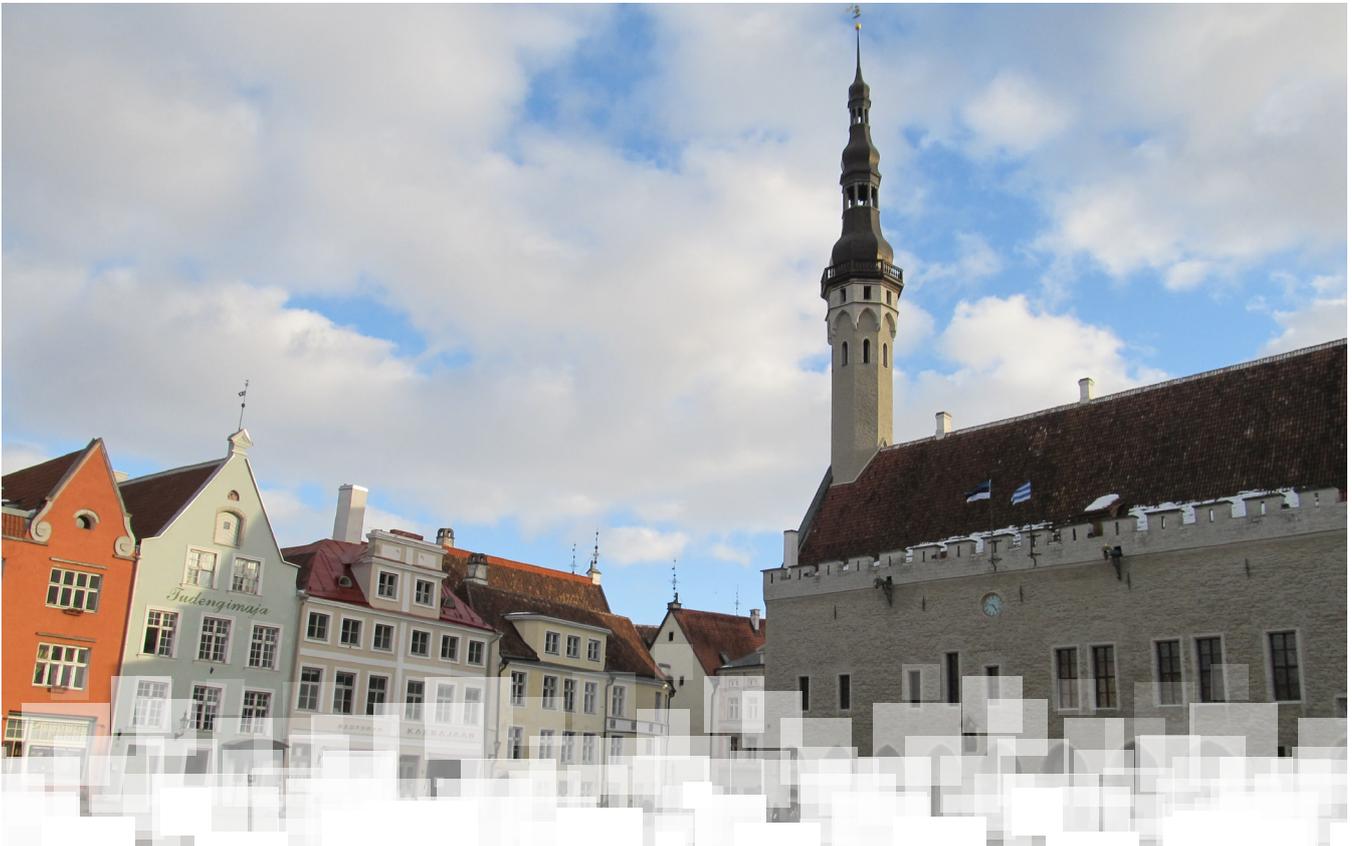
Mobile-ID (Mobiil-ID) was launched in 2007 as an extension of the digital ID scheme in which citizens can access information and personal data, and

authenticate online transactions using the secure PKI infrastructure in the ID-card. Currently, Mobile-ID can be used with over 300 organisations in both the private and public sector, ranging from electronic banking to applying for a driver's license, to entering or accessing academic grades at university to changing a pension plan, all through the electronic signature function of the mobile which holds legal equivalence to a wet signature. According to e-Estonia.com, Mobile-ID users can legally register a new business in just 15 minutes.²

Contrary to what one may assume, uptake of Mobile-ID in Estonia has been very much private-sector driven. Currently, there are around 40,000 Mobile-ID users in Estonia. While adoption of the service was initially slow during the first few years since its launch, uptake of Mobile-ID has been increasing rapidly in recent months as consumers in Estonia are

increasingly demanding services which can be directly accessible via their mobile device. As a result, there has been an explosion in the number of businesses rushing to meet this demand by directing more and more of their services through the mobile channel. As witnessed in many other countries across the world, these changing consumer dynamics create a powerful marketplace in which mobile network operators can play a central role.

Policy makers around the world have come to Estonia hoping to learn from and replicate the open and decentralised digital infrastructure which is making the country a top target location for private investment. This case study aims to showcase the many benefits of Mobile-ID and the perspectives of both consumers and businesses across a range of sectors on the role that mobile operators can play in this increasingly digital landscape.



1 Estonian Information Systems Authority, August 2011.

2 <http://e-estonia.com/components/mobile-id>

Brief introduction to the operators:



EMT

EMT is Estonia's largest operator and the largest mobile network provider operating in the Baltics. The company was formed in 1991 as joint company between Estonian Eesti Telekom and TeliaSonera, a larger regional operator with subsidiary operators located in 16 countries across the continent and beyond, including Denmark, Norway, Russia, Spain, Sweden, Turkey, and Georgia. Today, the company hosts 875,000 mobile subscriptions in Estonia. (Q1, 2013, GSMA Wireless Intelligence)

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, Operator's own statistics).

"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 Eesti is a fully-owned subsidiary of the Finnish telecommunications and ICT service group Elisa Oyj, hosting approximately 566,000 mobile subscriptions in Estonia and serving 2.2 million customers in total (Q1, 2013, Operator's own statistics). Elisa prides itself on being the fastest growing operator in the Estonian market, with an expanding consumer base and revenues increasing by over 11.9% in 2012. 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".



Tele 2

Tele2 Estonia is a subsidiary of one of Europe's largest telecommunications operators, serving around 15 million customers in 10 countries and 510,000 mobile subscriptions in Estonia. It serves as a fixed-line telephone operator, cable and Digital television provider, mobile phone operator and Internet service provider. As Estonia's third largest mobile operator, Tele 2 sees the market as an opportunity for continued growth, particularly in smartphone revenues; in 2012, the company experienced 10% growth in sales (Q1 2012, operator's own statistics).

