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

Service Description
Smart Registration Service (SRS)

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

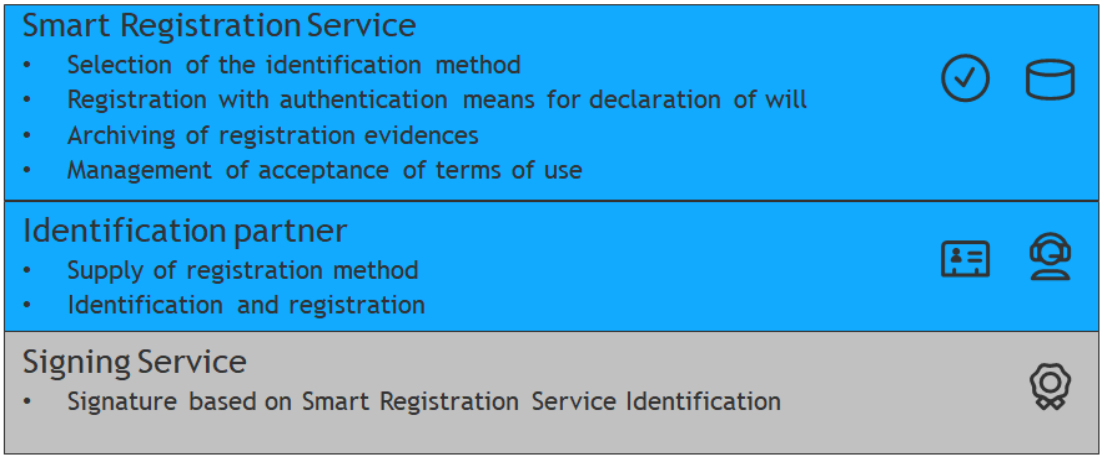
Switzerland

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

1 Content

2 Service overview

The Signing Service and the Smart Registration Service are a 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 identification services (hereinafter "**Smart Registration Service**" or, for the sake of simplicity, “Service” or "SRS") enables a subscriber to provide a subscriber application that allows the choice of one or more identification procedures to be used for the purpose of identifying persons authorised to use electronic signatures with Swisscom’s Signing Service.
The Smart Registration Service is based on the Signing Service and requires that the identified person later also signs using the Signing Service. In order for a person to be able to create an electronic signature, they must always first be identified as part of an identification procedure. In addition to the standard possibilities of the Signing Service, the Smart Registration Service allows subscribers to choose from a variety of other identification procedures to determine the procedures that suit their needs or to use their own identification procedure for the registration process. If the subscriber does not provide its own identification and registration procedure, Swisscom 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.

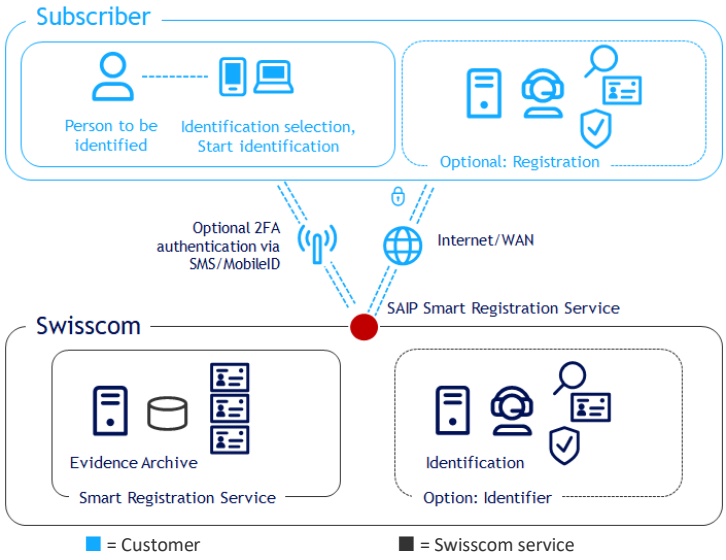


The Service provides the additional option of allowing the subscriber to perform the identification procedure in its own name with the respective identifier. In this case, the collected data are also supplied to Swisscom for the purpose of electronic signature. For example, the subscriber can instruct the identifier to perform the identity check at the same time for the purpose of combating money laundering. This avoids the need to perform multiple identification procedures. This option requires the subscriber to conclude additional contracts and is not the subject of this service description (see Section 8.1).

