Personal Data

Swisscom Mobile ID:

Enabling an Ecosystem for Secure Mobile Authentication

The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators with more than 230 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers and Internet companies, as well as organisations in industry sectors such as financial services, healthcare, media, transport and utilities. The GSMA also produces industry-leading events such as the Mobile World Congress and Mobile Asia Expo.

For more information, please visit the GSMA corporate website at www.gsma.com

or Mobile World Live, the online portal for the mobile communications industry,
at www.mobileworldlive.com

Author: Alix Murphy

With special thanks to:

Adrian Humbel, Swisscom
HP Waldegger, Swisscom
& the Swisscom Mobile ID Team

Daniel Gasche, PostFinance Bank
Claudio Lombardi, PostFinance Bank
Martin Moser, PostFinance Bank
Joachim Vetter, Abacus

Contents

Introduction

In early 2013, Switzerland's leading operator, Swisscom, introduced Mobile ID, a fully managed strong authentication solution and a complete service package for enterprise and business, as well as individual users. Using a PKI- based, "mobile signature" secure encryption technology on the SIM card, Mobile ID has been recognised highly within the security community for combining smartcard level security with a sophisticated ease of use for customers wanting to transact across a wide range of industries, including online and mobile banking, insurance, pensions and HR processes, secure enterprise access, as well as government and public services (such as tax, social security, housing, healthcare).

Within only a few months since launch, Mobile ID has now reached a user-base of 25,000, with steadily increasing adoption rates of around 10% each month. Much of this success may be attributed to simplified processes for customers in obtaining and using the authentication solution. However, a large degree of the success is due to Swisscom's determination to develop a broader ecosystem of partners and relying parties to ensure a strong market for the uptake of Mobile ID.

Swisscom's unique approach to the positioning of Mobile ID within Switzerland's high security-conscious business community provides important lessons for the telecoms industry as it adopts and explores new trusted roles within the evolving digital economy. Equally, Swisscom's success in gaining rapid traction among users and business customers reveals key insights into the effective operationalisation and deployment of a managed secure authentication service as part of its core product offering.

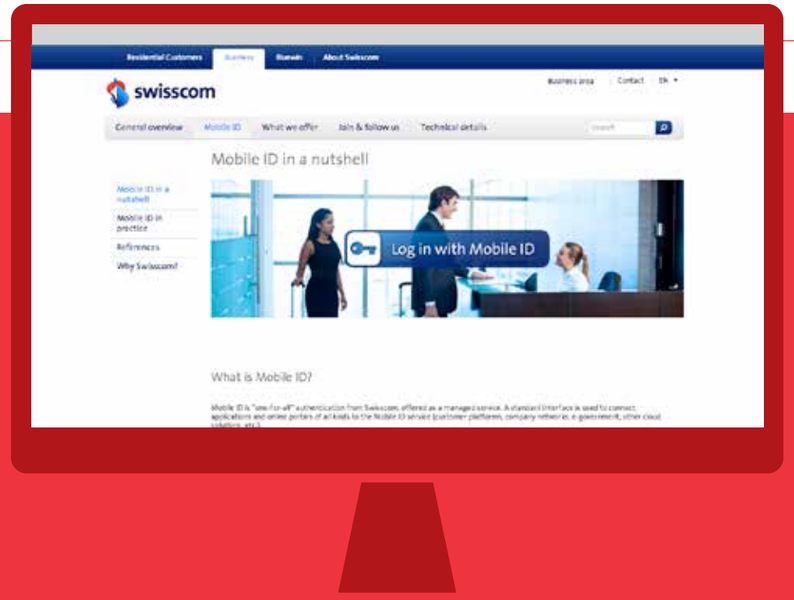
This case study follows the story of Mobile ID and explores the key "success factors" that allowed Swisscom to further solidify its position as a trusted brand among customers and partners. Beginning with the operator's pioneering strategy and rationale for a new identity product, the study explores the deliberate decisions taken by the Swisscom product team to ensure smooth integration, deployment and delivery of a product that has maintained a persistent level of uptake and satisfaction among users to date.

In December and January 2013-14, the GSMA's Personal Data team met with Swisscom to collect and expose these insights out to the broader mobile operator community.

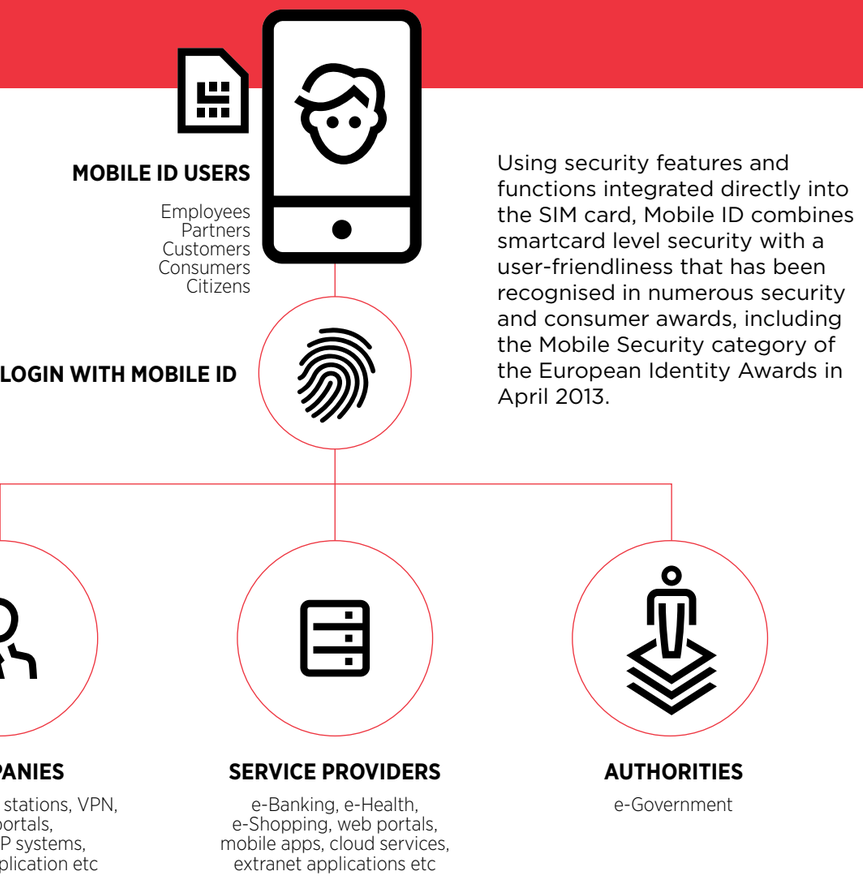
What is Mobile ID?