The company proudly states its ambitious goals of providing modern services to meet the widest possible range of customer needs, while continually adapting to meet the requirements of a rapidly changing telecommunications market. In 2012, Tele2 Estonia acquired Televõrgu AS, an optical fibre operator with a network reaching across Estonia, which it hopes will provide essential backbone infrastructure for the company's needs until 2025.

Tele2 operates in Austria, Croatia, Estonia, Germany, Kazakhstan, Latvia, Lithuania, the Netherlands, Norway and Sweden.

II Estonia: A Digital Society

A. Digital Agenda:

In the early '90s, as Estonia gained independence from the former Soviet Union, its leadership embarked on an ambitious agenda for administrative reform, aiming to build a tech savvy society that would be competitive on the world stage. The Tiger Leap Project of 1996 prioritized Information Technology infrastructure, bringing computers and ITC training into schools and businesses. As outlined in the Information Society Strategy 2006-2013,³ supporting the ICT uptake and use of eBusiness by enterprises has formed a major component to the national ICT infrastructure development plan.

Four principles were defined as the underlying foundation for e-Estonia:⁴

- 1. Decentralization.** Rather than housing a central database, every government department, ministry or business in Estonia can choose and develop its own system in its own time.
- 2. Interconnectivity.** Through a key tool named "X-Road", all the decentralized components of the system (including various databases and registers in both the public and private sector) are linked together and can operate in harmony regardless of what platform they use.
- 3. Open platform.** Any institution can use the public key infrastructure.
- 4. Open-ended process.** As a continuous project to keep growing and improving organically.

Underlying all of this, the eID is the nationally standardized system for verifying a person's identity in an online environment. Using a PKI infrastructure, it allows access to all secure e-services while maintaining the highest level of security and trust.

By 2007, Estonia made international headlines by becoming the first nation in history to successfully defend itself against a large-scale cyber attack,⁵ and Tallinn is now the home of NATO's Cyber Defense Centre.

With over 10 years of experience to offer, Estonia has provided a model to over 40 countries around the world in developing their own e-solutions. In February 2013, the UK Cabinet Office signed a memorandum of understanding with the Estonian Information System's Authority (RIA) for the two countries to exchange experiences in creating user-friendly governmental e-services,⁶ and last year RIA hosted a party of delegates from Brazil's National Congress to learn about e-government.

"We had heard about Estonian outstanding experience in e-governance and decided to get a more detailed look at it. Now, we are convinced that many of your e-governance projects like x-road and mobile services can be implemented not just in Estonia but also in much bigger Brazil. We are looking forward to the cooperation between our countries."- Paulo Pimenta, speaker of the budget committee of Brazil's National Congress, August 2012

Facts about e-Estonia:

- 78.4% of the Estonian population aged 16–74 uses the Internet and 75% of households have Internet access.
- Today 99.6% of banking transactions are done electronically.
- Over 80,000 digital signatures are made each day in the country. More than 100 million digital signatures have been made in Estonia since the system became available.
- In 2012, 94% of people declared their income electronically.
- 40% of Estonian ID-card owners have used them to authenticate themselves or provide a digital signature.
- It takes only 15 minutes to register a business electronically, using either an ID card or a Mobile ID. The company will be legalized within a few hours and can start conducting business the same day.

Source: e-estonia.com

B. ID-cards and digital signature

In 2001 the first nation-wide ID-card was introduced in Estonia. The ID-card is the primary identity document for Estonian citizens and is a mandatory ID document for residents, who make up approximately 15% of the population, from the age of 15. Valid for ten years, the card serves as an identification mechanism for use both in the real and digital world, and a travel document within the EU. Most importantly, the ID-card can also be used to affix a digital signature (legally equivalent to a handwritten signature) to digital documents and transactions using the national PKI infrastructure.



For more information on the Estonian ID-card and PKI infrastructure, please visit: www.ria.ee/id-card

³ <http://www.riso.ee/en/system/files/Estonian%20Information%20Society%20Strategy%202013.pdf>

⁴ e-Estonia website: <http://e-estonia.com/e-estonia/digital-society>

⁵ BBC news, "The cyber raiders hitting Estonia", Thursday 17 May, 2007.

⁶ <https://www.ria.ee/estonia-and-the-uk-sign-a-memorandum-of-understanding-on-cooperation-in-e-services/>

⁷ <https://www.ria.ee/facts-about-e-estonia/>
<https://e-estonia.com>
<https://www.ria.ee/facts-about-e-estonia>

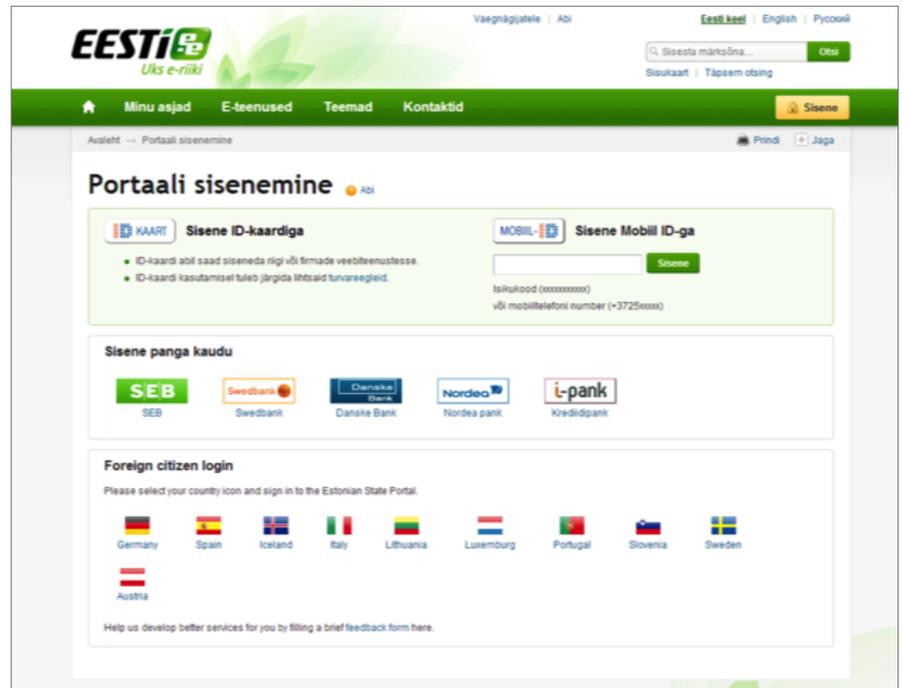
C. Baltic & International cooperation

Key elements of Estonia's economic strategy have been the creation of favourable conditions for FDI and openness to foreign trade. Estonia's balanced state budget, stable economic policy and relatively low labour costs make it an attractive location for foreign investors, the majority of which come from Nordic and Western European countries. Over 600 million euros came to Estonia in the form of foreign direct investment in 2011, according to Enterprise Estonia.⁸ The country ranks 21st out of all countries in the World Bank's Ease of Doing Business Index.⁹

Central to this attraction is Estonia's simple and transparent tax system, clear legal framework and relative ease with which a new business can be established, owing primarily to its advanced ICT infrastructure.