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 subscriber. It is also the point at which a service is monitored and the provided service level is documented.
The SAIP is the interface that receives requests from the subscriber application and answers them according to the Integration Guide (**https://documents.swisscom.com/product/filestore/lib/9b2c63c5-b3f4-4ff2-be3b-d63e8e77a05b/integration-guide-srs-de.pdf?idxme=pex-search**).
The following purely schematic diagram serves to demonstrate the services and service components of the Smart Registration Service:



The transfer point (SAIP) is the interface between the Smart Registration Service and the subscriber-specific part of the application to start the identification or optionally the transfer of the subscriber's own registration records. Registration via an identifier from Swisscom is performed via 2-factor authentication via SMS/mobile phone. 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 Subscriber.

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 Subscriber 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.

Term	Description
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.
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.
Subscriber	Swisscom provides the services covered by this service description to the subscriber. The subscriber 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.
Subscriber application	The subscriber 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 subscriber 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 subscriber 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 subscriber 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 subscriber 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 Selfie Ident EU: Self identification for EU signatures	○
SRS Video CH: Video identification for Swiss signatures	○
SRS Autoident CH: Auto identification for CH signatures	○
SRS Own: Identification through subscriber's own procedure	○
Restriction of the identification provided only to certain signature application installations ("Claimed IDs") of the Signing Service	○
Advice on integrating the interface and service	○
Use of the Smart Flow Functions	●

● = Standard (included) ○ = For an additional fee

4.1 Definition of service specifications and options

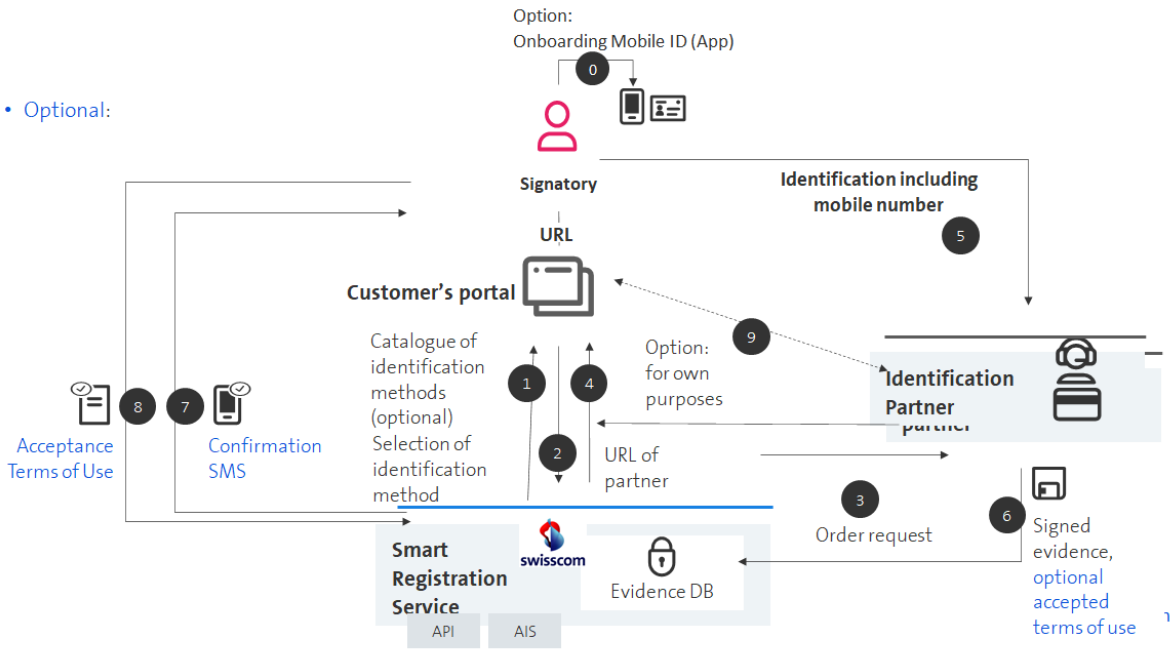
Specification/Option	Definition
SRS Video EU: Video identification for EU signatures	In the case of SRS video EU, the subscriber receives a URL to a website, which it passes on to the person to be identified. The person to be identified can then access the video identification service. For this purpose, 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 subscriber receives a URL which he passes on to the person to be identified. 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 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. • 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 subscriber receives a URL to a website, which it passes on to the person to be identified. 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 a 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.

