Service Description

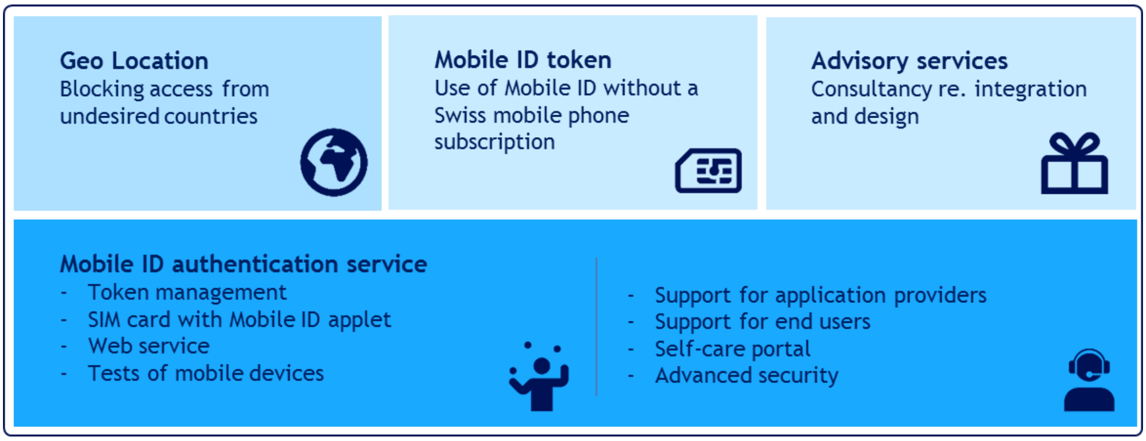
Mobile ID

Table of contents

1 **Service overview** 3
2 **Definitions** 4
2.1 Service Access Interface Point (SAIP) 4
2.2 Usage models 4
2.3 Other service-specific definitions 5
3 **Features and options** 6
3.1 Security elements on the SIM card 6
3.2 Token management 7
3.3 Web service 7
3.4 Online self-care portal for users 8
3.5 Compatibility testing for mobile devices 8
3.6 Support for application providers 8
3.7 Support for users 8
3.8 Security 9
3.9 Business Continuity Management (BCM) 9
3.10 Data protection 9
3.11 Service options 10
4 **Service description and responsibilities** 11
5 **Service level and reporting** 12
5.1 Service level 12
5.2 Service Level reporting 12
6 **Billing and quantity report** 13
6.1 Billing 13
6.2 Quantity report 13

1 Service overview

The Mobile ID service enables companies and application providers to strongly authenticate a personalised Mobile ID connection using their own or outsourced (hosted) applications or infrastructures.



Geo Location
Blocking access from undesired countries

Mobile ID token
Use of Mobile ID without a Swiss mobile phone subscription

Advisory services
Consultancy re. integration and design

Mobile ID authentication service
- Token management
- SIM card with Mobile ID applet
- Web service
- Tests of mobile devices

- Support for application providers
- Support for end users
- Self-care portal
- Advanced security

The service comprises the following elements (see Section 3 for a detailed definition):

- Provision of a standardised interface (based on ETSI TS 102 204) for digitally signed confirmations and/or declarations of intent (as Web services);
- Securing the interoperability with other involved mobile service providers;
- Distribution, administration and lifecycle management of the tokens (SIM cards) required for strong authentication;
- A 24/7 Service Desk and support for application providers and their users;
- Operation and maintenance of the underlying infrastructure;
- Advice and the services required for operation and use on the server;
- Geo Location, Mobile ID tokens and advisory services are available as options for the service.