Mobile ID is a PKI-based secure authentication service that enables users of business applications to access secure accounts, platforms, applications and cloud services in a single, unified mechanism. The service both simplifies the user experience and protects the individual's identity as they interact in the digital world.

Using a different login solution for each portal is a thing of the past. With Mobile ID on the SIM card, every mobile phone becomes an authentication tool. As a result, users have a single login solution for a wide variety of applications – and one that is always to hand.



Swisscom's USP is the ability for the user to access services across multiple applications using just one PIN number, thus simplifying the user experience and encouraging persistent use across multiple platforms.



Using security features and functions integrated directly into the SIM card, Mobile ID combines smartcard level security with a user-friendliness that has been recognised in numerous security and consumer awards, including the Mobile Security category of the European Identity Awards in April 2013.

Swisscom Mobile ID for employees and partners (business applications)

- Secure login for remote work stations
- Access control for data and enterprise applications (e.g. ERP)
- Protection of VPN access to company network
- Login to business-to-business and intranet portals
- Protection of web applications and single sign-on services
- Integration of mobile devices in CRM and ERP workflows
- Protection of terminal services and remote desktop
- Integration in complete solutions (e.g. authentication gateways and web application firewalls)

Swisscom Mobile ID for customers, consumers or citizens

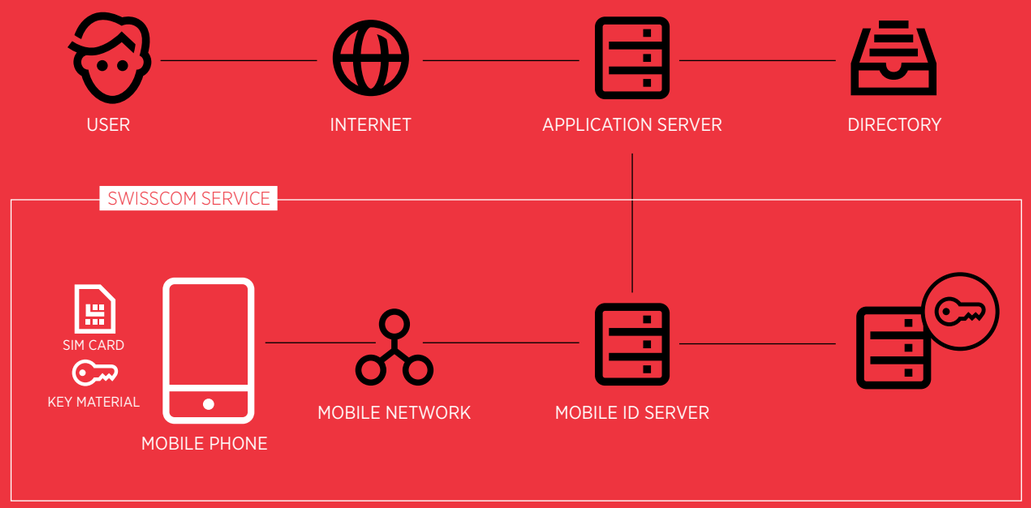
- Login to business-to-consumer and citizen-to-government platforms
- Login to online portals for banking, health, shopping, public sector, education, etc.
- Login to mobile apps
- Context-based transaction confirmation
- Protection of electronic financial transactions
- Protection of cloud services (e.g. software as a service)

Key success factor:
Authentication, not identification:

A key difference in Swisscom's offering to that of other mobile signature services is the fact that, although the service uses PKI technology for authenticating the user, there is no actual identity element beyond the user's mobile number and the MSISDN.

This means that, rather than making a statement to verify that "John Smith is accessing x account at this exact moment" (which entails a complex and rigid in-person identification process for the user), Mobile ID enables Swisscom to simply state to the relying party that "the same user who established an account with service X (e.g. personal insurance account) is the same individual who is accessing this account now."

Due to the strength of the PKI technology and the cryptographic hardware of the SIM, the authentication adheres to the highest level of assurance (Level 4, according to EU Level of Assurance standards), in asserting that the user is unique and the only one with ability to access the service.