Specification/Option	Definition
	• 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.
SRS Own: Identification through subscriber's own procedure	The person to be identified is identified by the subscriber's own identification procedure, which feeds the evidence into the Smart Registration Service. Optionally, an SMS containing the terms and conditions of use can then be sent out so that the person to be identified can accept them. An implementation concept is drawn up for the identification procedure used, which describes the procedure and all regulatory requirements. The Smart Registration Service mainly uses the storage of evidence data and optionally the administration of the terms and conditions of use. Depending on the jurisdiction and procedure, it may also be necessary for an audit of the subscriber's own identification procedure by a recognised auditor. It is necessary to sign an additional RA-Delegation Contract.
Restriction of the identification provided only to certain signature application installations ("Claimed IDs") of the Signing Service	Basically, identifications are carried out in such a way that the identified persons can provide signatures everywhere within the scope of the permitted possibilities in which the Signing Service is used. There is the additional option of restricting the signature options for identified persons in case of an own identification (SRS own) so that they are only allowed to sign for a specific signature application (i.e. specific access to the Signing Service).
Advice on integrating the interface	The interface is based on a token-based OAuth protocol. Swisscom can provide consulting services that are charged on the basis of time and effort.
Use of the Smart Flow Functions	The Smart Flow functionalities 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 Process description for identification and registration with procedures offered by Swisscom

The Subscriber 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.



The signatory must decide in advance (0) which authentication method he or she would like to use for registration: If Mobile ID or Mobile ID App is to be used, it must be installed or initialised in advance. Otherwise, the person can use the password - one-time code via SMS procedure.

If the subscriber does not use its own identification procedure, the subscriber submits optionally a request via this interface asking which identification options are available. In the reply from Swisscom, the subscriber receives a catalogue of the connected identification possibilities containing details of the identifier (1), specification of the associated jurisdictions (EU, Switzerland) to which identification is applicable, and further restrictions concerning the respective identification procedure.

The subscriber or the person to be identified now selects an identification procedure (2) and receives a URL (3) of the identification partner in response, which the subscriber can pass on to the person to be identified. This URL will also been sent by email to the person thus he or she is able to retry the identification in case of a failure. The URL can only be used within a validity time frame (see below).

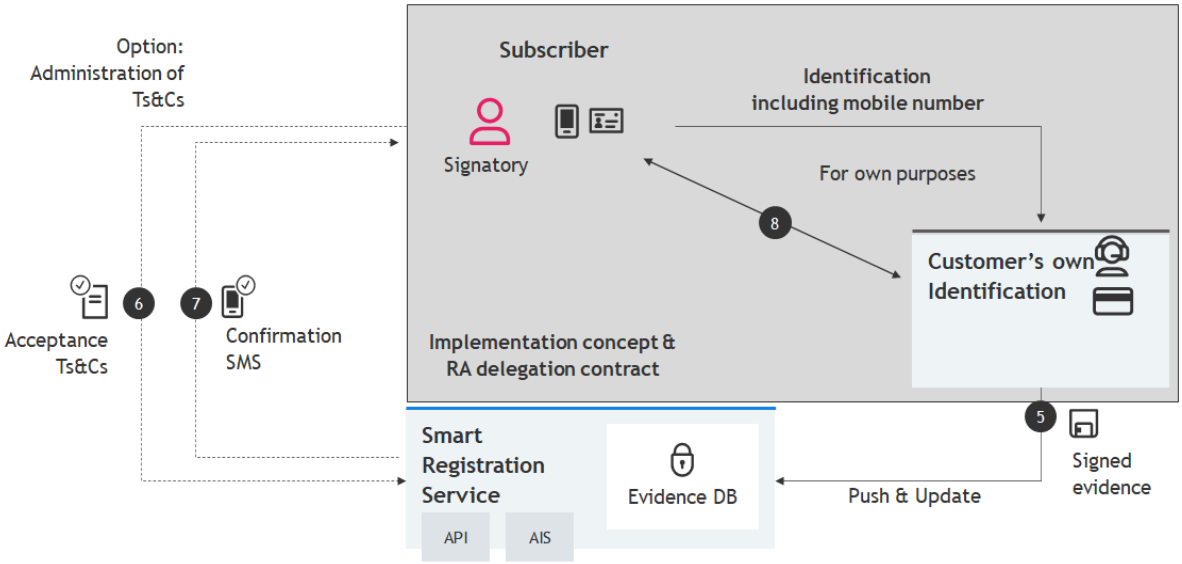
The person to be identified accesses the URL (4) and is directed the identifier's website. They then follow the instructions necessary for identification.