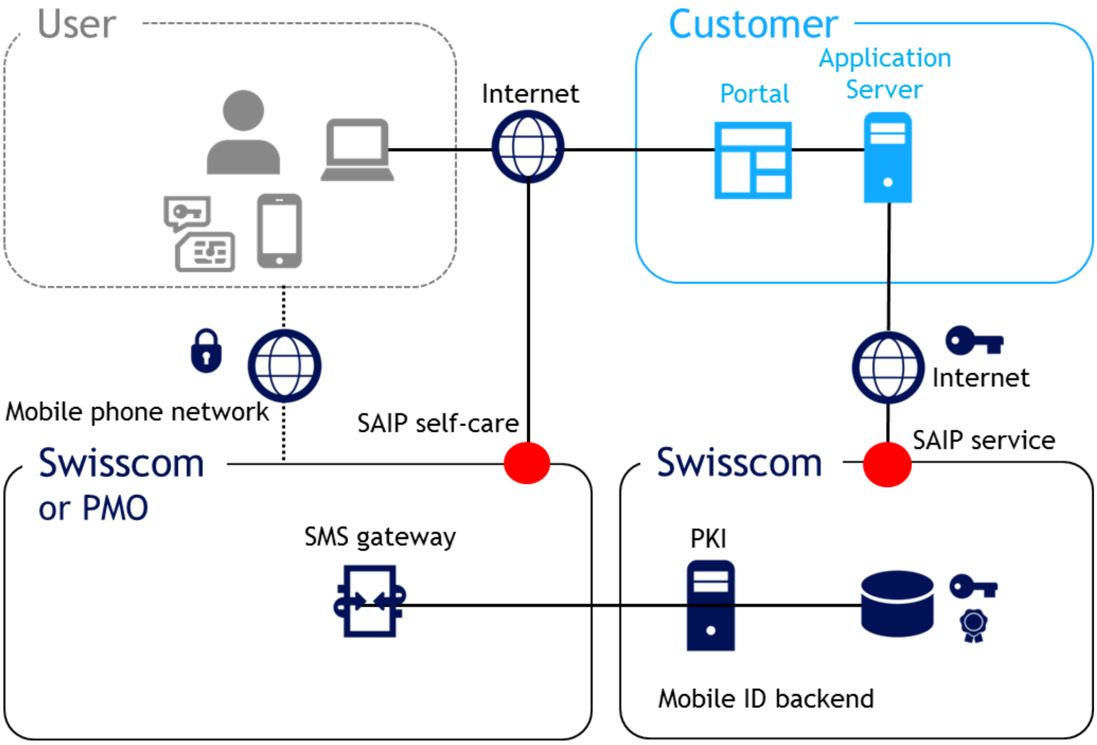
The service is provided at Swisscom data centres in Switzerland, taking account of the appropriate safety requirements.

2 Definitions

2.1 Service Access Interface Point (SAIP)

The Service Access Interface Point (SAIP) is the contractually agreed, geographical and/or logical point at which a service is delivered to the customer who is receiving the service. It is also the point at which a service is monitored and the service level reported.

The following diagram illustrates the elements of the service as well as the service components used therein:



For the Customer (=application provider), the SAIP service is the interface (cf. Section 3.3) via which the applications send Mobile ID queries to the Swisscom Mobile ID backend and receive responses.

SAIP Self-Care grants users access to the online self-care portal (cf. Section 3.4) which is the main tool for users to manage their Mobile ID service. This SAIP self-care portal is independent of the user's mobile service provider and made available accordingly by Swisscom or a third-party provider (PMO).

2.2 Usage models

The service is available in two usage models: business to business (B2B) and business to consumer (B2C).

Usage model	Description
B2B	For companies that use strong authentication for their internal and external staff in order to meet their own requirements (i.e. within the company).
B2C	For application providers that use a strong authentication solution for their own customers. This model is therefore exclusively for applications in which an application provider's external customers use Mobile ID.

Both models essentially have the same pricing model, but differ in the application of the prices. For both models, the service is billed in accordance with the standard price list.

2.3 Other service-specific definitions

Usage model	Description
PMO	PMOs (Participating Mobile Operators) are all mobile service providers whose telecommunications customers can use Mobile ID. PMOs use the Swisscom Mobile ID infrastructure, on which they can either operate their own mobile network infrastructure or function as a virtual provider. All PMOs have installed the Swisscom Mobile ID applet on their SIM cards. A list of current PMOs is available from Swisscom on request.
SIM Toolkit applet	A SIM Toolkit applet is an application that is installed on a SIM card and protected specially. The SIM Toolkit is a GSM standard that enables a SIM card to interact with a mobile device.
MSISDN	A globally unique mobile telephone number. When using Mobile ID, assignment takes place via the MSISDN. The actual user of this number remains anonymous on the service.
Application provider (Customer)	This is the Mobile ID customer that concludes a Mobile ID contract with Swisscom and is thus Swisscom's direct contractual partner. By contrast, an application provider offers its users the Mobile ID service for their applications.
User	Mobile ID users are the end customers of this service. They may be either an internal staff member or an external user. Users must have a valid mobile telecommunication subscription and a latest-generation SIM card from either Swisscom or the PMO.