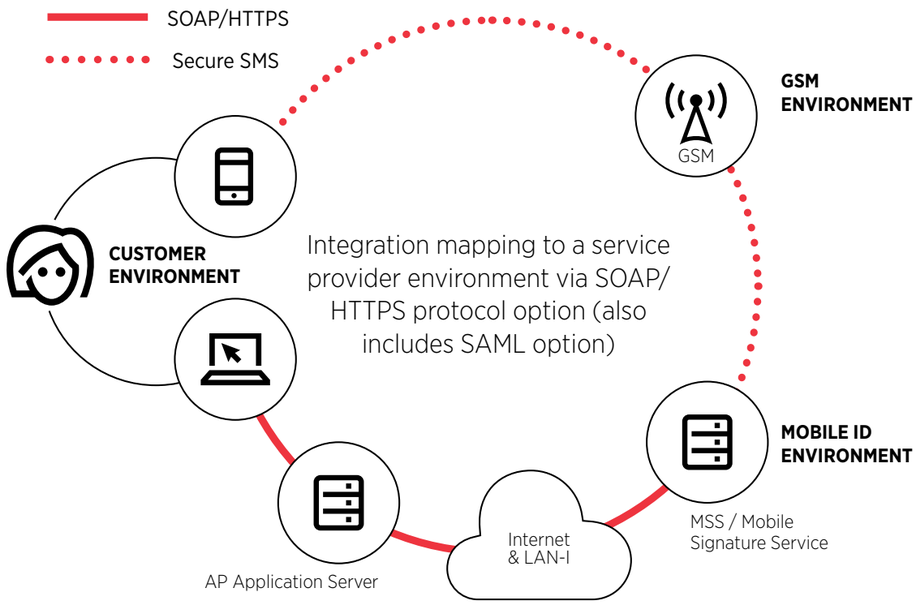
'After having spoken to our partner service providers and to the regulatory bodies here in Switzerland with regards to using certificates with the user credentials stored in them, we realised that this was not really necessary. And it did not match with the freedom we wanted for the Mobile ID in that the individual should be able to utilise Mobile ID for many purposes: they should be recognised as both an employee and an ordinary citizen and a bank account holder. If we had chosen to go ahead with the full mobile signature option from the beginning, this would have required many different certificates for each of these "identities," and different PINs to remember for each one.'

HP Waldegger, Swisscom Mobile ID Business Consultant

Key success factor: Product Simplification

The team at Swisscom understood that new business customers would need to evaluate Mobile ID on more than just the highest security criteria if it was going to prove a success. Far too often in the development of new technology products, the needs of IT infrastructure managers and web developers go overlooked, particularly when it comes to integrating the product with existing technical platforms. Underestimating the technical challenges involved in this integration process, or leaving the client to deal with these aspects of implementation, can lead to delays and sometimes significant challenges to the user experience

The team developed a standard interface to connect applications and online portals of all kinds to the Mobile ID service (customer platforms, company networks, e-government, other cloud solutions, etc.).



Service Interface

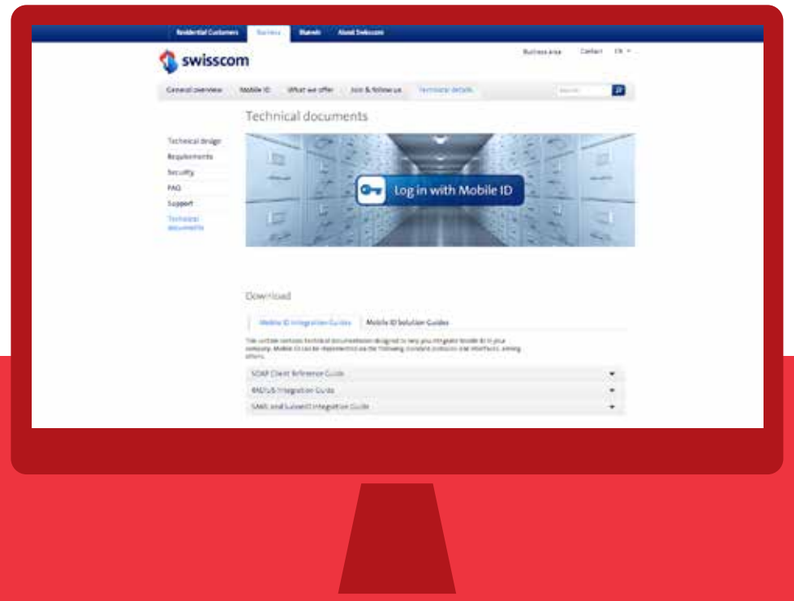
The Mobile ID interface is a web service (SOAP/XML). The protocol and data structures are based on ETSI-standard ETSI TS 102 204. Three pieces of information must be provided for each authentication so that Mobile ID can be used:

1. Mobile number: To whom should the request be sent?

2. Text: What should be displayed on the user's mobile device?

3. Language: In which language should messages be displayed?

From the outset, the Swisscom team determined to ensure that the technical process guides would be open-source, allowing technicians and developers from every client enterprise to access documentation detailing every aspect of technical implementation (including signature codes) via the Swisscom website.



Product-specific documentation designed to help you incorporate Mobile ID in environments with VPN, access gateways, business applications, cloud and collaboration services, etc., including for Google, Microsoft, Oracle, Cisco and others.

Managed Service

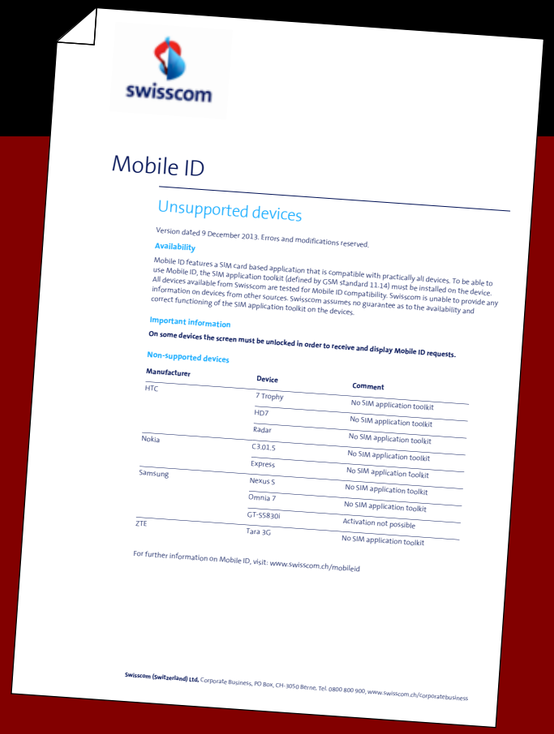
Support for service providers and enterprises covers the following individual services:

- Maintenance of the Mobile ID service interface
- Customer service desk 24 hrs / 365 days
- Fault management
- Defined service level agreement

"The use of this simple protocol gives service provider extreme flexibility for the future. We can build in additional functionality on top of the baseline authentication service: after the initial authentication with Mobile ID, why not introduce a second step with facial recognition, for example?"

Adrian Humbel,
Head of Identity & Access Management,
Head of Swisscom Mobile ID team

Sample of Swisscom's SOAP Client Reference guide



All devices available from Swisscom are tested for Mobile ID compatibility.

Mobile ID is already preinstalled on the SIM card as a SIM toolkit (STK) applet, which can only be accessed by the mobile provider "over the air" (OTA) via the correct identification key. As a result, Mobile ID works on all mobile devices that meet the GSM standard (GSM 11.14 or 3GPP 31.111), regardless of the operating system.

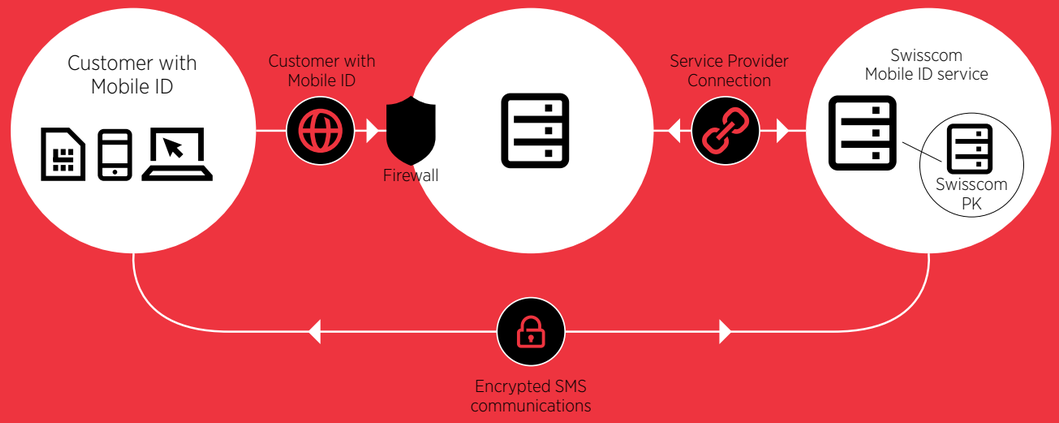
"Customers who use Mobile ID log in more often than customers who use another login"

PostFinance

"We have two specialists in our software team who are members of the Hacker Group in Berlin. They tested out the Swisscom Mobile ID and compared it with the Suisse ID and determined that they have the same level of security, only the Mobile ID system is much simpler."

Joachim Vetter, Head of Development and Customer Relationships for Abacus

To guarantee the security of the STK applet and the initial SIM-specific key and subsequently generated user-specific key, Mobile ID is available on EAL5+ certified hardware. The latest-generation SIM cards contain a cryptographic coprocessor and the Mobile ID SIM applications.



Key success factor: Simplified User Journey

User experience is one of the most important factors which determines the ultimate success of a new product. In the case of Mobile ID, ease of use for the customer was paramount to this service offering, given the product's placement within the Swiss market alongside other high-end security authentication products. The Swisscom Mobile ID team were conscious to ensure that end-users had a postive experience at every step.

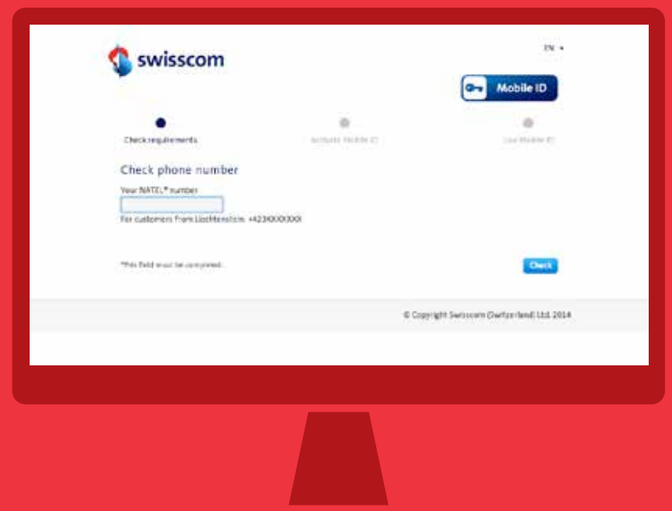
Our first customer was ourselves: Swisscom rolled out the service to its internal employees, which gave us some good insights into the user experience. In fact, there were several mistakes with the rollout which we could avoid with other customers, such as sending both the activation code and the new SIM in the post, which prevented a lot of people from activating it simply because they lost interest if they had to wait. We realised that the activation had to be online in the self-service portal."

Swisscom Mobile ID Product Development team member

Rather than having to go into a Swisscom store in person to purchase and register for their new Mobile ID SIM, Swisscom customers can order it directly from the Swisscom website. Once the customer's account details and address are verified, a new Mobile ID SIM card is sent directly to their registered address via post. This simple process was in fact one of the more challenging steps to implement at first, due to the change in mindset that this required as a business that typically looks to maximise customer touch-point opportunities.

