As a leading trust service provider in Europe, we enable the most innovative digital business models .

Service Description
Online Remote Registration (SRS)

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

Switzerland

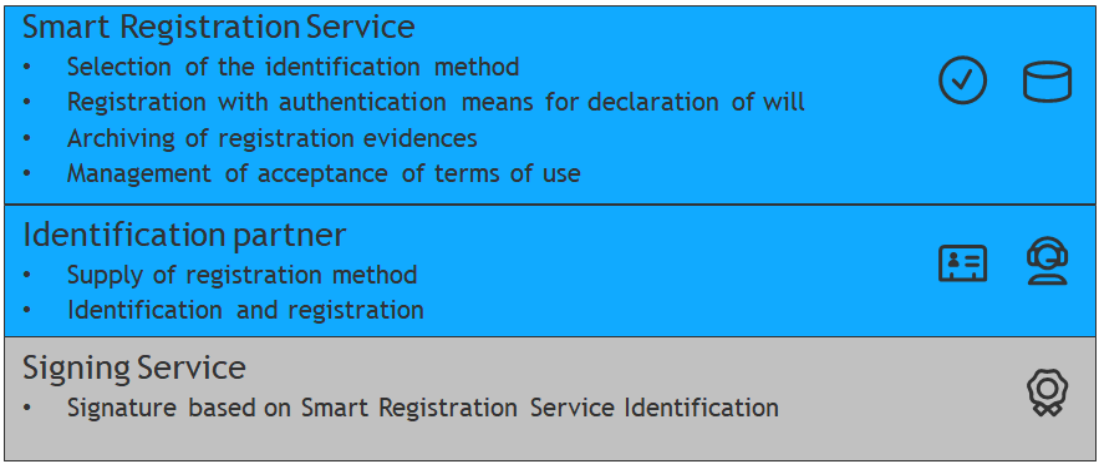
https://trustservices.swisscom.com
E-Mail: sts.salessupport@swisscom.com

1 Content

2 Service overview

The Signing Service and the Smart Registration Service are server-based services for remote signature and identification distributed by Swisscom Trust Services AG and provided by Swisscom IT Services Finance S.E., Vienna, Austria, hereinafter “Swisscom ITSF” and Swisscom (Switzerland) Ltd..
Swisscom Trust Services AG distributes the Services in its own name or grants the right to third parties to distribute the Services in their own name.
Swisscom’s facility for providing remote identification services (hereinafter "**Smart Registration Service**" or, for the sake of simplicity, “Service” or "SRS") enables a signatory to make the choice of one or more identification procedures to be used for the purpose of registration for the use of electronic signatures with Swisscom’s Signing Service. Proper registration entitles our sales partners and their customers to issue signatures to the signatory in future. This requires a contractual relationship with a provider of the Swisscom Trust Services signature service. Swisscom Trust Services does not offer signatures for direct sale to private individuals.
Registration requires that the user also uses authentication, which is then later used to approve the signature. This can be, for example, the Mobile ID app or a combination of password and one-time code via SMS or another authentication solution offered. If the authentication is based on an app or a hardware token, this must usually be initialised in advance.

Swisscom Trust Services uses partners (hereinafter “Identifiers”) for the identification procedures of the Smart Registration Service and commissions them to carry out the respective identification procedure in accordance with EU and Swiss legislation on electronic signatures.
After successfully completing the respective identification procedure, Swisscom archives the identification data for the legally prescribed period and manages the acceptance of the Swisscom terms and conditions of use. From this point on, the identified person can create advanced or qualified electronic signatures (“repetitive signing”) via the Swisscom trust service – depending on the identification method – on the basis of the means of authentication (e.g. mobile number) verified during the identification procedure and until the validity of the identification expires.



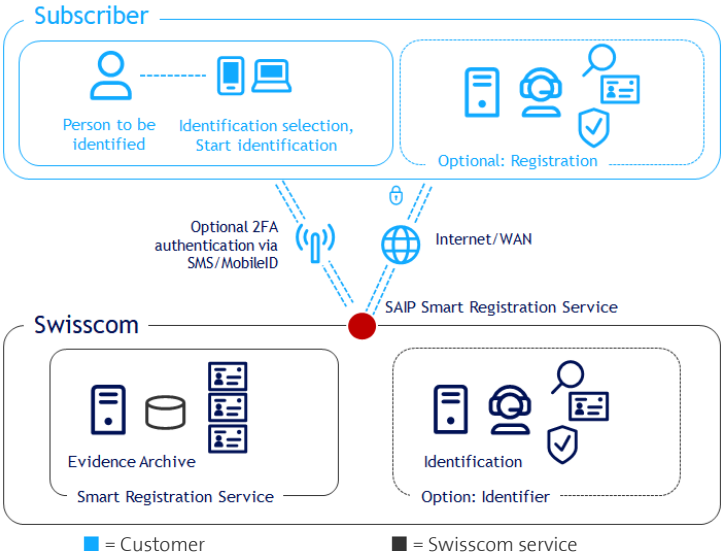
3 Definitions

3.1 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 service user, i.e. the user. It is also the point at which a service is monitored and the provided service level is documented.
The SAIP is here the web page https://srsident.trustservices.swisscom.com . The user can choose between variant methods, can do the payment by credit card or voucher code and perform the registration process. Dependant on