Since 2011, citizens of Belgium, Portugal, Lithuania and Finland can access state websites, sign contracts and conduct business online in Estonia using the national ID-card of their originating country, such as in the State Portal (above right).

Estonia and its neighbouring countries in the Baltic region, Latvia and Lithuania, have a long-standing history of close economic and political cooperation, and have most recently come together for joint cooperation on ICT services integration. For example, between 2006-2008 the Baltic WPKI Forum, consisting of mobile operators, banks and certification service providers across a number of Baltic States, was established with the objective of fostering mutual economic development through improved communication between the business community and government through the use of modern ICT technologies.



State Portal: one gateway to e-services

The State Portal, eesti.ee, is a gateway site enabling Estonian residents to access hundreds of e-services offered by various federal and local government institutions through one single entry-point. To enter the system, the user only needs to login once with their Mobile ID or another electronic ID, giving them federated access to all other sites housed in the portal. The site receives 72,000 visitors per month and is actively used by over half the Estonian population.

Whereas, earlier, an applicant would have had to visit a number of different offices to collect various documents proving their eligibility, now records from hospitals, the health insurance fund and other institutions are integrated via a platform known as X-Road, eliminating the applicant's need to visit them in person. In addition, the site offers a service which can be used via the portal to create, sign and share documents using digital signature.

e-Business Register:

Entrepreneurs are able to set up new businesses online in under half an hour by using the e-Business Register. All that is required is an ID card, card reader and Internet connection – or, more simply, a Mobile ID – and the data from completed online forms is then sent automatically to the Courts and Central Commercial Register.

By 2011 98.2% of all company submissions were made using this advanced, secure, and simple method. Through the State portal it is also possible to submit and view annual reports, submit and verify a business name, change data in the business register in real-time and make detailed inquiries into other companies. Due to cross-border digital signatures, Portuguese, Finnish, Belgian and Lithuanian citizens can set up companies in Estonia, and vice versa, using their national ID cards or Mobile ID.

⁸ EnterpriseEstonia.com, February 2012

⁹ World Bank Ease of Doing Business Index, 2012

Source: e-estonia.com

1994	Information Policy passed	2003	e-Vehicle registry opens Public Information Act Launch of ID bus ticket State Portal launched
1996	Tiger Leap project created Personal Data Protection Act First internet bank in Estonia	2005	First i-Elections e-Police system comes on line
1999	Data Protection Department created	2007	First Mobile-ID system comes on line
2000	Digital Signatures Act e-Tax filing begins Mobile parking introduced e-Cabinet introduced Population Registry Law passed	2008	Launch of e-Health system
2001	Introduction of X-Road Population Registry opens	2010	e-Prescription introduced
2002	e-School project comes on line ID Card introduced Law on e-Election passed	2011	Smart Grid introduced in Energy Sector First m-Voting in national Parliamentary elections

Mobile ID use cases

With a Mobile ID, users in Estonia can:

- Submit tax returns (income tax, local council tax, business & property taxes) online with the national Tax and Customs Board
- Register a motor vehicle with the Road Administration
- Apply for a driver's license (and obtain and submit the required health certificate through the same portal)
- Register a new company
- File court cases, access and monitor legal proceedings in civil, administrative, criminal and misdemeanor proceedings with the Centre of Registers and Information Systems
- Access and process real estate data and documents
- Buy tickets online for railway travel, sports events, museums, zoo, recreational fishing rights, etc.
- Apply for and monitor personal and corporate pensions
- Apply for a personal loan
- Access student account, grades, class info at Tallinn University
- Purchase and manage accounts for home, motor, accident, travel and pet insurance
- Pay water, electricity and gas bills, monitor consumption and change contract information with utility companies
- State agencies (hospitals, schools, defence agencies, sports clubs, etc.) can procure hospital beds, building installations, minivan hire, etc., with the Ministry of Finance
- Sign and share documents using DigiDoc, an online portal for storing, sharing and signing documents, photos, voice recordings or even an instant messaging chats.
- Access personal information (health insurance, disability assistance, school support benefits, educational qualifications, construction applications, public event applications, etc, etc.) from the State Agency for Information System
- Vote in national elections

Source: e-Estonia.com

III Estonian Mobile-ID

A. Vision & principle:

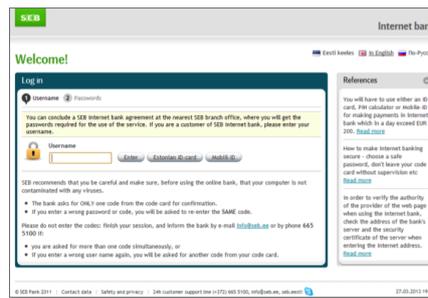
Mobile-ID is a service that allows the subscriber to use their mobile phone as a form of secure electronic ID. Introduced by the mobile operator EMT as the commercially available technical evolution of the National ID-card, Mobile-ID was intended to make the everyday transactions that people conduct easy and fluid. Like the National ID-card, Mobile-ID can be used for accessing secure e-services, transmitting and authorising payments, and digitally signing documents. The agreement can be made for both private and corporate clients using their mobile numbers.

Unlike other mechanisms of authentication, Mobile-ID does not require any additional hardware, such as a card reader, and frees the user from password cards, PIN calculator, usernames and passwords. Moreover it works on any handset so the user does not have to have a smart phone.

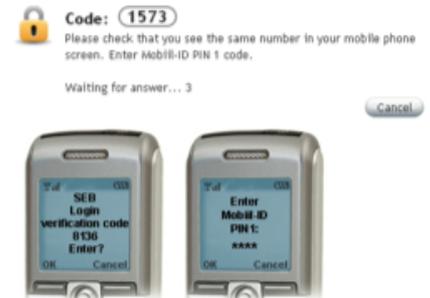
The PKI technology used in Mobile-ID offers the highest level of security for transactions involving payment or secure data transfer.