1

To order Mobile ID, the customer first is asked to check their mobile number against the Swisscom CRM database. By checking the customer's account details, Swisscom is able to ensure that the customer is in possession of the right handset.



2

Their postal address is confirmed and a new Mobile ID SIM is sent via post.

3

Once the customer receives their new Mobile ID SIM card, he or she is asked to activate their account. During activation, an individual RSA key is generated on the SIM card and the user defines his or her Mobile ID PIN. This PIN must be entered for every service provider request(e.g. a login).

Upon activation, with this SIM card the mobile phone becomes the user's personal "security token".

"It is fairly normal that we Swiss expect an electronic process in most things we do nowadays. Many are already at the stage where we believe that everything should be available on the web, so it seems archaic to require someone to physically go all the way into the shop to obtain something that is made for an electronic process. It should be available instantaneously. That's what we have tried to do with Mobile ID, but it did entail a big change in philosophy internally.

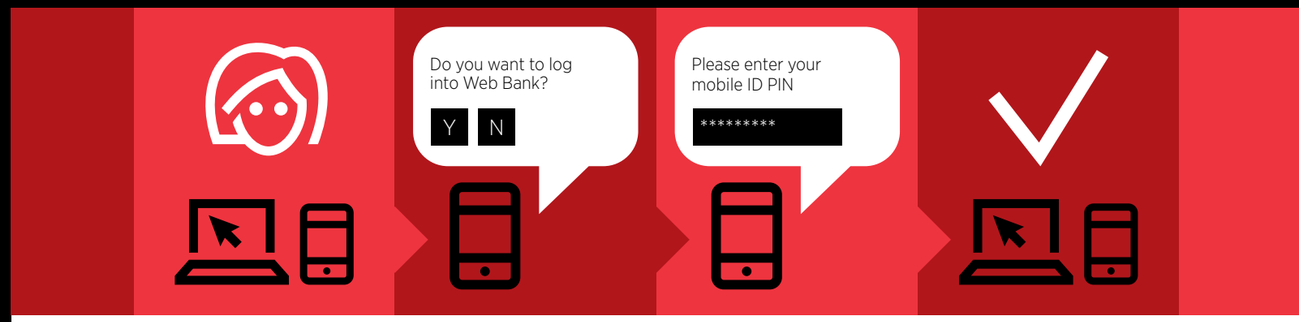
Most of the work done in the last year has been about reducing the complexity that the team originally built. Another example was language support on the applet - now Mobile ID has the same language as the portal. But the most important element was making it much more user friendly with things like this and the online self-service portal."

Adrian Humbel, Head of Identity & Access Management, Head of Swisscom Mobile ID team

"It's always a balance between user experience, complexity and security, but of course we had to include a hardware element as this is really important for our banking-grade security. The SIM card as hardware solved one of our major problems. And you don't have to rely on a physical token: the Mobile ID is always handy, the mobile phone is something you always have with you."

Daniel Gasche, Project Manager of Digital Products, PostFinance

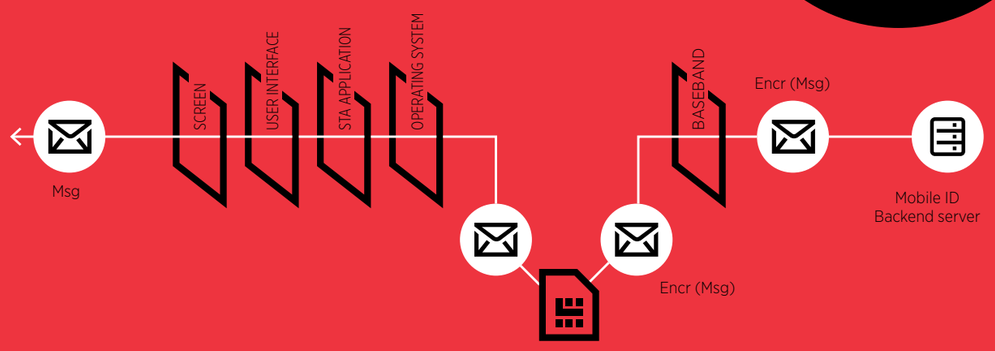
When the customer is using Mobile ID to log in to an account or authenticate themselves for a secure process, this principle of simplification is still maintained.



The main processing steps that are performed by the end-user and the mobile signature service are described below:

1. The end-user uses any application relying on Mobile ID for authentication, which sends a mobile signature request through the dedicated web interface of the authentication platform (AP), including the personal MSISDN as input parameter to login.
2. The AP receives the end-user request, forms the contents to be signed (in accordance with the ETSI TS 102 204 standard) and forwards the request to the MID service.
3. The MID platform receives the signature request and validates the AP in accordance with the service agreement.
4. The MID platform ensures that the end-user signature request is allowed and forwards the signature request to the end-user's mobile phone.
5. The end-user gets a message on his mobile phone to sign the mobile signature request. The end-user signs the request by entering his Mobile ID PIN code.
6. After the AP has received a valid electronic signature, the end-user will be granted access to the corporate application.

The user-specific Mobile ID PIN is independent of the SIM PIN for normal mobile services and is automatically locked if an incorrect PIN is entered five times.



Key success factor: Customer Care

The product team in Swisscom recognised early on that one of the most important components to making the Mobile ID service a success – particularly in the early stages of deployment – would be to ensure that the Operator's business customers had access to support services at all times. This meant having a dedicated business consultant embedded within the Swisscom Mobile ID team to be on call to support customers with any issues, ranging from technical integration queries to customer marketing advice

Equally, when it came to end users, Swisscom endeavoured to place as much support into a self-service portal as possible.