3 Features and options

The following variants and options are available for the service:

Standard services	Swisscom	PMO
Security elements on the SIM card	●	●
Token management	●	●
Web service	●	
Online self-care portal for users	●	●
Compatibility testing for mobile devices	●	
Support for application providers	●	
Support for users	●	●
Security	●	●
Business continuity management	●	
Data protection	●	●

Options		
Advisory services	⊙	⊙
Geo Location	⊙	⊗
Mobile ID token	⊙	⊗

● = Standard ⊙ = For an additional fee ⊗ = Not available

3.1 Security elements on the SIM card

Secure environment

Mobile ID is pre-installed directly on the SIM card as a SIM Toolkit (STK) applet. As a consequence, Mobile ID functions on all GSM standard (GSM 11.14 or 3GPP 31.111) mobile devices, irrespective of their operating system. The STK applet is loaded directly on the SIM card in a secure environment by the SIM card supplier. Following loading and initialisation, all local access is blocked. Thereafter, the applet can only be accessed "over the air" (OTA) by the mobile service provider using the correct identification key. These communication keys are generated randomly and individually for each SIM card by the SIM card supplier.

Certified hardware

To guarantee the security of the STK applet, the initially employed SIM-specific key and the subsequently generated user-specific key, Mobile ID is available on hardware certified at the very least in accordance with EAL4 of the ISO/IEC 15408:2005 standard or Level E3 High of ITSEC version 1.2.

Personal authentication features

The user-specific 2048-bit RSA keys are generated on the SIM card and protected by a PIN chosen by the user. The private key and the PIN never leave the SIM card and can neither be accessed nor exported by Swisscom or third parties. The PIN is a six-digit number that is blocked after five incorrect entries.

3.2 Token management

With regard to token management, Swisscom or the PMO provide the following services to their respective subscribers (telecommunication customers):

Event	Condition	Swisscom or PMO service
Ordering Mobile ID	Subscription/agreement with mobile network operator	Mobile ID orders can be placed via the self-care portal of either Swisscom or the PMO
Identification	Ordering Mobile ID	The mobile number is checked
Activation	Positive identification	The owner of the Mobile ID connection number must set his individual Mobile ID PIN and obtains a unique certificate
Loss/theft/ defects	Mobile subscription and positive identification	The owner of the Mobile ID connection orders a replacement via the self-care portal or the Service Desk (Support)
Resetting the Mobile ID PIN	Mobile ID and positive identification	The owner of the Mobile ID connection can apply for a new Mobile ID PIN via the self-care portal or the Service Desk (Support)
Mobile subscription termination	Mobile subscription and positive identification	Access to Mobile ID is blocked after termination
Subscription expiration	Mobile subscription	Access to Mobile ID is blocked
Certificate renewal	Mobile subscription and forthcoming authentication	The certificate is extended once it is about to expire
SIM exchange	Subscription/agreement with mobile network operator	Proactive or reactive replacement by Swisscom or the PMO depending on the state of technology

3.3 Web service

The Mobile ID service offers the following functions as a Web service (SOAP or RESTful) in accordance with the ETSI TS 102 204 standard:

- MSS signature request: sending text messages to specific Mobile ID subscribers (UTF-8: max. 119 characters; GSMDA: max. 239 characters).
- MSS signature response: reception of signed confirmations for sent messages.
- MSS status request: sending status requests for a previous query.
- MSS status response: reception of responses to previous status requests.
- MSS profile request: sending status requests to a specific mobile number.
- MSS profile response: reception of responses to previous status requests.
- MSS receipt request: sending an encrypted message following a previous query (UTF-8: max. 119 characters; GSMDA: max. 239 characters).
- MSS receipt response: reception of responses to an encrypted message.

Further information about the functions and parameters is published in the “Mobile ID Client Reference Guide”, which can be found on the Swisscom Web site at www.swisscom.ch/mid.

Changes to the interface
If the service interface is further developed in a way that affects customer applications, Swisscom shall inform the Customer about the changes at least six months in advance. Swisscom shall provide the Customer with instructions about the changes in a timely manner. The existing interface shall remain available for at least 12 months after notification of the further development, thus ensuring that the Customer can continue using the existing interface for another 12 months. Support and maintenance services shall continue to be provided during this time at no additional cost.

Changes to the interface must be implemented by the Customer within 12 months of notification of the further development thereof.

Interface changes are made through no more than two releases a year.

Swisscom may make important changes due to safety requirements without advance notification and be implemented immediately.