B. How it works:

Here's how ID-card would be used for logging into a secure site, for instance the SEB Bank account:



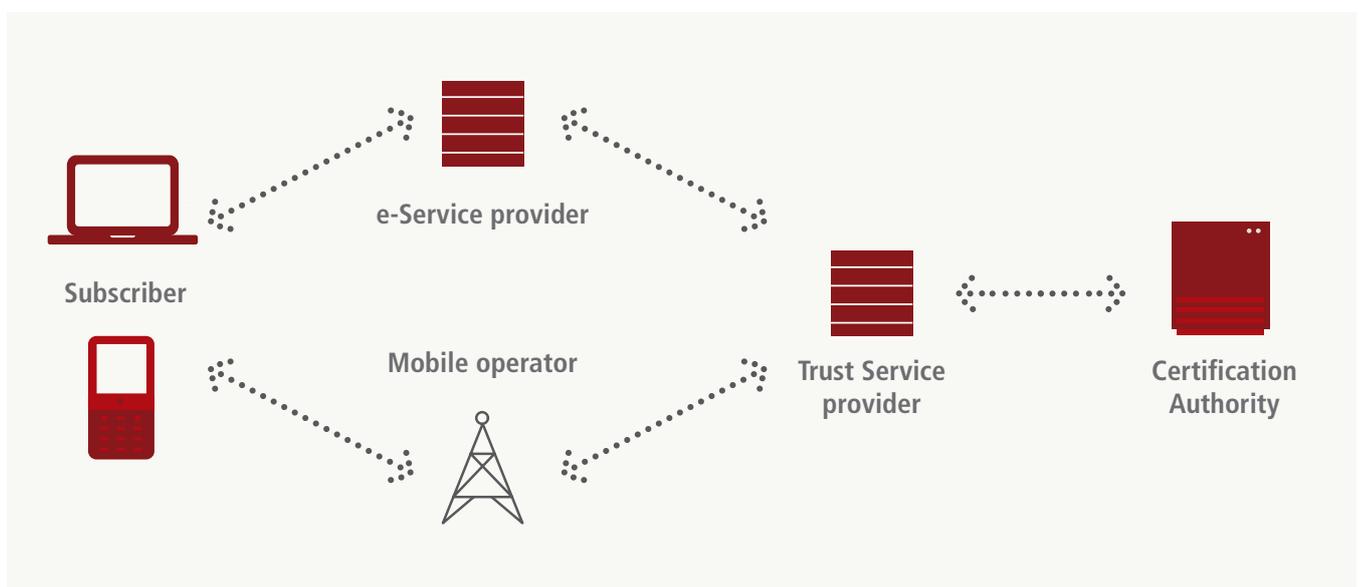
1. The user clicks the "Log in with Mobile-ID" option on a supported website and enters their user ID. When using it for the first time, the user also enters their mobile number.
2. The user then receives a pop-up message on their mobile phone, which prompts them to enter PIN 1 of their Mobile-ID (a 4 digit PIN known only to the user).
3. The user enters the correct PIN onto their phone. The screen on the phone disappears and the website is automatically reloaded with a logged in screen.



(No other steps are required for access authentication)

4. For confirmation of transactions (or signature of contracts, voting, permission authorisation, etc.), the site asks the user if they would like to digitally sign the information.
5. If the user clicks 'yes', a window from a third-party Certificate Center pops up, asking for the PIN codes connected to the user's electronic ID-card.
6. The Certificate Center verifies the codes and sends a confirmation back to the website the user must enter PIN 2 of their Mobile-ID (a 5 digit PIN) when prompted.

When using an ID-card, the process is similar, except that an additional card reader is required to link the PIN code to the card.



C. Technical solution:

The system is based on a specialized Mobile-ID compliant SIM card which the customer must request from the mobile phone operator.

Private keys are stored on the mobile SIM card along with a small application for authentication and signing.

The Mobile-ID compliant SIM card contains both PIN and PUK security codes.

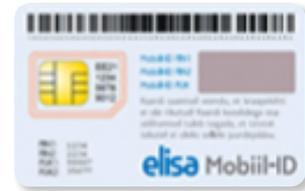
The Mobile-ID codes needed for the service are:

- Cell-ID PIN1 - or 4-digit code for identification purposes
- Cell-ID PIN2 - at least 5-digit code for the digital signature
- Cell-ID PUK - code Cell-ID PIN codes to open if they are locked

Certificates are issued for a validity period of 3 years, after which the contract must be awarded to a new SIM card.

The ID-card service must be activated after subscribing to the service. This can be done at the web page of the Police and Boarder Guard <https://www.politsei.ee/> using the ID-card, ID-card's PIN 1 code and ID-card reader device.

To date, no known reports of falsified or repudiated transactions have been attempted with Mobile-ID during its 5 years of operation.



Mobile ID: A Developer's Perspective

Madis Aasla is a self-employed software developer who has provisioned Mobile ID to over 15 private companies. He speaks about his experience as both a software provisioning expert and personal user of Mobile ID.

"I've developed internal networks for companies that basically want to have a secure way of identifying their employees which doesn't involve regular username-password combinations. It's becoming a bigger issue in Estonia, and companies are beginning to recognise that they need to have better security measures.

"There isn't a specific "type" of company that chooses to use Mobile ID. Some companies decide to go straight to Mobile ID, so it's not true to say that the majority are those making a transition from the ID card. Sure, the Mobile ID isn't that common yet, but I'm seeing more and more companies interested.

"As a developer, I think Mobile ID is really easy to implement. It's well documented, so implementation doesn't take a lot of time and effort. I think a lot of businesses are hesitant because they think it must be expensive, but in business terms it doesn't cost much. I've seen a lot of different solutions and Mobile ID is really cheap, even if you're a small company.

"I think the biggest value that companies see in Mobile ID is that the digital signature has legal value - you can reduce all the paper pushing that takes for ever! When you think about this, the private sector could easily do anything with the Mobile ID. For example you can do a full credit check and automatically apply online for a credit card, have it signed and validated in 5 minutes, with no paperwork whatsoever. You can even sell a car without going to the DMV - how cool is that?

"Having been accustomed to digital documents for over a decade, we in Estonia are pretty calm about it, we know it works. What was life like before we went digital? It was all hell..."

IV Uptake and Scale

Despite its introduction to the market nearly 7 years ago, Mobile-ID has only recently started to see strong levels of growth. For example, year on year growth rates for Mobile ID users in banking applications was 56% in 2012.

There are a number of explanations for this which provide useful insights for those looking to implement similar services in their own markets.