If users forget their Mobile ID PIN or lose their phone, they can contact Swisscom Support via an automated customer help line, which enables the user to identify themselves via a number of different means. The user can prove his or her identity by means of an activation code sent to a previously stored address, and then receives a new certificate with the same run number in the certificate DN (pseudonym). If the user's identity cannot be confirmed, a new pseudonym/run number, and therefore a new digital identity, is issued for the user. From a financial point of view, this makes a huge difference as a call with a call centre can cost up to 50-60CHF, whereas this process now is free.

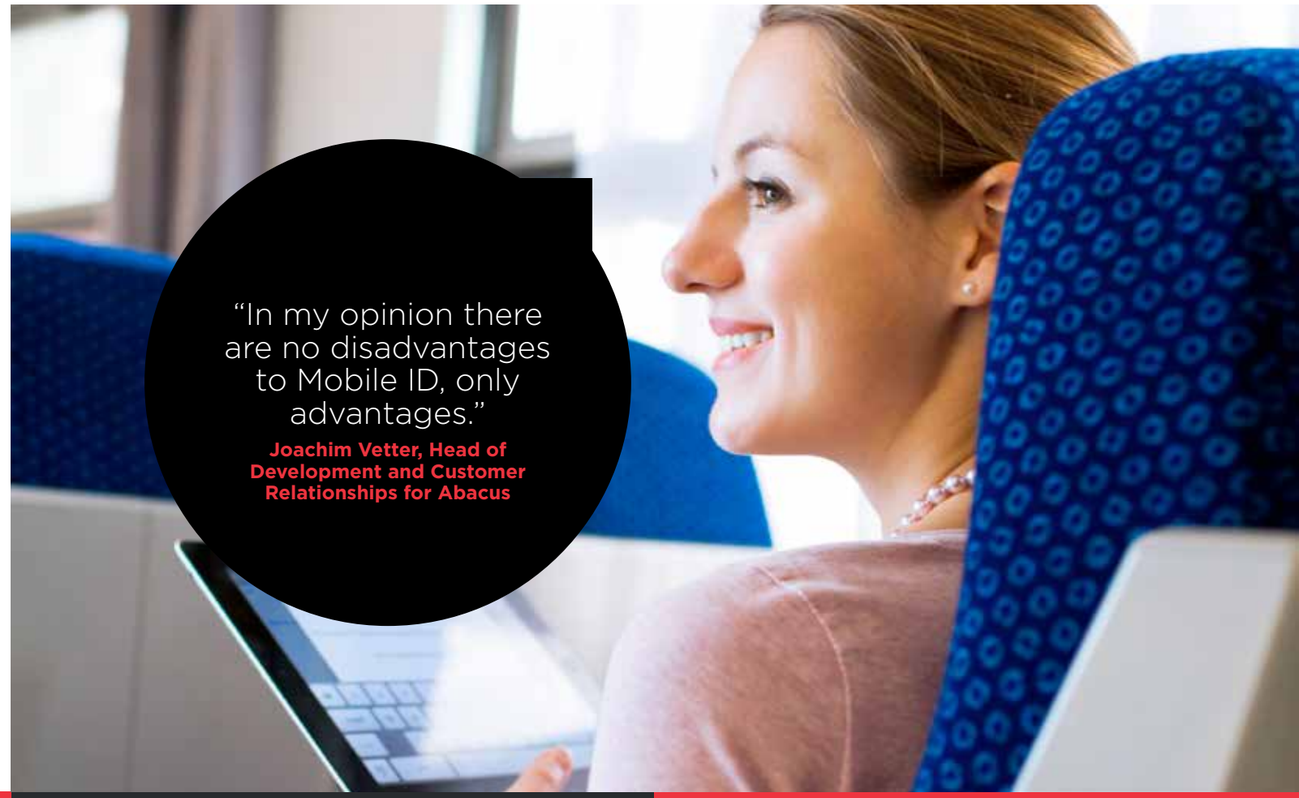
Key success factor: Simple pricing

Mobile ID is offered at a monthly price per user, with differentiation on whether the end-user is using the service in a B2B or B2C context:

Mobile ID price per user (B2B): CHF 4.50 / month (€3.70)
Mobile ID price per user (B2C): CHF 1.00 / month (€0.80)

Companies wishing to use Mobile ID for its employees are charged a one-off lump sum of CHF 1,500 for the activation, setup and provision (regardless of the number of users) and a fixed charge for provision of the interface, support, SLA and reporting is CHF 1,500/year. The costs for SIM cards and technical SMS communication are undertaken by Swisscom.

For companies offering Mobile ID to their own customers as a secure authentication service (e.g. for logging in and accessing accounts and secure web pages), Swisscom allows the enterprise to determine their own customer charging models. For example, PostFinance, a leading Swiss bank, charges 9CHF for a 1 year subscription to Mobile ID.



Interview with Abacus

Abacus is a leading software company in Switzerland and world renowned in the field of EAP (Enterprise Architecture Planning) software. The company currently has around 39,000 customers (small to medium enterprises ranging between 1-500 employees), and approximately 150,000 users of their software services in total.

The GSMA interviewed Joachim Vetter, Head of Development and Customer Relationships for Abacus, on their decision to use Mobile ID for their employees and partners:

"When it comes to ensuring safe access for its employees and partners, Abacus has always been committed to using solutions that did not entail simple username and password combinations. Many of our companies are working in the "trusted accounts" business (such as accountants and others in charge of bookings, financial records and HR processes) and use our software for their internal processes as well as for their own customers. Therefore, having trust in your authentication processes for digital tools is very important - it's part of the Swiss mentality – we are very protective of our data on the web.