the registration method the user will be redirected to the identification service partner which performs the identification.

The following purely schematic diagram serves to demonstrate the services and service components of the Smart Registration Service:



The user first communicates with the Swisscom Smart Registration Service (SRS) via the Internet. After forwarding, he communicates directly with the identification service provider. The identification service provider makes the identification data, the so-called "evidence", available to Swisscom. If this has not already been done during registration, the signatory must also sign the terms of use for the signing service. Swisscom sends out an SMS with the links to the terms of use, which must then be accepted using the authentication method.
Mobile services used for the identification, authentication or declaration of consent are not included in the service level commitment. The availability of this service is assured if enquiries are accepted by the Service and answered correctly to the SAIP in line with the interface description. The correct response can also consist of an error message that is documented or meaningful for the User.

3.2 Service-specific definitions

Term	Description
Advanced Electronic Signature (AdES)	Advanced electronic signature provided by the Signing Service in accordance with the certification guidelines of Swisscom (Switzerland) Ltd. or those of Swisscom IT Service Finance S.E.
eIDAS regulation	EU regulation on electronic identification and trust services for electronic transactions in the internal market.
Evidence	Evidence in the form of a signed PDF document. This PDF typically contains the photos and scans created during the identification process as well as the collected data or other data required by regulatory authorities for proof of identification. The electronic signature of the organisation that carried out the identification is attached to the evidence.
Identifier	If the User does not provide its own identification and registration procedure, Swisscom offers identification and registration through an identification partner, known as an identifier.
MobileID	Managed service for secure user authentication via mobile phone. MobileID can be purchased from various Swiss providers, including Swisscom.
OTP	One Time Password – password created for use on one occasion which is sent via SMS.
Password with One Time Password	Procedure for 2-factor authentication in which a password is selected for signature for the signature service and a one-time password sent by SMS is also entered.

Term	Description
Person to be identified	Natural person who must be identified in advance in order then to electronically sign a document with authentication and declaration of intent.
Qualified Electronic Signature (QES)	Qualified Electronic Signature provided by the Signing Service in accordance with Swisscom's certification guidelines or those of Swisscom IT Service Finance S.E.
RA delegation contract	Contract between Swisscom and the identifier to which Swisscom has recourse for the implementation of the identification procedures.
Registration	Regulated process for identifying and storing identification data and the means of authentication associated with such identification data that are required to trigger an electronic signature via the Signing Service.
Registration Authority (RA)	Authority responsible for identifying the signatories. Under an RA delegation agreement, Swisscom (Swisscom) Ltd. or Swisscom ITSF may outsource parts of the registration process to third parties.
User	Swisscom provides the services covered by this service description to the user. The user is either a direct Customer of Swisscom with an Signing service contract (including acceptance declaration) or has a commercial contract with a reseller of Swisscom services.
User application	The user provides one or more persons to be identified with access to an application with which they can register for the Signing Service in accordance with Swisscom's terms and conditions of use, and the user ensures the selection of the registration method, sends optionally pre-identification data, and ensures the transmission of the received URL referring to the identification partner to the person to be identified. The user application in this context is not part of this service description. It is provided outside of the Signing Service, for example, by partners of Swisscom or the user itself.
Terms and conditions of use (for Swisscom signature service)	The terms and conditions of use govern the terms for using the signature certificates and signature service within the scope of the relationship between Swisscom (Switzerland) Ltd or Swisscom IT Services Finance S.E. and the signatory on a user application. They may be viewed at https://trustservices.swisscom.com/repository/.
VZertES	Swiss ordinance on certification services in relation to electronic signatures and other digital certificate applications (Schweizerisches Verordung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate).
ZertES	Federal Act on certification services in relation to electronic signatures and other digital certificate applications (Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate).