A. Rapidly changing consumer demand:

- i. Smartphone penetration is rising quickly in Estonia. While still at around 30%, the introduction of smartphones is significant. As people switch to smartphones, their consumption of data and data-based services (both via apps or the mobile web-browser) increases. As a consequence, smartphone users expect to be able to access the same services – and, arguably, even more services (since they can browse from anywhere at any time over a wifi or GSM connection) - than they would from a PC.

“I actually do most of my banking these days over mobile, like when I’m lying in bed or waiting for someone, I can pay my bills and everything.”

– Mobile-ID user

“I basically use it every day. I use it whenever I’m not at the office. I don’t even carry my identity card around with me because it’s in my phone.”

– Mobile-ID user

- ii. Similarly, the introduction of tablet devices into the Estonian market has meant that using the physical ID-card for authentication and signature processes has in fact become more inconvenient to the user. Most tablets do not have a USB port for a card reader, for example, while the perceived impediment to being “mobile” in terms of using the device on-the-go increases once the user has to focus back and forth between two items: holding the ID-card in one hand while manually entering information into the device in the other.

“One way you could judge the usefulness of a technology like this is by asking yourself: Does it pass the ‘traffic light test’? Can I send money to my friend or pay a bill while waiting at the traffic lights? With Mobile-ID, I definitely can.”

– Mobile-ID user

B. Businesses increasingly turning to mobile

- i. Consumer-facing businesses are increasingly recognising the importance of the mobile channel for reaching and serving their customer-base and, as a consequence, are looking to offer an greater amount of services and content via mobile. Fundamental within this is the recognition that consumers want one single, fluid process from entry to content exploration to payment.

“Mobile-ID has reduced our customer acquisition cost because the dropout rate at the point of payment is lower. If you note that the average attention span is 3 seconds, you need to ensure that you don’t lose the customer at this crucial stage.”

– IsePankur, peer-to-peer lending

- ii. The past few months have seen an increase in the number of apps which have integrated Mobile-ID into their service. The two largest banks in Estonia, Swedbank and SEB, both added Mobile-ID as a login and authentication option for transactions: banking customers using the apps are now able to view their account balances, issue a payment or transfer money to a third party all in the same interface and entering their secure 4-digit pin once (for authorising payments, the customer also needs to enter the 5-digit signing pin). Comparatively, authenticating a transaction using Mobile-ID through the PC is also possible, but would require the user to additionally manually enter their phone number in addition to the authentication PIN.



Typical physical ID-card reader + USB attachment cord.
Not available for all tablets.

DigiDoc:

DigiDoc is an online service that allows Estonians to store, share and digitally sign documents. Users may log in using their physical ID-card + reader or with Mobile-ID, and any type of file can be uploaded, including voice recordings by phone. As digital signatures carry the same legal weight as paper signatures and the robust public key encryption meets EU standards for security, DigiDoc is not only popular with private citizens, but

is also commonly used in the public sector (e.g. for court documents and municipal contracts) and banking. This system was introduced in 2005, and particularly focused on improving communication between organisations as a means to fulfil the potential of digital signature. Other benefits include the fact that the process is cheaper, faster and kinder to the environment than using paper; the system is also easy to use and entirely free.

iii. One of the more common use cases of Mobile-ID adopted by businesses is for secure enterprise access for their employees. As the number of employees wishing to use their personal laptops, tablets and mobile devices for work increase, businesses are forced to adapt and develop policies and processes that meet the security requirements for accessing their corporate VPN and internal data systems – part of a broader phenomenon occurring around the world known as BYOD (Bring Your Own Device). In 2012, 89% of enterprises used employee's physical ID-cards attached to readers for digital signatures and 67% used ID-

cards for establishing users in internal information systems.¹⁰ For many, using Mobile-ID is a much simplified method for conducting the same processes at a faster speed and with greater flexibility for their employees.

According to the 2008 Estonian Labour Force Survey, over 10% of Estonians work from home, or spend the majority of their time out of the office, making a Mobile-ID solution perfect for this need.

“When we use Mobile-ID we can save time and a whole lot of footwork in terms of paper processes – otherwise it takes a few days at least to register someone.”

– Enterprise user, Mobile-ID

iv. In addition to the potential increase in revenue generation, businesses are also recognising the significant role that mobile also plays in terms of cost reduction. Paper processes, including printing and courier services, cost businesses up to hundreds of thousands of dollars per year in both financial cost and time. Many corporate entities, as well as government departments, have already made the transition to paperless.

Mobile ID: Changing the face of the financial services industry – A Client Perspective

Established in 2008 and operated by SõbraLaen OÜ, isePankur is the oldest operational peer-to-peer lending platform in Scandinavia allowing individuals and businesses to borrow and lend between each other. With customers in 28 countries and investors from Europe, Australia and the United States, isePankur aims to establish an open pan-European peer-to-peer credit and payments platform connecting people and companies with excess capital in stable economies with growing credit-thirsty markets in Central and Eastern Europe.

In 2011, isePankur won the “Best Estonian E-service of 2011” and was a quarter-finalist at the World Summit Awards of 2011. With a net income of 118,804 euro on sales of 208,664 euro in 2011, the company is one of the few profitable peer-to-peer lending start-ups in the world.

Pärtel Tomberg, CEO of isePankur, describes the reasoning behind his company's decision to adopt Mobile ID:

“As a financial services provider, security and safety are a core part of our services; our investors rely on us to manage their money effectively. It is therefore vital for us to be sure that the recipient is the right person. Mobile ID is currently one of the various mechanisms by which a person who comes to us for a loan can identify themselves. Around 30% of our customers are using Mobile ID, but I wish it was all of them!

“Our prime commodity as a financial services provider is the quality of our service. This is ultimately what makes the customer go through with the transaction. Mobile ID has reduced our customer acquisition costs because the dropout rate is lower. If you note that the average attention span is 3 seconds, you need to ensure that you don't lose the customer at this crucial stage.

“For the customer, it's ultimately about convenience. Consumers don't worry about security. They assume the process secure because you're offering it to them. Therefore, we need to make sure it's secure! Mobile ID definitely meets this requirement.

“However, we don't look at mobile as a completely different sales channel, it's part of our whole service offering to the customer. If you think about it, financial services are all about data services. It's not technology driven; it's process driven. A consumer is a consumer in every industry; regardless of which shop they're standing in or website they're on, they behave the same and they want the same processes [for payment, accessing information and content, etc.] across all the things they do.