In either case, the Customer is notified about changes as soon as possible.

3.4 Online self-care portal for users

The online self-care portal provides users with a simple way to order, activate and manage (lost or locked PIN code) the Mobile ID service.

The Web-based portal also contains information about Mobile ID in the form of a user community and FAQs as well as advice on devices that do not support the Mobile ID function.

The following services are available on the self-care portal:

- Ordering Mobile ID (SIM card)
- Activating Mobile ID
- Testing Mobile ID
- Resetting the Mobile ID PIN
- Further information (e.g. a list of the devices that are not Mobile ID-compatible, FAQs, user community)

The online self-care portal is the main tool for users to manage their Mobile ID service.

3.5 Compatibility testing for mobile devices

Swisscom regularly tests the compatibility of Mobile ID with the most important mobile devices available on the market as well as their operating systems and regularly publishes a list of incompatible devices on the Internet. Swisscom cannot guarantee the completeness of this list.

3.6 Support for application providers

The Swisscom Service Desk is the central point of contact for support for application providers. Requests can be made by telephone by authorised persons defined by the application provider. A ticket is issued for every customer enquiry. This 1st-Level Support provides round-the-clock (24/7) incident management for the service. It also coordinates and monitors the downstream areas providing 2nd- and 3rd-Level Support as well as the associated escalation and problem management processes. The Service Desk regularly notifies the application provider about the status of their ticket, confirms successful completion of customer queries and closes the ticket. Support (from the Service Desk) is available in English, German, French and Italian.

Swisscom notifies the Customer and Mobile ID users on a publicly-accessible Web page about current outages, planned maintenance windows and already resolved outages. This information is also made available to the Customer in an editable form.

3.7 Support for users

The primary support for users is secured via an online self-care portal (cf. Section 3.4 above).

The relevant PMO's service desk is also available to answer more in-depth queries. The support services are generally available in English, German, French and Italian. They are monitored solely by and the sole responsibility of the relevant PMO.

3.8 Security

IT Security Level Basic (ITSLB)

The security measures implemented for Mobile ID are based on the basic IT security concept, checked constantly and, where necessary, improved. Compliance is confirmed by periodic ISO/IEC 27001 audits. Details of the implemented measures can be found in the enclosure entitled “Information Security”.

IT Security Level Advanced (ITSLA)

In addition to the measures included in ITSLB, this service also implements the following Mobile ID-specific security measures as standard:

- Protection of the user-specific private keys in certified hardware
- Each use of the key requires the entry of the personal PIN set by the owner
- Proof of every declaration of intent via personal digital signatures
- Transport encryption of Mobile ID messages from the Swisscom backend to the SIM
- Use of digital certificates from an environment certified in accordance with international standards (ETSI TS 102 280)
- Every application provider is provided with a unique caller identification number (prefix) for recognition purposes

IT Security Level Customized (ITSLC)

Customers with enhanced security requirements can check implemented security concepts in workshops and receive confirmation of the implementation of individual measures. These workshops are subject to a charge. In addition, measures and proofs of the Customer's compliance with regulatory conditions can be agreed on a case by case basis subject to an additional charge.

3.9 Business Continuity Management (BCM)

Objective

Swisscom's BCM is designed to safeguard the service in the event of a BCM incident (IT crisis or catastrophe). Swisscom has processes and procedures that aim to counteract the interruption of the service and protect customers from the effects of material outages or catastrophes.

Business recovery levels

The availability of the service is secured in accordance with the recovery levels defined under “Continuity” (cf. Section 5.1 below).

- The RTO specifies the maximum allowable time period for restoring a service after an IT crisis has been declared (for details, see the Annex “SLA Definitions”).
- The RPO defines the earliest possible restore point for a system that has been recovered following an IT crisis (for details, see the Annex “SLA Definitions”).

Crisis management

Swisscom shall provide the following services if a BCM event occurs:

- A Swisscom crisis management team is responsible for restoring provision of the services and works together with the Customer’s crisis management team.
- Measures to restore the service are initiated and monitored by the Swisscom crisis management team
- Swisscom takes steps to return to normal operation.

3.10 Data protection

The provisions of the General Terms & Conditions and/or the framework agreement apply.

3.11 Service options

Advisory services

Swisscom shall offer customers advisory services on security, designing and planning Mobile ID projects and connecting them to existing customer environments.