4 Variants and options

Standard variant	Smart Registration Service
Identification by identifier:	
SRS Video EU: Video identification for EU signatures	○
SRS-eID DE: eID identification (Germany)	○
SRS Bank DE: Identification by use of e-Banking login	○
SRS Selfie Ident EU: Self identification for EU signatures	○
SRS Video CH: Video identification for Swiss signatures	○
SRS Autoident CH: Auto identification for CH signatures	○
Use of the Self-Service Portal	●

● = Standard (included in the Price) ○ = For an additional fee

4.1 Definition of service specifications and options

Specification/Option	Definition
SRS Video EU: Video identification for EU signatures	In the case of SRS video EU, the user receives a URL to a website, on which he can start the registration. The person to be identified can then access the video identification service. For this purpose, it is necessary to have a PC with webcam or a smartphone equipped with a camera and an installed app. The app to be installed is shown on the website. Within the context of a web session, the person to be identified must show their ID under the guidance of an operator of the video identifier and answer questions to confirm the ID data and demonstrate that they are present in person. The data determined in this way are then transmitted to Swisscom.
SRS eID DE: eID identification (Germany)	The user receives a URL to a website, on which he can start the registration. After calling up the URL, the person has to install an App on the Android or Apple mobile device in order to perform the following steps: - The user must take a picture of the front and back side of the German ID card ("Personalausweis") or a German eID Card or foreign eID card ("Aufenthaltstitel"). - Afterwards the user must allow to read out the identification data from the the chip of the ID card. The data will be read out. - The mobile number must be confirmed by entering a one time password which is transmitted via SMS. The evidence data set with the proof of registration will be transmitted to Swisscom.
SRS Bank DE: Identification by use of e-Banking login	In the case of SRS bank DE, the user receives a URL to a website, on which he can start the registration. The person to be identified now calls up the bank identification service, which first asks for the identification data, including mobile number, for future declaration of will. The person to be identified then enters the account details of its e-banking-enabled bank. The person to be identified logs into its bank account and confirms the authentication requests made by the bank and carries out a reference money transfer. The mobile number is now confirmed by an SMS one-time password. After this procedure, the person to be identified leaves their bank account again and is thus identified. The identification data, the mobile number and reference to the bank login process data are transferred to Swisscom. In this case, the identifier keeps the exact operation data as a delegated registration authority.
SRS Selfie Ident EU: Self identification for EU signatures	The person to be identified has to download and to install a self-identification app and to follow up the procedures indicated in the app: • The front and, if applicable, the back of the approved ID document must first be captured with the smartphone's rear camera. • The ID document must be tilted and moved so that all optical security features (e.g. holograms) can be recognised in the light. • The photo of the ID document is compared with a self-taken picture of the person to be signed by means of the front camera. • A liveness check is carried out (e.g. by speaking two predefined random words in a video recording or fulfillment of a predefined movement of the head). • The identification data is checked in the background supported by AI algorithms. (up to 2 minutes) • The mobile number is checked and Swisscom's terms of use are accepted.

Specification/Option	Definition
	• The authentication method (Mobile ID app or password / one-time code procedure) is initialised here: i.e. no SMS with the terms of use is sent out after this identification method. The result data record is then transmitted to Swisscom.
SRS Video CH: video identification for Swiss signatures	In the case of SRS video CH, the user receives a URL to a website, on which he can start the registration. The person to be identified can then access the video identification service. For this purpose, it is necessary to have a PC with webcam or a smartphone equipped with a camera and an installed app of he uses the browser (not supported on mobile phones). The app which can be installed is shown on the website. Within the context of a web session, the person to be identified must show their ID under the guidance of an operator of the video identifier and answer questions to confirm the ID data and demonstrate that they are present in person. The data determined in this way are then transmitted to Swisscom.
SRS Autoident CH: Self-identification for CH signatures	The person to be identified has to download and to install an auto-identification app and to follow up the procedures indicated in the app: • The front and, if applicable, the back of the approved ID document must first be captured with the smartphone's rear camera. • The ID document must be tilted and moved so that all optical security features (e.g. holograms) can be recognised in the light. • The photo of the ID document is compared with a self-taken picture of the person to be signed by means of the front camera. • A liveness check is carried out (e.g. by speaking two predefined random words in a video recording or fulfillment of a predefined movement of the head). • The identification data is checked in the background supported by AI algorithms. (up to 2 minutes) • The mobile number is checked • The result data record is then transmitted to Swisscom. • A SMS will be sent out with a link to Swisscom's terms of use which must be accepted by Mobile ID (App) or password/one-time code.
Use of the Self-Service Portal	The Self-Service Portal enable the verification of the registration. It can be checked whether the registration has been carried out correctly for the respective jurisdiction, the signature level and under acceptance of the terms of use. If necessary, the acceptance of the terms of use can also be triggered.