As soon as identification is completed, Swisscom receives the electronically signed evidence and identification data record (hereinafter "Evidence") from the identifier (5) together with the mobile number that will later be used to authenticate and approve the signatures. Unless Swisscom's terms of use were accepted, signed and submitted with the evidence at the same time as the identification process, Swisscom sends an SMS to this mobile number containing a URL to a website that requests the identified person to accept Swisscom's terms and conditions of use for the Swisscom Signature Service (6). As soon as the person to be identified has confirmed its acceptance by "checking the box" on the website (7), Swisscom archives the Evidence in accordance with the obligations to which Swisscom is subject in Switzerland as a certification service and to which Swisscom IT Services Finance S.E. is subject in Austria and Swisscom (Switzerland) Ltd as trusted service provider.

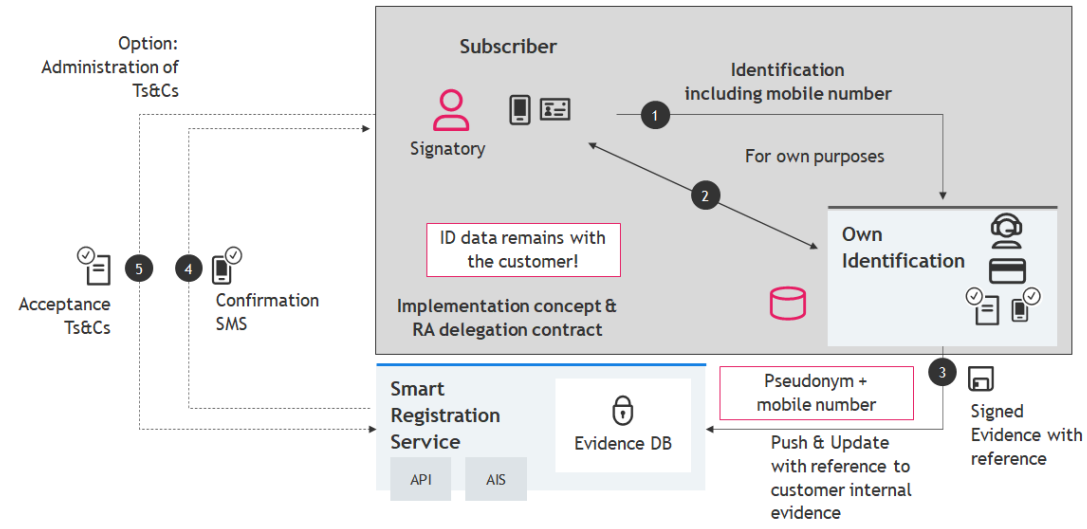
In contrast to the subscriber-specific procedure outlined below, Swisscom's trust service is the responsible registration authority in this case. An implementation concept is not required for this.

4.2.2 Process description for identification and registration with subscriber-specific procedures (SRS own)

In the case of subscriber-specific identification procedures, steps (1) to (4) are omitted and the person to be identified performs identification and registration of the mobile number using the subscriber-specific procedure described in the implementation concept. The subscriber thereby assumes the role of registration authority.



In the case of subscriber-specific identification procedures, the terms and conditions of use can alternatively be managed by the subscriber. The procedure for this is to be described in the implementation concept.
Instead of explicit names, pseudonym data including mobile number can also be transmitted. The subscriber must ensure that the pseudonym data are linked up to the actual identification data. The evidence records then contain a reference to the identification data managed by the subscriber. In the implementation concept, it must be ensured that storage is within the legal retention period.



The advantage here is that the identified person can also use other signature applications that verify identity using the Smart Registration Service; additionally, administration of acceptance of the terms and conditions of use can be outsourced.

4.3 Use of Smart Registration Service identities in the signature process

If a signature is requested from any signature portal in the Signing Service, the Signing Service checks with the Smart Registration Service whether the person has already been validly identified and requests a declaration of intent (authentication) to confirm the signature. This can take the form of confirmation in the MobileID Authenticator App, a MobileID, or a combination of password and One Time Password with SMS (OTP), for example. If the password and OTP are to be used, the password is set for the first time directly after the terms and conditions of use for the Swisscom Signature Service have been confirmed following identification.

4.4 Advance submission of identification data

When selecting and activating an identification method offered by Swisscom, it is possible to provide pre-existing identification data of the person willing to sign, thus facilitating the procedure, since these data only need to be checked using the identification method of the identifier and do not need to be recorded (e.g. mobile number, name, etc.).

4.5 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. The subscriber is responsible for observing these conditions when selecting the identification procedure. The subscriber acknowledges that selecting an identification procedure that is not permissible for the desired electronic signature will result in an error message during the process of creating the electronic signature and will prevent the electronic signature from being created.
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.

All identification procedures can only be offered within the scope of the Smart Registration Service as long as they are also offered by the provider in accordance with regulatory and legal requirements. If the conditions for a regulatory and/or legally correct service provision are no longer met, these options will be terminated by Swisscom Trust Services and removed from the offer, irrespective of the termination period of the Smart Registration Service.