Geo Location

Geo Location offers additional information for more in-depth checking of user authentication. When logging on, Mobile ID requests two current data parameters from the Geo Location function:

- The country (mobile country code)
- The mobile service provider used (mobile network code)

This allows the Customer to restrict access by users to specific applications and/or data depending on the country they are in and the mobile service provider used.

In contrast to Geo IP, Geo Location Mobile ID data cannot be circumvented through the use of VPNs, proxies or similar measures. Mobile ID Geo Location also prevents the local modification of data such as GPS localisation of the user.

Due to the data protection regulations, the application provider is responsible for obtaining the user's prior consent to evaluate the Geo Location information.

Mobile ID token

A Mobile ID token is a dedicated authentication token for users. Thanks to this token, all users can use the application provider's applications in conjunction with Mobile ID, even if they do not have a suitable mobile phone subscription.

This token is a Swisscom SIM card on which all services except for Mobile ID (i.e. voice, data, SMS and SIM PIN/PUK) have been technically blocked. In this, the application provider manages the Mobile ID tokens (i.e. distribution to users) itself. In the event of loss or replacement, the application provider is the users' primary point of contact.

4 Service description and responsibilities

Non-recurring services

Activities (S=Swisscom/C=Customer)	S	C
Provision of service		
1. Provision of the Mobile ID infrastructure	X	
2. Sending of the prefix, IP addresses and SSL connection certificate		X
3. Configuration of the firewall		X
4. Connection of the application provider and sending customer-specific access data	X	
5. Integration of Mobile ID into the customer-specific application(s)		X
Other non-recurring activities		
1. Ordering optional extras		X
2. Provision of optional extras	X	
Termination of service		
1. Removal of firewall configurations	X	
2. Deletion of customer rights in the Mobile ID infrastructure	X	

Recurring services

Activities (S= Swisscom/C=Customer)	S	C
Standard services		
1. Operation and maintenance of the Mobile ID infrastructure	X	
2. Provision of support services (Service Desk, incident management, etc.)	X	
3. Updating customer-specific information (contact persons, certificate, etc.)		X
4. Lifecycle management (infrastructure, self-care portal, SIM cards, etc.)	X	
5. Proactive customer notification in the event of outages (major incidents) and maintenance	X	
6. Provision of information about expected use for ongoing capacity planning		X
Provisioning of software licences		
1. Included in the service	X	

5 Service level and reporting

5.1 Service level

The description of the service levels (operation time, support time, availability, process, performance, security and continuity), the measurement methods and the reporting system for the following standard service levels is set out in the document entitled "SLA Definitions".

The following service levels shall be provided for the offer variants (see Section 3). If multiple service levels are available for each variant, the service level shall be selected in the individual contract.

Service level & target values		SAIP service	SAIP self-care
Operation time			
Operation time	7x24	●	
Provider maintenance window	Tues 11 p.m. – Wed 2 a.m.	●	⊗
Support time			
Support time	Mon-Fri, 7 a.m. to 6 p.m.	⊗	●
	Mon-Sun, 24 hours a day	●	⊗
Fault acceptance	Mon-Sun, 24 hours a day	●	●
Availability			
Service availability	Best effort	⊗	●
	99.90%	●	⊙
Security			
	Basic (ITSLB)	⊗	●
	Advanced (ITSLA)	●	⊗
	Customized (ITSLC)	⊙	⊗
Continuity			
	RTO/RPO best effort	●	●

● = Standard ⊙ = Option for an additional fee ⊗ = Not available

5.2 Service Level reporting

Within the scope of the service, the customer receives the following standard level reports.

Service level report		SAIP service	SAIP self-care	Reporting period
Availability	Availability in %	⊙	⊗	monthly
Security	ISO 27001 certificate	●	●	annually
	ETSI 102 280 certificate	●	⊗	annually

● = Standard ⊙ = For an additional fee ⊗ = Not available

6 Billing and quantity report

6.1 Billing

Services are billed retroactively for the previous month.

The following details are shown on the bill or are used as the basis for billing:

Price position	Unit/period	Minimum usage/ billing	Maximum usage/ billing	Included volume
Price per user	MSISDN/month	0	Unlimited	0
Setup and connection charge	Connections/year	1	Unlimited	0

The per-user price (B2B and B2C) is due in every month in which the relevant user actively uses the Mobile ID service at least once.

6.2 Quantity report

The following data and information about the provided service elements can be shown:

Product services/options	Reporting information on billing
Anonymised MSISDN	List of all mobile phone numbers billed for in the usage period