“Identification and authentication are also a central part of our internal processes, such as internal payment transfers, for which we already use 2-factor authentication. For every legal transaction the customer does, everything needs to be signed and authenticated. Operators could be capitalising on this need by providing these types of strong authentication services.

“I think the telcos should move a bit faster. From a business standpoint, if we want to grow our business in multiple countries, we can't build our entire infrastructure on Mobile ID as the service process needs to be as similar as possible in every place. The problem in Estonia is that they [the operators] concentrate on making the solution too technical, whereas they could be launching authentication services to other service providers who need them right now. You don't need to have a complex technology to provide a service. The device is there. The demand is there. MNOs have the assets now so should offer them before start-ups come and develop something else in their place. Until the time when Mobile ID is offered in multiple countries, we'll need to use a One-Time-Password mechanism as an alternative.”

The mobile operator Elisa, for example, is among a number of companies now charging its customers for paper bills in an effort to encourage use of digital resources and as part of its commitment to carbon reduction. The Estonian Parliament has gone as far as to make all votes in the cabinet paperless: decisions are now voted on with a click of a button and the results made available to the public the same day.

C. Early adoption and promotion by Banks

While ease of use and convenience is at the heart of growing adoption of Mobile-ID by consumers, this represents only one side of the equation. For companies and organisations for whom the security of their customer's information is of utmost importance, Mobile-ID has become a crucial mechanism for ensuring that this level of security is met.

- i. Banks in Estonia were among the first entities to adopt Mobile-ID, and have continued to be some of the product's most active proponents. Today, 99.6% of banking transactions in Estonia are done electronically and, according to the national e-Estonia portal, the number of Internet banking users – including corporate accounts and users with multiple bank accounts - is greater than 1.8 million clients (greater than the whole population of Estonia, 1.3 million).

“Customer penetration is a key point from which we look at Mobile-ID: how to make it easier to attain the customer, to make it easier to login and use our services.”

– Manager, Swedbank

Banks in Estonia allow a variety of ways for clients to access their online banking services, including plastic code cards (cards listing a series of series of codes to be used once each during the login process, after which the code is scratched off) and hardware tokens (one-time-

password generators), as well as the ID-card and Mobile-ID. Unlike the phenomenon seen in other countries where banks have resisted uptake of Mobile-ID solutions for fear of undermining their pre-existing bank-issued authentication methods, the Estonian banks recognised the value of the PKI infrastructure method within the ID-card and Mobile-ID as a more secure method for authenticating transactions. Swedbank and SEB Bank, for example, have now set a limit on the daily transaction amounts authorised using methods other than the ID-card or Mobile-ID to 200 euros in an attempt to phase out these less secure methods and encourage use of Mobile-ID and ID-cards.

“We once thought the [plastic] ID-card would eventually be the default authentication method for payment transactions, but now demand for smartphones and tablets has changed our view. Mobile-ID is the only form which is both secure enough and convenient enough for our clients.”

– Manager, Swedbank

- ii. Banks arguably were the catalyst for creating a broader infrastructure for the identification of a person within an electronic environment. As commonly seen in other markets where mobile identity products have been introduced, a crucial driver for successful uptake by consumers is the frequency of use. Banks are therefore key players in this space due to the frequency with which clients view or conduct transactions on their accounts (most commonly on a daily or weekly basis, as compared to an annual tax income claim). Once banks in Estonia began to use digital identification and authentication methods on a regular basis, other entities followed suit.

Swedbank: A banks perspective

Swedbank is Estonia's largest bank, holding around two thirds of the market share in terms of customer transactions. Around 900,000 customers in the client-base use electronic banking, of which around 0.5 million customers are considered active on a monthly basis.

Arno Pae, Head of the E-Channels Department at Swedbank in Estonia, describes the strategic rationale behind the decision to encourage Swedbank customers to use Mobile ID.

"Customer penetration is a key point from which we look at Mobile ID: we want to focus on how to make it easier to attain the customer, to make it easier to login and use our services. One area where we see the greatest value in the future is mobile banking, which is a strategic focus area and a strong reason for us to support the take-off of Mobile ID.

"We saw the monthly uptake of new Mobile ID users more than double as soon as we launched the Mobile ID feature on our mobile banking app (in May 2011).^{*} Consequently, our mobile banking app usage has grown 200 times as a year-on-year figure.^{*} These two things clearly support each other in a virtuous circle. Although it's a relatively new service for our customers, the numbers are pretty clear:

- 2.5% of our Internet banking customers use Mobile ID and make up 2.5% of all logins
- 26% of mobile banking customers use Mobile ID and make up 38% of logins^{*}

"I think the reason for this rapid uptake of Mobile ID is clearly the increased usability of the service. It's an easier way to get into the app and conduct transactions. It suddenly becomes an all-in-one process: the user only needs to

remember the universal access code they use across all online services and the pin is generated on the spot.

"Other banks have similar user-base numbers (around 2%) but we know they are also actively welcoming Mobile ID. Unfortunately for banks, the default authentication method for the majority of online banking is still the code card, but we don't see this as extremely good security. In fact, we've tried to actively discourage use of the code card by setting an amount limit on transactions that can be made with it.

"We're glad to see that the operators and national government are now making efforts to advertise Mobile ID. EMT have been kind enough and smart enough to use banking as one of the main use cases for Mobile ID. We also try to actively promote Mobile ID use among our customers by encouraging them to tell others about it. We've had great feedback from our Mobile ID customers so far. They have been very happy.

"This leads me to the most important point value that Mobile ID represents, which is the ability to build all sorts of additional services based on the authentication feature. We've taken the view that mobile payment is about much more than just the payment; it's a channel for innovations in m-wallets and m-apps. For example, we use it in our call centre: Clients can now opt to "log in" to the call centre before they are connected. An interactive voice recognition prompts them for login details and, once the real call starts, the client is already authenticated. When you think about the possibilities here, they seem endless."

^{*}Source: All statistics have been provided by Swedbank for the purposes of this study.

D. Public Sector recognition and promotion

- i. Mobile devices are being increasingly recognised by governments around the world as an important channel for enhancing reach and access to public services for their citizens. As mobiles become increasingly ubiquitous, a number of countries are adopting mobile strategies for facilitating citizen access to healthcare systems, transportation, border control and local government. In Estonia, a number of public sector entities are placing mobile at the heart of their citizen engagement strategies.
- ii. While the public sector has avidly promoted the use of ID-cards for access to public services and digital signature, Mobile-ID has only recently been placed at the forefront of Estonia's e-Society agenda.

The primary reason for this is that, up until relatively recently, Mobile-ID had been offered only a single operator (EMT), meaning that official promotion of the service had to be limited in the interest of neutrality. Once Mobile-ID became commercially available from all three operators in 2009, public sector entities were able to openly advocate the adoption of Mobile-ID in their processes.