"We have two specialists in our software team who are members of the Hacker Group in Berlin. They tested out the Swisscom Mobile ID and compared it with the Suisse ID and determined that they have the same level of security, only **the Mobile ID system is much simpler.**

The implementation was very simple. Testing and integration took around 2-3 months in total: we tested on our employees before rolling out to our customers. It was great – there were no problems at all! From the users' perspective it was very positive. Especially because Mobile ID is very handy – the mobile is always with you. Then the actual implementation process took only 3-4 days.

So far, it's been a great decision for us. Since we launched Mobile ID one year ago it's been running perfectly. We have received feedback from our partners and clients, which has all been very positive: users are satisfied with this solution, they find it very good to have mobile access all the time that is not dependent on additional piece of software or hardware. The only ones who are not happy are the non-Swisscom customers who don't have it yet!

In my opinion, Swisscom Mobile ID will gain rapid traction in Switzerland because one of the major banks, PostFinance, now uses it and it seems to be gaining ground pretty quickly among a lot of businesses.

For example, we are soon going to launch Mobile ID for our HR and salary tool, which is currently used by around 900,000 employees in Switzerland to manage and access their salary and employee benefits information via Abacus. With Mobile ID, they will also be able to access it safely in the cloud. We aim to launch this capability towards the middle of this year.

One thing we are waiting for is to be able to allow users to sign documents digitally. This will be possible in April this year and we are already working on it together with Swisscom by providing specialist expertise to support it.

In my opinion there are no disadvantages to Mobile ID, only advantages.

Key success factor: Developing the Ecosystem

In the early stages of product development, the Swisscom Mobile ID team set clear priorities for the development of Mobile ID as a tool for multiple industry sectors. By establishing a mutual partnership with well-known security software firm, AdNovum, Swisscom was able to immediately offer Mobile ID to a range of high profile enterprises, including some of Switzerland's leading banks, HR system providers and management consulting firms.

In this way, "developing the ecosystem" has been a core part of Swisscom's Mobile ID strategy from the outset, recognising the long-term strategic benefits that come from being prepared to invest both time and resource to establishing partnerships across different sectors in the marketplace. As enterprise IT and security departments worldwide continue to grapple with "bring-your-own-device" challenges, Swisscom has successfully positioned itself as an integral part of the mobile security value chain and a trusted provider of personal data services.

"When we talked to Swisscom and started discussing the Mobile ID, we just thought it was a brilliant idea. Many of our clients were having a lot of trouble providing 2FA (second factor authentication) to their customers – it is a big and growing trend as enterprises are trying to keep up with everyone using multiple devices. Through this partnership with Swisscom, we could combine our strengths to offer a simple solution that used all the Operator strengths of requisite hardware of the SIM, network and customer care, plus our trusted Nevis software and security engineering experience."

Dr. Tom Sprenger, CTO, AdNovum

"The ecosystem for whatever you do as an Operator is extremely important. Authentication and signature services are not just about identifying the customer, they are about trust. The most important thing when developing the ecosystem is maintaining this trust among your partners and customers in everything that you do."

Adrian Humbel, Head of Identity & Access Management, Swisscom

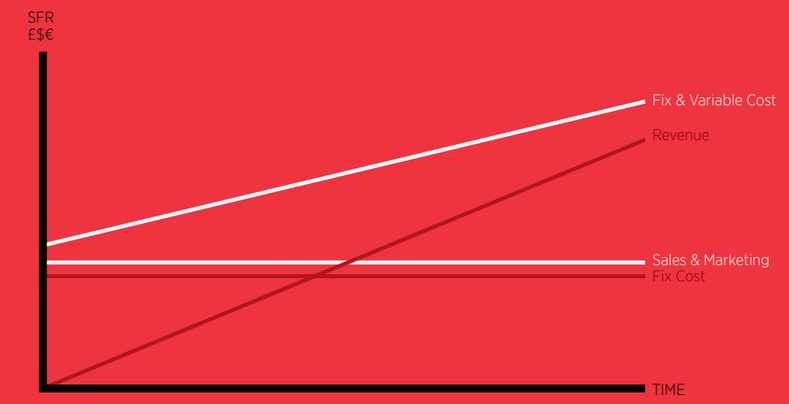
A few core guiding principles helped the Mobile ID team stay focused on the partnerships that would drive scale most quickly in the Swiss market:

- Establish and maintain strong partnerships among secure firms
- Only approach industries / areas where strong authentication is absolutely needed (i.e. banking, secure enterprise access, government services) to ensure that Swisscom's reputation for security is maintained. At a later date, when uptake is more widespread, lower-level authentication services can be pursued.
- At the start, try to get a "lighthouse" account in each sector or vertical as a driver for more uptake within that sector and to ensure a wide range of applications within the whole market (e.g. banking, insurance, local government, federal government)
- Be ready to invest both financially and in terms of human effort in developing ecosystem partnerships. The indirect benefits to driving scale by treating ecosystem investment as a "fixed cost" can be significant and lead to quicker realisation of more sustainable revenues in the long run.