4.2 Procedure for identification and registration

4.2.1 Selection of the registration method

The person to be identified visits the web page:
https://srsident.trustservices.swissom.com

The user selects a suitable method based on the following criteria:
- The procedure allows registration according to the appropriate jurisdiction. For signatures under EU law, a registration procedure must be selected which is approved in the EU under the eIDAS regulation. For signatures under Swiss law, a procedure must be selected which is approved under the Swiss Signature Act ZertES.
- The legal signature quality must be right: As a rule, qualified electronic signatures, which can usually replace handwriting, require more complex registration than advanced electronic signatures. Advanced electronic signatures, however, might not be allowed for certain legal processes (e.g. granting of credit). The user is responsible for

observing these conditions when selecting the identification procedure. The user acknowledges that the selection of an inadmissible identification method for the desired electronic signature will result in an error message in the electronic signature creation process and prevent the creation of the electronic signature.
- The identification method must fit. Each identification method specifies the requirements that must be met. For an eID identification, the person must be in possession of a state-approved eID solution and also have a smartphone with NFC and/or an app that is state-approved. For video and auto identification procedures, a machine-readable ID (passport or EU/CH ID card) must be available.
- Price/voucher code: The procedures have - depending on the effort - different prices. If payment is not made by credit card but by voucher code, the voucher code may be restricted to a specific procedure. In this case, it may be necessary to check with the party that provided the voucher code.
The User receives access to the Smart Registration Service to enable it to use the contractually agreed identification procedures. This access is certificate-supported and enables secure data transmission.

4.2.2 Payment

After the appropriate payment procedure has been selected, the user can pay for the identification by means of the specified credit card or voucher code. Credit card sales result in contracts with private customers who subsequently receive a payment receipt. Legal entities should contractually purchase individual vouchers through Swisscom Trust Services partners or a voucher package (at least 200 registrations) through direct sales. Only voucher customers receive an invoice.

4.2.3 Optional: Installation of the authentication means

Before the installation process is started, the authentication medium that is to be used later for signature approval must be installed. If no authentication medium is installed, the user is forced to use a combination of self-selected password and one-time code via SMS. Otherwise, he can install one of the authentications means offered, e.g. the Mobile ID App, in advance. For example, a fingerprint can then be used instead of a password. It is important that the installation always takes place BEFORE the identification.

4.2.4 Identification process

To start the identification process, the user is now forwarded to the provider. At the same time, the user will also receive the link via the e-mail address provided, under which he or she can start the identification process with the corresponding provider. The links / redirections have expiry dates (see below).The identification process is now carried out according to the instructions on the screen with the external identification provider. If necessary, data must be provided in advance, which is then requested in the process. In some cases, an app from the provider must be installed or the process can be carried out completely in the browser.
During the identification process, attention must be paid to the following topics:

- Depending on the procedure, the user must have the necessary means available, e.g. an adequate camera or an NFC reader, etc.
- When presenting an identification document, the user must always show the correct document (passport or EU/CH ID) and not, for example, a foreigner's residence permit, driver's licence, etc.
- If necessary, wait for the app or the process to transfer the data to Swisscom and do not cancel the process prematurely.

In many situations, you can provide an e-mail address in advance during the identification process. You will then receive an e-mail with a link where a process that may have been interrupted can be resumed.

In principle, an identification service is provided based on the ID documents or data offered and the quality of the equipment used by the user. If, for example, the ID images are washed out or unreadable, or a false ID has been presented, or IDs are not considered sufficiently secure, the registration may be rejected. Payment does not constitute an entitlement to a positive registration, but payment covers the costs of an identification process that has been carried out.

4.2.5 Terms of use

The terms of use of Swisscom Trust Services must be accepted in the process. For acceptance, the authentication means is used for the first time. If the authentication includes a password, the password is set for the first time. Often the terms of use are already displayed and accepted in the process of the external identification provider. If this is not the case, an SMS with the terms of use is sent to the mobile number specified in the registration process.

The link in the SMS must then be opened and the terms of use must be confirmed with the intended means of authentication. If the instructions in the SMS are not followed, the SMS will be sent more frequently within 15 days. If no consent is given after this period, the registration process will be deleted, and the user has to register again.

4.2.6 Signature

The user can only sign with partner signature applications and partner portals after acceptance of the terms of use and delivery of the evidence by the identification provider.
Depending on the procedure used, the registrations have expiry dates, e.g., they may be linked to the expiry date of the ID card or are generally only valid for one year. Before expiry, the user is warned again by SMS that he or she must re-register, provided that the mobile number is known.