One such entity is RIA (Estonian Information Systems Authority), the entity responsible for developing and administering Estonia's PKI and digital signature infrastructure. RIA has recently undertaken an advertising campaign through local media outlets and in shopping malls around the country to encourage the use of Mobile-ID among Estonian

citizens. Likewise, EMT has also run a number of advertising campaigns on local television channels, newsprint and online media in order to promote Mobile-ID among citizens.

"Mobile-ID is the next generation means of authentication. It's much easier to implement because it doesn't need any extra infrastructure to be set up (such as card readers) and it's much easier for people to use."

– Mihkel Tikk, Head of the State Portal Department, Estonian Information System's Authority

"The telcos have seen the customers, they know the customers, they've already registered them, they know who they are, where they live, how they transact, so why would we need to go through this registration process again?"

– Online financial services provider

Mobile-ID: Health Records

The Electronic Health Record is a nationwide system that integrates data from Estonia's different healthcare providers to create a common record for each patient presented in a standard format. By logging into the Patient Portal with Mobile-ID, the patient can review their past doctor visits and current prescriptions, control which doctors have access to their files, and even receive general health advice. Within a few minutes, patients can renew a prescription by calling their doctor directly from home; the doctor then writes the prescription and forwards it to the national database using their Mobile-ID. In emergency situations, doctors can use the system to read time-critical information, such as blood group, allergies, recent treatments, ongoing medication or pregnancy.

Since launching the system, the state has recorded an enormous reduction in paperwork in hospitals and pharmacies, while the Ministry of Health is able to measure health trends, track epidemics and make sure that its health resources are being spent wisely using the data compiled for national statistics.

Nutitefoniga saad rohkem kui lihtsalt rääkida

Mobiili-ID kasutamine on lihtne

Mobiil-ID-ga saad ID-kaarti ja kaardilugejat kasutamata mugavalt siseneda e-keskkonda, teha makseid ja sõlmida tehinguid ning anda digitaalalkirja. Võta vaid oma nutitelefoni ning asjad saavad aetud kiirelt ja turvaliselt.

[Uuri järgi >](#)

EMT Live - parimad üritused Sinu mobiilis

Nüüd on võimalus Sul otse enda mobiilist vaadata parimate kultuuri- ja spordiürituste kavasad, koostada enda kava, lisada üritustele meeldetuletusi ja osta pileteid.

[Uuri järgi >](#)

Parkimise äpp teab tsoone sinu eest

Uuenenud parki.ee äpp teeb parkimise veelgi mugavamaks – tuvastab lähimad parkimissoonid, annab nende kohta detailset infot, teavitab aktiivset parkimisest ja limiidi täitumisest jpm.

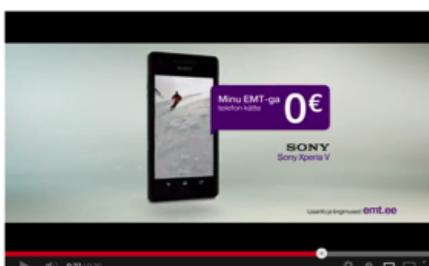
[Uuri järgi >](#)



“With Mobile-ID, you can comfortably and easily enter e-environments, make payments and conduct transactions, and provide a digital signature. Your smartphone can take care of things quickly and safely.”

EMT online campaign

https://www.emt.ee/ul/minuemt_jaanuar/



EMT Mobile-ID awareness campaign, Youtube

<http://www.youtube.com/watch?v=WzWgc1D4Tw>

Convenience at the heart of citizen access: A Government Perspective

RIA is the Estonian Information Systems Authority, the entity responsible for developing and administering Estonia's PKI and digital signature infrastructure. RIA is in the process of developing a mobile version of the State Information Portal (eesti.ee), which is an umbrella portal for accessing state e-services from information drawn from various separate databases.

Mihkel Tikk, Head of the State Portal Department, discusses RIA's vision for Mobile ID:

"We want to make the portal into one single point of contact for citizens. Here in Estonia, we view the State's role as being to make it possible for the citizen to do what he or she wants to do, and to make it more convenient. That's why e-governance started in Estonia, because we saw people going online more and more for banking and shopping, so we thought we should do it ourselves.

"Our e-Success is very much supported by the private sector. People are much more likely to trust a bank or someone who's offering them a service they're paying for because they're being treated well. You need to include the private sector if you want to build trust in the eyes of citizens. Right now, we have the technical means to do this, so we're ahead of other countries.

"Fundamental to RIA's efforts is recognition of the enhanced security of the PKI infrastructure which Mobile ID brings to the process. For example, RIA is considering ways to phase out or discourage use of login methods other than the ID card

or Mobile ID (see separate box). The organisation has recently undertaken an advertising campaign in shopping malls around Estonia's major towns to encourage use of Mobile ID among Estonian citizens. In RIA's view, the promotion of Mobile ID is simply an extension of the digital signature infrastructure already in place and in use by the majority of Estonia's citizens.

"Much still needs to be done to promote awareness among citizens of the benefits of digital access, even with the ID card. We have 2.1 million logins to the state portal each month, and 3% of those logins last year were using Mobile-ID. Half of the Estonian population has been to the portal, which means that we need to reach that other half of the population who have yet to try it.

"Part of the problem is that people take a long time to adapt to new technology. It took the older generations a few years to start confidently using the physical ID-card for digital purposes. Because the ID-card was relatively complicated – in terms of needing a card reader and using a PC, people assume that the Mobile-ID is going to be even more complex. But in fact it's the simplest way of all.

"We are also conducting awareness programmes through local media channels and in schools, teaching children how to securely browse data. We want to encourage people to talk to their kids about internet safety. Raising this kind of awareness takes years. If you talk to them now, they'll be the ones acting securely online in the future."

E. Clarifying legislation

With the onset of the February 2011 parliamentary elections drawing near, there was a push to recognise Mobile-ID as an official proof of identity. Prior to this time, Mobile-ID was recognised as an identification medium that met technical security requirements, but which could only be used outside the public sector. There were two main obstacles to official recognition:

- a. The Identity Documents Act 2000 made no reference to Mobile-ID. In January 2011, the wording was adjusted to include Mobile-ID as an official identity document equivalent to the national ID-card.