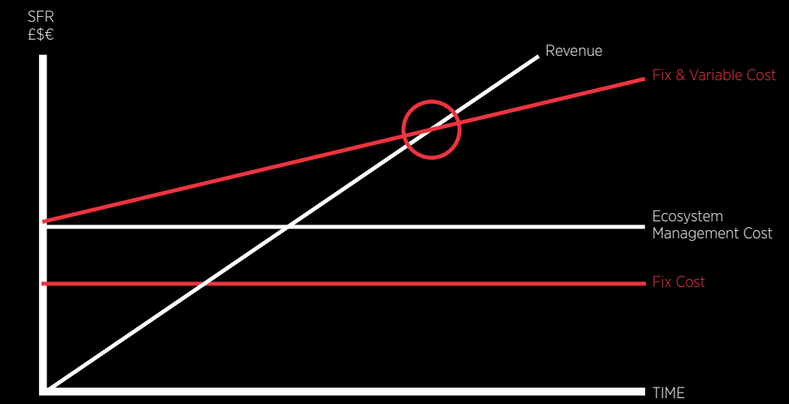
The Swisscom Mobile ID team details its rationale for investment in ecosystem development from the beginning of product development by considering it as a "fixed cost" - this leads to a steeper rise in revenues and a shorter time to obtaining ROI.

As the user base continues to grow and more service providers request Mobile ID for their customers, providing a ubiquitous service across the Swiss market will be an important factor in ensuring that adoption of the service continues to escalate. Swisscom recognised that enabling the other Swiss mobile operators to offer Mobile ID would be key to ensuring long-term success of Mobile ID for all Swiss customers.

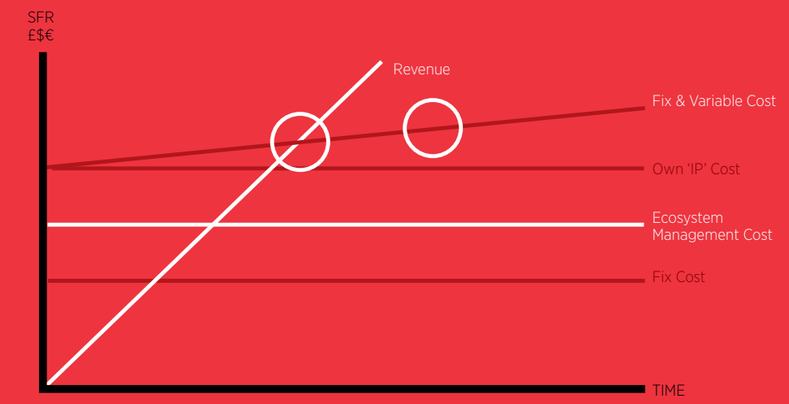
Time to Market without Ecosystem Management



Time to Market with Ecosystem Management



Ecosystem Management on Steroids: Own 'IP'



Interview with PostFinance

The GSMA spoke to the PostFinance team in charge of managing the implementation of Swisscom Mobile ID to understand why they chose to use and market the strong authentication service to their personal and enterprise banking customers.

A few years ago we were already looking for a convenient and secure authentication service to access online banking, especially for mobile users, who were becoming a bigger segment of our customers.

We had a very good business relationship with Swisscom from the beginning, which I think helped a lot in ensuring that we had a good communication process for both the technical implementation and commercial negotiations. Swisscom had already launched the business platform for Mobile ID for B2B services, but we were the first to use it as a customer-facing service, so we were prepared to work together with Swisscom to build these processes.

One way we did this at first was by conducting a technical live test with our internal staff to prove that Mobile ID would work smoothly with our online banking system and so that customers would understand the end to end processes. By sharing the test results, we helped Swisscom to improve the customer experience of their new self-service web portal for customers to order and activate the Mobile ID SIM card.

We don't get many phone calls to our customer care service – this is a good sign, and in fact was one of our own internal criteria for indicating success. It seems that as soon as customers learn about Mobile ID and see how it works they are satisfied. We track our user logins and can clearly state that one of the most important indicators of success is that **customers who use Mobile ID log in more often than customers who use another login**. This is an important sign that typical authentication processes are a big challenge for users.

Of course our goal is to offer our customers the most convenient solution. For the time-being, however, we will continue offering Swisscom Mobile ID as one alternative way to for users to authenticate themselves, since it is not yet offered by the other Swiss mobile operators.

With many thanks to Daniel Gasche, Project Manager of Digital Products, Claudio Lombardi, Product Manager, and Martin Moser, Marketing Manager at PostFinance

"We believe that this is an important service that all the mobile operators in Switzerland should provide. Think about it: it's a win-win for everyone if the pie grows larger. We are working to support the other Swiss mobile operators to launch Mobile ID so that the entire market will increase to +90% if all Operators provide the same service."

Adrian Humbel, Head of Identity & Access Management, Head of Swisscom Mobile ID team

Future services

In January 2014, Swisscom released its latest evolution of the Mobile ID service: **signature.**

Mobile ID signature is an "all-in signing service", with the idea being that an individual can digitally sign any type of media in a legally binding manner (equivalent to a handwritten signature), including music and photos, yet still without requiring any further identity proofing than the original Mobile ID identifiers (the MSISDN and the mobile number).

"The mobile signature function works like a snapshot where at a certain given time we as Swisscom can say: "at this time what we received refers to the original." If the item that was signed gets altered, we can immediately see th at it has been tampered with. This is part of the privacy enhancement: we as Swisscom do not see what has been changed within the document or file (we don't ever even see the original file) but we can confirm that it has been tampered with.

This process is based on segregation of duty; we don't make judgements, but we put everything in the seal and hand it back. So if there is a dispute even 5 years later we can show that record. In this way, Mobile ID signature is a "context oriented" signature – it generates a one-time-use certificate on the spot which expires rapidly. We believe that this will have a huge advantage in many business processes. That's the new way to sign."

Adrian Humbel, Head of Identity & Access Management, Head of Swisscom Mobile ID team

GSMA Personal Data Programme
7th Floor, 5 New Street Square,
London, EC4A 3BF, United Kingdom
Email: personaldata@gsma.com
Web: www.gsma.com/personaldata