4.2.7 Refund

If a fault occurs due to errors in the registration process, there is either the right to a refund in the case of a card payment or the possibility of a replacement voucher if a voucher is used.
Reasons are in particular:

- SMS not received on mobile numbers supplied by mobile operators of the EU, Switzerland and EEA.
- Cancellation of the app or the process due to misconduct
- Process "stuck" for longer than 15 minutes

There is no entitlement to a refund in the case of:

- Use of SIM cards with mobile numbers supplied by mobile providers outside the EU/Switzerland/EEA.
- non-receipt of SMS due to settings or filters on the mobile device
- Cancellation of the process within 15 minutes of an alleged hang-up.
- Use of unauthorised ID or passport documents
- Failure to follow instructions in the process
- Entering incorrect data, e.g., including bank account numbers
- Use of non-NFC-capable terminals for identification with an eID card that requires an NFC procedure.
- Non-acceptance of the terms of use

4.3 Restrictions to identification procedures

For regulatory reasons, the various identification procedures can only be used in their respective jurisdiction and subject to certain conditions, as shown in the overview below.
Only passports and IDs from Schengen countries are permitted for the identification independently from the information to be found in the lists indicated below.
The abbreviations in the column “Jurisdiction” have the following meaning:

- EU: QES: Qualified Electronic Signature: identification procedure approved in the EU according to eIDAS.
- EU: AdES: Advanced Electronic Signature: identification procedure approved in the EU according to eIDAS.
- Switzerland: QES: Qualified Electronic Signature: identification procedure approved in Switzerland according to ZertES.
- Switzerland: AdES: Advanced Electronic Signature: identification procedure approved in Switzerland according to ZertES.

Service variants/option	Jurisdiction	Restriction
SRS own		Project-specific – is defined in the implementation concept
SRS video EU	EU: QES EU: AES CH: AES	Video identification is restricted to certain countries and certain ID types; see **https://trustservices.swisscom.com/downloads** "List of countries for the video identification and POS". Electronic signatures based on the authentication medium “mobile number” can be generated for a maximum period of five years after identification or until the expiry date of the ID document submitted. After that, re-identification is required. Voice and app or browser guidance: at least English and German.
SRS bank DE	EU: QES EU: AES	This requires a bank account with a German e-banking institution. Some banks are not supported, see

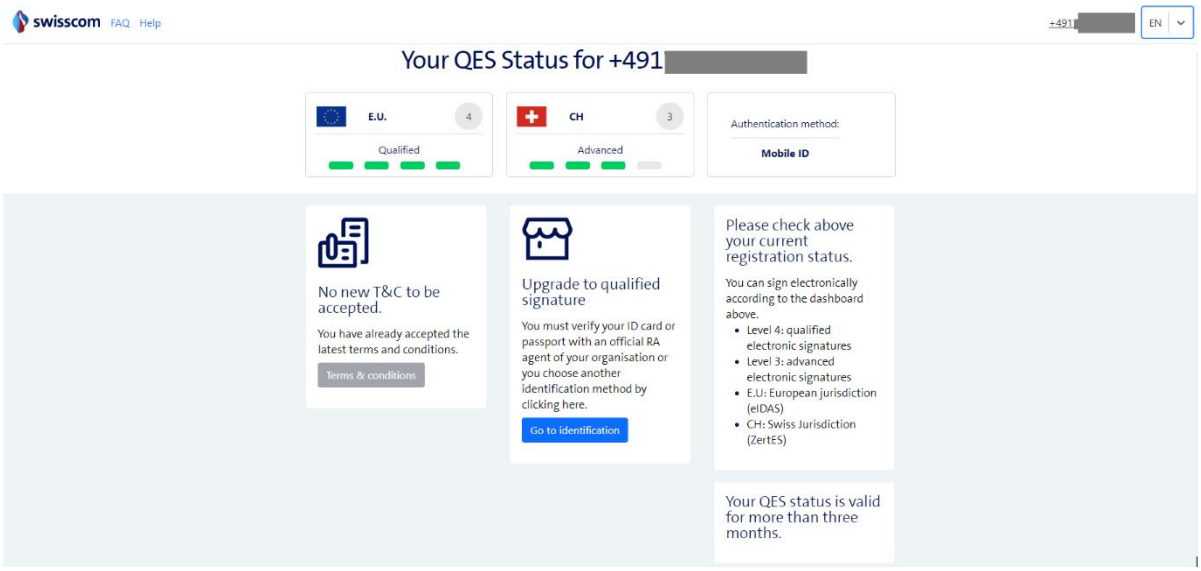
Service variants/option	Jurisdiction	Restriction
	CH: AES	**https://trustservices.swisscom.com/downloads,** "SRS Bank DE/QES Ident". Electronic signatures based on the authentication medium "mobile number" can be generated for a maximum period of two years after identification. After that, re-identification is required. Voice guidance: German.
SRS eID DE	EU: QES EU: AES CH: AES	The prerequisite is the use of the German identity card or an electronic residence permit with eID function authorised in Germany. Electronic signatures based on the authentication medium "mobile number" can be generated for a maximum period of five years after identification or until the expiry date of the ID document submitted. After that, re-identification is required. Voice guidance: at least English and German.
SRS Selfie EU	EU: QES EU: FES CH: FES	The identification is restricted to certain countries and certain ID types; see **https://trustservices.swisscom.com/downloads** "List of countries for the SRS Selfie Ident EU identification". Electronic signatures based on the authentication medium "mobile number" can be generated for a maximum period of five years after identification or until the expiry date of the ID document submitted. After that, re-identification is required. Voice and app guidance: at least English and German.
SRS Video CH	EU: AES CH: QES CH: AES	Video identification is restricted to certain countries and certain ID types; see **https://trustservices.swisscom.com/downloads** "List of countries for the video identification". Electronic signatures based on the authentication medium "mobile number" can be generated for a maximum period of five years after identification or until the expiry date of the ID document submitted. After that, re-identification is required. Voice and app or browser guidance: at least English and German.
SRS Autoident CH	EU: AES CH: QES CH: AES	Autoidentification is restricted to certain countries and certain machine readable ID types; see **https://trustservices.swisscom.com/downloads** "List of countries for the video identification". Electronic signatures based on the authentication medium "mobile number" can be generated for a maximum period of two years after identification or until the expiry date of the ID document submitted. After that, re-identification is required. Voice and app or browser guidance: at least English and German.