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 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-

Service variants/option	Jurisdiction	Restriction
		identification is required. Voice and app or browser guidance: at least English and German.

4.6 Onboarding process

Provided that the order is correct, the contract for the Smart Registration Service has been concluded and all signed contracts have been submitted to Swisscom, Swisscom technical support will set up access within 10 days. The selected identification types are activated for the Subscriber.

4.7 “Smart Flow” Service Functions

For a more pleasant and better onboarding, Swisscom provides a toolbox "Smart Flow", which supports a person to be identified in their onboarding process and always allows to continue (parts of) the process in case of termination:

- Query onboarding status including approved signature level (advanced/qualified), jurisdiction (EU/Switzerland).
- Query whether the Mobile ID has been reactivated without using the recovery code or whether the password for the Password/SMS code procedure has been changed or the mobile number has been changed (which would result in a "serial mismatch" error message)
- Possibility to access and accept the terms of use directly in the browser flow, i.e., without the need to receive the SMS with the terms of use. This also enables acceptance of new versions of terms of use to be accepted.
- Possibility to receive the link to the terms of use for a specific user based on the MSISDN.
- Access to the Smart Flows interface to design the terms of use acceptance in the own look & feel and to transmit the customer's agreement to Swisscom.
- Polling method to query the signature of the terms of use.

4.7.1 Toolbox (API) and its setup

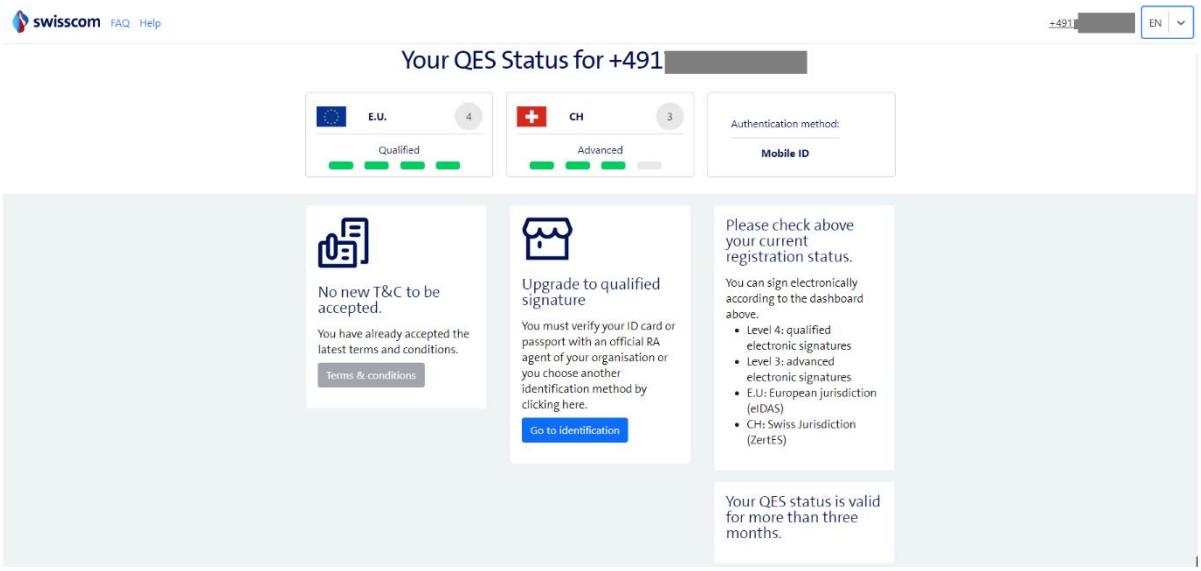
If the subscriber wishes to integrate the functions into his workflow himself, he can also access the individual functions via web components. In addition to the setup, an API key is required.
The following functions are then available:

- Verification of the mobile number
  A one-time code can be sent via SMS to the mobile number of the signatory to check whether it can be received and confirmed by the user.
- Request URL to confirm the terms of use
  This can be done either by displaying the corresponding confirmationpage in the neutral design or in the Smart Flow design with Swisscom logo or in a customised design of the customer. In the case of the solution in the customer's customised design, it is important that the text requesting acceptance of the terms of use is not changed without consulting Swisscom.
- Query on the status of onboarding
  This returns the level of signature capabilities ("LoA" Level of Assurance), the jurisdiction, the expiry of validity (date), or the message that the number is unknown. Errors such as "serial mismatch" in the event of, for example, an exchange of the SIM card during a Mobile ID deployment can also be intercepted.
- Query whether Mobile ID has been installed/initiated ("phone/verification/mobile-id/check") during registration

The subscriber enters a domain name for this and is authorised for this toolbox with API keys during setup. The API documentation is available at https://smart-flow-api-preprod.scapp.swisscom.com/swagger/index.html?urls.primaryName=Admin%20Doc#/ .