- b. Mobile-IDs were, up until this point, issued outside of the state's jurisdiction. The Police and Border Guard were responsible for establishing the identity of users, but the Mobile-ID compliant SIM cards were issued by mobile operators. In order to prevent users needing to make multiple trips to both the operator and the Police and Border Guard office to activate the Mobile-ID (a challenge which all recognised would significantly limit uptake), a solution was established in which the Mobile-ID certificates could be activated directly by the user on the Police and Border Guard office website by using their ID-card.

F. Wider availability of Mobile-ID

Until 2009, only one mobile operator, EMT, offered Mobile-ID to its subscribers. The service was later opened up to other Mobile operators, Elisa and Tele 2, who started offering and promoting Mobile-ID to their subscribers. Since opening the service to other operators, adoption rates have increased rapidly. The majority of Mobile-ID users (approx. 80%) are still those of EMT. Since 2012, EMT has offered Mobile-ID to its clients for free and has actively promoted the service through advertising campaigns and public communications.

V Challenges

Despite increasing uptake of Mobile-ID across many sectors, some challenges still remain to the wide-scale adoption of the product:

A. Awareness

“Once you see it, it’s magic. But you don’t really understand it until you have it.”

– Mobile-ID user

- i. A key obstacle to customer uptake is lack of awareness about Mobile-ID. While much effort can be made toward explaining how the service works, the real switch comes when the user is able to “see it with their own eyes” and to use it on a daily basis. Part of the challenge lies in the need for repeated use of the service before fully recognising and understanding its benefit.
- ii. One issue iterated by many different service providers interviewed for this case study is the perceived complexity of Mobile-ID when compared to existing digital or “traditional” paper-based processes. As self-service technologies, both the ID-card and Mobile-ID are inherently more convenient, but also require responsibility on the part of the user to ensure that the equipment is in good condition and up to date. Because the ID-card requires additional hardware to work (including an electronic card reader compatible with the PC/tablet, a driver for software installation, and physical upgrade of the plastic card itself – sometimes within less than one year, depending on the frequency with which the card is used), perception among users is that the Mobile-ID will entail similar maintenance. Significant effort needs to be placed into dispelling these myths.

- iii. Additional distortions of current perceptions regarding Mobile-ID originate from political groups who are concerned that the digital agenda of the current government excludes their traditional voter-base. Negative ad campaigns during the 2011 elections (during which the law recognising Mobile-ID as an equivalent digital signature to the ID-card was signed to allow for voting via Mobile-ID), tried to paint both voting via ID-card and Mobile-ID as lacking in the sufficient levels of security required. Such groups worried that digital voting would unfairly skew the outcome with greater voter turnout for those parties who represented more digitally savvy segments of the population (in the 2011 elections, the e-voter turnout was 20:80 for Leftist versus Centre party voters). These groups continue to portray Mobile-ID as easily “hackable” and open to security breaches, despite the fact that the Mobile-ID has never been hacked during its 5 years of commercial availability.

- iv. Anecdotally, older clients are considered less likely to want to use the “self-service” processes available through the PKI digital infrastructure, and tend to be less tech-savvy than those of younger generations. However, this is not the case when looking at the data on current Mobile-ID users:

- The age-range of Mobile-ID users is between 18-75 years, with the majority of users aged between 26-48 years
- Male-female ratio is approximately 61:49

Those wishing to implement similar services in other countries need to be cognizant of the fact that a small portion of citizens will always prefer to go in person or speak directly to a service provider rather than conduct their business online.

Mobile-ID: revolutionising the voting process

Estonian citizens can vote in local and parliamentary elections using Mobile ID or through any internet-connected computer, anywhere in the world. This remote voting system is simple, elegant and secure, and avoids the problems of electronic voting systems used elsewhere which are costly and problematic. Estonia is a true trailblazer in this field; it was the first nation to hold legally binding elections over the Internet (utilising an ID card and card reader) in a local election pilot in 2005, the first nation to allow i-Voting for parliamentary elections in 2007, and again in 2011 pioneered voting through mobile phones, removing the necessity of a card reader. Whilst it is too early to speak of m-Voting (as an Internet connection is still required), i-Voting has become remarkably popular and 24.3% of participating votes in 2011 were i-Votes.

B. Cost

- i. Similar to misconceptions on the perceived complexity of Mobile-ID is a misrepresentation of the costs involved in subscribing to the service. The Mobile-ID costs 10 euros to the consumer to purchase the Mobile-ID-compliant SIM card and the certificates, and an additional subscription fee of between 65c and 1 euro is added to the customer's mobile bill each month. While this may appear minimal to some, for those subscribers paying only 5 euros a month subscription for basic voice and text, this is a significant additional cost.
- ii. Nevertheless, the research for this case study showed that perceptions on cost are always multifaceted and depend on the user's perceptions of the alternatives. When compared with upgrading a lost or worn ID-card, for example, which costs around 30 euros to replace (in addition to the original cost of the card + card reader + software), the difference in cost between this and a one-time Mobile-ID installation plus subscription fee is significant.

"65cents to me is nothing. I don't even notice it and I use Mobile-ID all the time, so I think it's great value"
 – Mobile-ID user

C. Business model

Complicating the cost perception further is the fact that the Estonian operators compete on the cost of offering Mobile-ID to their subscribers. In some cases, Mobile-ID is offered for free as part of an incentivising scheme; in others, the operator subsidises the cost of the tax to the government for issuing identification certificates. While these incentives have significantly increased the number of users, others argue that this distorts the perception of a fair price and makes it more difficult to ensure sustainability of the service in the long run. Since 2012, EMT has offered Mobile-ID to its clients for free, which has encouraged greater uptake of the service. According to EMT, many users felt that the state fee charged for the certificates was too high for an average user.

For the operators, Mobile-ID is not a major revenue driver, but is viewed as a vehicle for more innovation of services on the Mobil ID.



VI Mobile-ID: A vision towards the future

Within a short period of time, mobile identity has become an issue of considerable importance within the wider digital economy. Although the majority of activities that require digital identity validation and authentication around the world continue to take place online, changing consumer trends suggest that the mobile channel will be used increasingly in this space. As a result, mobile operators have a key role to play within this space. As this case study aims to show, Mobile Operators can successfully insert themselves into the centre of the digital economy and become the trusted source of security and convenience for consumers and businesses alike.

Despite the challenges, the future looks good for Mobile-ID in Estonia. Changing demand for services on-the-go means Mobile-ID is increasingly recognised as the medium of choice for consumers and businesses. Commitment from the Operators and from SK to dedicate more attention to raising awareness of Mobile-ID and its benefits points to the strong likelihood of further adoption throughout Estonia. As consumer-facing organisations start to recognise the opportunity in offering Mobile-ID to their customers, penetration is likely to grow.





Mobile Identity

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