4.4 Self-service portals for authentication methods based on mobile numbers

Two self-service portals allow the correct check of the registration status or allow also the acceptance of the terms of use without using the links in the SMS sent out. A second portal allows a test signature to check beforehand if the signature could be authenticated correctly and/or there are some problems. E.g., a change of the mobile device or the SIM card could lead to an error message in case of a Mobile ID authentication due to the fact that the second factor of ownership has changed.

4.4.1 Check of registration status

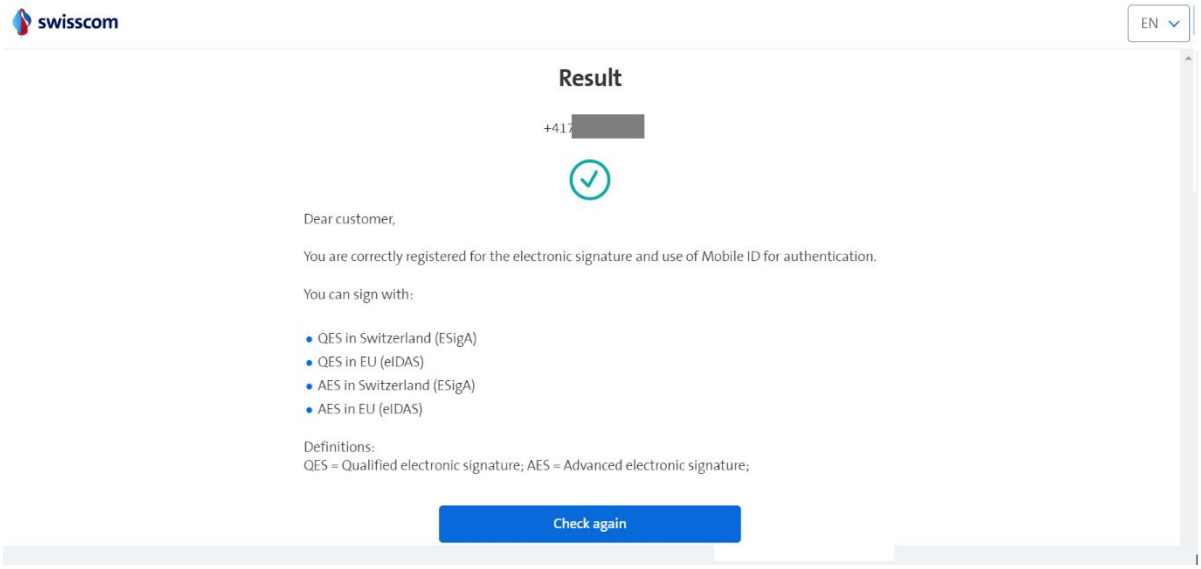
The check of the registration status can be initiated by a call of the following web page:
https://smart-flow.scapp.swisscom.com/



After login by a mobile number which was verified by a one-time code via SMS it will be shown if the registration is valid for a qualified electronic signature (level of assurance factor 4) or an advanced electronic signature (level of assurance factor 3) and if it is valid for the jurisdiction of eIDAS (EU/EWR) or Switzerland (CH). Additionally, you can see the chosen authentication method and the end date of validity. As far as the terms of use are not already accepted or new terms have to be accepted it is possible to accept them by clicking on the button "Terms & Conditions". The web page showing the different registration methods can be reached via the button "Go to identification".