4.7.2 Statuspage: Check of the registration status by using the “Smart Flow” functions

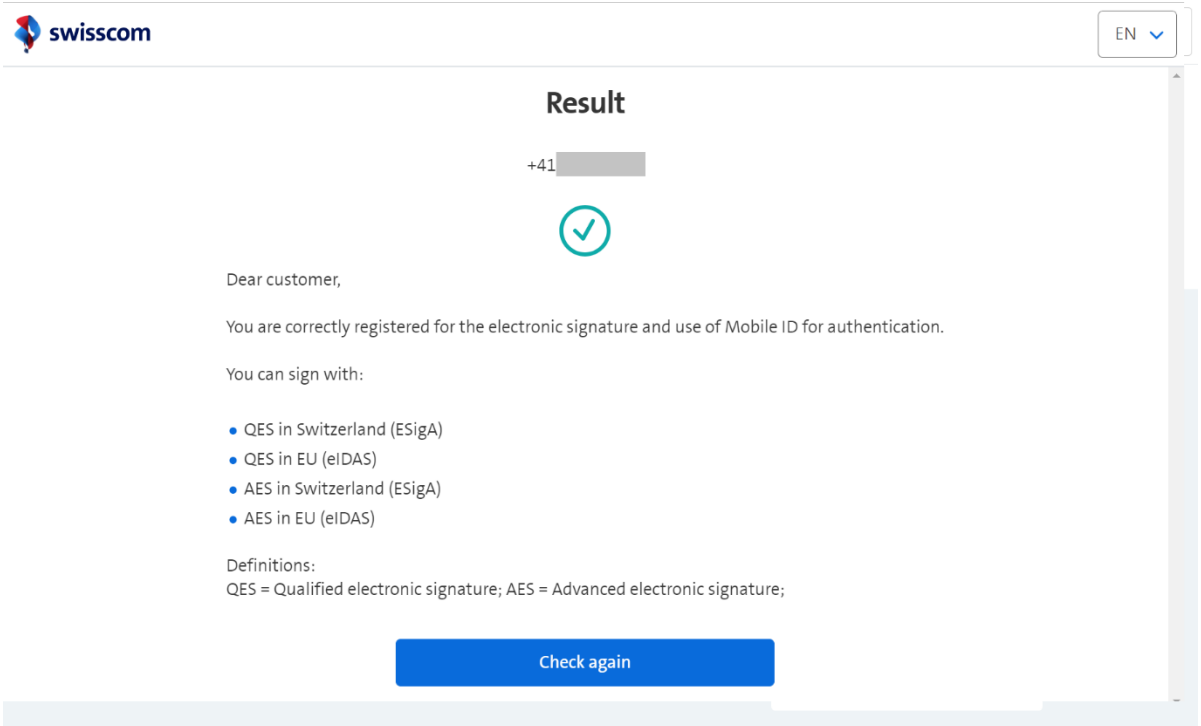
The check of the registration status can directly be done via https://smart-flow.scapp.swisscom.com/



After logging in with a mobile number, which is verified by an SMS with a one-time code to be entered, it is displayed whether the registration for a qualified electronic signature (Level of Assurance Factor 4) or an advanced electronic signature (Level of Assurance Factor 3) is permissible in which legal area (Switzerland = CH, or eIDAS states EU/EEA). The authentication method and the expiry date of the registration are also displayed. If the Terms of Use have not yet been accepted or if they have been updated, they can be accepted here by pressing the button "Terms & conditions". The online identification page can be reached by pressing the button "Go to Identification".