4.4.2 Check the ability to sign

On the web page
https://check-signature.scapp.swisscom.com/
you can check if your authentication method based on a mobile number can be used for a signature. A test signature comprising a text string "hello world" will be signed. Afterwards the result is presented:



4.5 Service Desk

Swisscom provides a service desk (1st level support) for identifications purchased with credit cards. Users who carry out identifications by voucher should contact the site that gave them the vouchers. According to the request, Swisscom resolves the incidents directly with the service points of the identifiers if necessary if no own identification procedure is used.

5 Service provision and responsibilities

Non-recurring services

Activities **(S = STS / User)**	S	User
Service provision		
1. The user can access the appropriate registration on https://srsident.trustservices.swisscom.com and pay by voucher code or credit card		✓

Recurring services

Activities (**S = STS / User**)	S	User
Standard services		
1. Providing and maintaining the service infrastructure and operating access.	✓	
2. Ensuring that the identification procedures are in compliance with the respective types of electronic signature according to the categorisation in Section 4.3.	✓	
3. Selecting the suitable identification procedure that is compatible with the desired electronic signature according to Section 4.		✓
4. Providing and maintaining the interface to the partners selected by Swisscom for performing identification.	✓	
5. Notifying the person to be identified about the identification to be made, the purpose of the identification and the procedure to be followed for identification.	✓	
6. Providing a URL for the person to be identified.	✓	
7. Assuming Responsibility for the identification process after provision of the URL by prompt or user guidance in the appropriate portal and compliance with all regulations for the selected identification procedure, i.e. in particular provision of the necessary means (e.g. camera, NFC access on the mobile device) and the necessary means of identification (account number with account access, correct required ID/passport documents), acceptance of the terms of use, sufficient illumination in the case of video procedures, installation of the necessary identification apps/programs, necessary entries or statements to be entered if asked.		✓
8. Obtaining the evidence data from the external identification partners	✓	
9. Reporting security incidents that affect identification.		✓
10. Ensuring conformity with the chosen signature type and jurisdiction.	✓	
11. Support and coordination of support cases with the respective identification service provider	✓	
12. Inform the support in case of a problem about the order reference, time of identification, identification method and mobile number.		✓
13. Provision of the voucher system and voucher redemption options as well as processing of credit card payments via payment service providers.	✓	
14. Invoicing (by e-mail) to the user	✓	
15. Archiving identification evidence and consent to the terms and conditions of use in accordance with applicable legislation.	✓	
16. Assumption of costs for aborted identifications (e.g. video identification) if this was due to an incorrect process at Swisscom Trust Services, subject to compliance with the user's cooperation obligations.	✓	
17 The user confirms that he or she only uses the service if he or she is permanent resident of Switzerland, an EAA country or EU country.		✓
18. Own communication cost of the user for request of support, e.g. phone cost, SMS cost, etc.		✓
19 The user accepts that he/she is not entitled to registration. This may be refused for reasons of risk. The only compensation here is a refund of the costs he has paid for this registration. Alternatively, Swisscom can also send a voucher for another registration method.		✓

Activities (**S = STS / User**)	S	User
20 Support exclusively by web form or e-mail and attempt to solve the problem by voucher for alternative procedure, or refund. Telephone support, personal support and personal analysis of the respective problem case are not provided.	✓	

6 Service levels and reporting

6.1 Service levels

6.1.1 Validity of the target URL link and count of retries

The links with the redirects to the identification providers, which are sent to the recipient by e-mail after payment, are subject to expiry dates. If the identification has not been redeemed within the time specified below or has been restarted after an error, the identifications must be purchased again. The expiry time is always calculated from the date of purchase and is extended after a failed attempt. There is also a maximum limit of retries, should the identification be faulty.

Service Level	SRS Video EU SRS eID DE	SRS Bank DE	SRS Selfie Ident EU	SRS Video CH	SRS Autoident CH
Validity time in days	90	30	30	90	90
Number of retries	No Limit	5	5	No Limit	No Limit

6.1.2 Validity of voucher codes

Voucher codes are guaranteed to be valid for a maximum period of 18 months. If procedures are no longer available during this period for regulatory or operational reasons, these codes can be refunded at the pro rata price or exchanged for voucher codes of similar identification methods based on a special agreement.