4.7.3 Status Page: Check of signature capability

On the page
https://check-signature.scapp.swisscom.com/
you can check whether a signature can be triggered with an authentication procedure based on a mobile number. For this purpose, a text "Hello World" is to be signed with the authentication procedure for test purposes.
After the signature, the result is displayed:



4.8 Service Desk

Swisscom provides a Service Desk (1st level support) for identifications. 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 / Sb = Subscriber)**	**S**	**Sb**
Service provision		
1. If the Subscriber has commissioned the Swisscom identifier to perform identification on the basis of a separate contract: notification to Swisscom.		✓
2. Activating access to the Smart Registration Service and activating the communication protocol.	✓	
3. Using a Subscriber-specific identification procedure: creating an implementation concept and signing an RA delegation contract; depending on the implementation concept, performance of an audit with an approved auditor.		✓
4. In the case of a subscriber-specific identification procedure, the subscriber provides Evidence (according to the specification in the implementation concept) containing the meta data of the identification and exports this to the database of the Smart Registration Service. The Evidence must be signed, and the public key for signature verification must be made known to Swisscom as a matter of priority in order to activate the supplier.		✓
Termination of the Service		
1. Deleting authorisations and accesses to the Service.	✓	
2. Termination of identification procedures that no longer meet regulatory or legal requirements, or are no longer supported by the provider.	✓	

Recurring services

Activities (**S = STS / Sb = Subscriber**)	**S**	**Sb**
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 4.4.	✓	
3. Selecting the suitable identification procedure that is compatible with the desired electronic signature according to Section 4.4.		✓
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. Creating and activating specific terms and conditions of use for the subscriber which apply in addition to the terms and conditions of use for the Swisscom Signature Service.		✓
7. Providing a URL for the person to be identified.	✓	
8. Assuming responsibility for performing identification of the person to be identified after the URL has been made available by request or user guidance has been provided in the appropriate portal.		✓
9. Unless a subscriber-specific identification procedure is used: notification to the person to be identified that they will be redirected to a portal operated by an identifier (e.g. “By accessing the URL http://xxx you will be redirected to the identification portal of our identification partner, where you can identify yourself”). Obtaining consent as defined by data protection legislation, provided that preliminary data are sent.		✓
10. Triggering identification based on the URL sent.		✓
11. Providing evidence data in the Smart Registration Service when using a Subscriber-specific procedure.		✓
12. Obtaining acceptance of the terms and conditions of use for the Swisscom Signature Service as far as not otherwise agreed in the SRS own implementation concept.	✓	
13. Lifecycle management of the Subscriber’s infrastructure: updating the infrastructure to the current status of technology and security (security patches, updates, etc.) in order to protect the interface.		✓
14. Reporting changes to Subscriber-specific information (contact persons, name of the organisation, etc.).		✓
15. Reporting security incidents that affect identification.		✓
16. Ensuring conformity with the chosen signature type and jurisdiction.	✓	

Activities (**S = STS / Sb = Subscriber**)	S	Sb
17. Including the identification method in the repeat audits.	✓	
18. Maintaining the interface for identification selection and to the identifiers.	✓	
19. Archiving identification evidence and consent to the terms and conditions of use in accordance with applicable legislation.	✓	
20. Providing support and coordination and assigning support cases to the respective identification service provider based on the contract number, order reference, time of identification and identification method used as well as mobile number.	✓	
21. Assuming the costs of aborted identifications (e.g. video identification) and expenses incurred by the identifier in connection with these.	✓	

Recurring services (optional): Smart Flow

Activities (**S = STS / Sb = Subscriber**)	S	Sb
Standard services		
1. Providing and maintaining the Smart Flow service according section 4.7.	✓	
2. Compliance with the obligations to design the communication with the customer regarding the question on the acceptance of the terms of use and the acceptance process: The following sentence, or a sentence agreed with Swisscom in deviation, is displayed in the signature process with the applicant in the national language(s) used in the signature application in form of an opt-in procedure (i.e. e.g. a box to tick): "I have read and agree to the <Terms of Use> <URL-NB-QTSP> of Swisscom." For <Terms of Use> insert in each case: • Terms and Conditions of Use Swisscom ITSF Trust Service for qualified and advanced electronic signatures in the legal area of EU according eIDAS • Terms and Conditions of Use Swisscom Certification Service for qualified and andvanced electronic signatures in the legal area of Switzerland (QES according ZertES) For <URL-NB-QTSP>, the following URL is to be used for the Swiss legal area, depending on the language used: • German: https://w3.swissdigicert.ch/TermsOfUse_Pers_CH-de.pdf • English: https://w3.swissdigicert.ch/TermsOfUse_Pers_CH-en.pdf • French: https://w3.swissdigicert.ch/TermsOfUse_Pers_CH-fr.pdf • Italian: https://w3.swissdigicert.ch/TermsOfUse_Pers_CH-it.pdf For <URL-NB-QTSP>, the following URL is to be used for the EU legal area (eIDAS), depending on the language used: • German: https://w3.swissdigicert.ch/TermsOfUse_Pers_EU-de.pdf • English: https://w3.swissdigicert.ch/TermsOfUse_Pers_EU-en.pdf The signing process with the applicant may only be continued once this box has been ticked; if necessary, the applicant must be explicitly informed of this again.		✓

6 Service levels and reporting

6.1 Service levels

6.1.1 Validity time frame of the URL and retry

The URL 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 Selfie Ident EU	SRS Video CH	SRS Autoident CH
Validity time in days	90	30	90	90

Service Level	SRS Video EU SRS eID DE	SRS Selfie Ident EU	SRS Video CH	SRS Autoident CH
Number of retries	No Limit	5	No Limit	No Limit

6.1.2 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			
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

6.1.3 Partner identification service level

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

[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 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	●	–		
	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,F,I	Multiple, minimum E,G,F,I

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

6.1.4 Support

If the Smart Registration Service was purchased via a Swisscom partner, this partner 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. Subscriber-specific problems and service activations and are handled by 2nd level support, Mon-Fri, during business hours from 8 a.m. to 5 p.m. The public holiday schedule provided in the basic document “SLA definitions” must be observed.

6.2 Service level reporting

Service level report	Smart Registration Service	
Availability, pick-up rate	●	Monthly on request

7 Billing and quantity report

7.1 Billing

Price position	Unit/period
Connection price based on transaction volume per year	Once per month
Registration completed by Swisscom identifier	Price in service contract / registration

7.2 Quantity report

Quantity report Product services/options	Reporting information for billing
Registration completed by Swisscom identifier	Date/time of registration and identification procedure

8 Special provisions

8.1 Service limitations

The identification procedures with the RA app and with the RA Enterprise app as well as identification procedures at points of sale in Swisscom Shops («SRS Direct») are not covered by this service description. If the Subscriber wishes to use these identification procedures, they must be contractually agreed taking into account other service descriptions.
The creation of an implementation concept as well as the performance of an audit and approval for own identification procedures do not form part of this contract. If the Subscriber wants support in this regard, this must be ordered separately within the framework of an Onboarding Support contract.

8.2 Distinction when using the identifiers' identification data for other own purposes

In combination with SRS Video EU, SRS Video CH, SRS Autoident CH and SRS SelfieIdent EU the Subscriber has the option of concluding a contract directly with the identifier with a specific purpose in mind in order to carry out the same identification process and to use the Evidence thus obtained (e.g. within the scope of combating money laundering). In this case, the identification data record created from this contract are made available not only to the Subscriber, but also to Swisscom (Evidence) along with the data relevant for the electronic signature. The process is the same, i.e. the call address (URL) for identification is transmitted by Swisscom to the Subscriber and Swisscom imports the evidence record. The Subscriber can also request the identification data record required for its purposes from the identifier via the reference identification transmitted by Swisscom.
This process requires the conclusion of additional, mutually agreed contracts (between the Subscriber and the identifier, on the one hand, and between the identifier and Swisscom, on the other), which are not the subject of this service description. The identifier must admit that the Subscriber can obtain the data.
If the Subscriber makes use of this possibility and these contracts are concluded:

- the Subscriber is responsible, within the scope of this service description, for submitting terms and conditions of business to its users setting out the construct, together with a transparent data protection regulation.
- The Subscriber is obliged to inform Swisscom of the existence of any contract with an identifier before the Smart Registration Service is activated.

8.3 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.

8.4 Sending preliminary data

If Swisscom's identifiers receive data of the person to be identified in advance when the identification method is accessed, the Subscriber is responsible within the scope of the present service description for submitting terms and conditions of business to its users outlining the advance sending of data to Swisscom and its identification partner, together with a transparent data protection regulation.

8.5 Modification due to regulatory changes

In the event of new or amended regulatory or legal requirements, Swisscom may be forced to make modifications to the Smart Registration Service (e.g. to the identification methods or accesses described in this service description). The Subscriber is also obliged to implement any such modifications to the access protocol or enhanced duties of notification before the change takes effect. Failure to comply with this provision may result in Swisscom restricting or preventing the Subscriber from using the service by deleting the access. Any intervention of this nature on the part of Swisscom shall not constitute a breach of contract.
Due to new or amended regulatory or legal requirements, certain identification methods may no longer be permitted. Swisscom will consequently be required to prevent use of these identification methods and will notify the Subscriber of this in good time, if possible, at least three months before the restriction comes into effect. The Subscriber can then make use of a special right of termination as of the date of entry into force. The deactivation of an identification method required by regulatory or statutory provisions does not constitute a breach of contract by Swisscom.

8.6 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 Subscriber, 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, unless these act independently as data controllers vis-à-vis the person to be identified.

8.7 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.