6.1.3 Smart Registration Service

The following service levels generally relate to the agreed monitored operation times. Definitions of terms (Operation Time, Monitored Operation Time, Support Time, Availability, Security and Continuity) and the description of the measurement method and reporting are set out in the contractual element "Base Document".
The following service levels are provided for the service variants (see section 3). If several possible service levels are available for each variant, the service level is selected in the service contract.

Service levels & target values			Smart Registration Service
Operation Time			
Operation Time	Mo-Su	00:00-24:00	●
Provider Maintenance Window	PMW DC	PMW Swisscom data centre	●
	PMW-S: with advance notice for security and system-critical updates	Daily 19:00-07:00, only for announced maintenance	●
Support Time			

Service levels & target values			Smart Registration Service
Support Time [1]	Mo-Fr	08:00-17:00[2]	●
Fault Acceptance	Mo-Su	00:00-24:00	●
Availability			
Service Availability			
• Access to the Smart Registration Service	99.5%		●
Security			
	See base document		●
Continuity			
Service Continuity (STSSC)	Best Effort		●
	RTO 4 h | RPO 1 h		○

● = Standard (included in the price) ○ = For an additional fee

6.1.4 Partner identification service level

The partner identification service level is geared to the SLAs of the involved partners.

Service levels & target values		SRS Video EU SRS eID DE	SRS Bank DE	SRS Selfie Ident EU	SRS Video CH	SRS Autoident CH
SLA Time values						
Operation Time	Mo-Su 00:00-24:00		●	●		
	Mo-Sa 07:00-22:00				●	●
	Mo-Su 07:00-24:00	●				
Support Time	Mo-Fr 08:00-17:00	●	●	●		
Fault Acceptance	Mo-Su 00:00-24:00	●	●	●		
Performance						
Call pick-up rate	80% of calls are picked up within the first 90 seconds, measured on a monthly basis	●	–	–		
	90% of calls are picked up within the first 120 seconds, measured on a monthly basis	●	–	–		

[1] If the Service was purchased via a Swisscom partner, they should generally be contacted in the event of faults. If the partner is not able to rectify the fault, the partner will pass it on to Swisscom.

[2] See holidays definition in the base document

Service levels & target values		SRS Video EU SRS eID DE	SRS Bank DE	SRS Selfie Ident EU	SRS Video CH	SRS Autoident CH
	95% of calls are picked up within the first 180 seconds, measured on a monthly basis	●	–	–		
Processing Time	Maximum processing time from end of identification dialogue until submission of Evidence: 1 minute	–	●	–		
	Maximum processing time from end of identification dialogue until submission of Evidence: 20 minutes	●	–	–		
	Maximum processing time from end of identification dialogue until submission of Evidence: 15 minutes				●	●
	Average processing time for analysis of identification data: 1-2 minutes	–	–	●		
Supported Languages	G=German, E=English, F=French, S=Spanish, I=Italian	E,G,F	E,G	E,G	E,G,F,I	Multiple, minimum E,G,F,I

● = Standard (included in the price) — = Not available

7 Billing

In the case of credit card payment, the user receives a payment receipt including the amount of VAT by e-mail. Voucher customers receive an invoice. The prices result from the price announcements on the website or the order form for the vouchers.

8 Special provisions

8.1 Exchange of identification partners

Swisscom reserves the right to replace the identification partners for the respective services with equivalent partners offering the same process flows as can be found in this service description, provided that the customer has not concluded a parallel contractual relationship with the partner in accordance with 8.2. The partner companies used in each case are named in the order. Any exchange will be announced 3 months in advance. Swisscom reserves the right to offer the same identification service from several partners in parallel.

8.2 Data processing by third parties in Switzerland or abroad, emergency access

The identification data transmitted by the identifiers are archived exclusively on Swisscom servers in Switzerland. Depending on the identification method chosen by the User, identifiers from the EU and Switzerland are enlisted in order to perform the respective identification and mentioned in the service contract. These identifiers are contractually bound to data protection in accordance with GDPR as this pertains to the transfer of data processing.

Swisscom concludes an agreement governing commissioned data processing with external identifiers under the EU General Data Protection Regulation and Swiss Data Protection Act, unless these act independently as data controllers vis-à-vis the person to be identified.

8.3 Identification of persons domiciled outside the EU/EEA/Switzerland

The Smart Registration Service and Swisscom Trust Services are aimed at persons domiciled in the EU, the EEA and Switzerland, as different legal provisions (e.g. consumer protection and data protection law) often apply to persons domiciled outside these regions. It is optionally possible to allow registrations for persons outside the EU, the EEA and Switzerland. This option must be explicitly ordered. The legal possibilities will then be examined and, if necessary, the terms of use or other provisions will be adapted.