Service description

Smart Registration Service

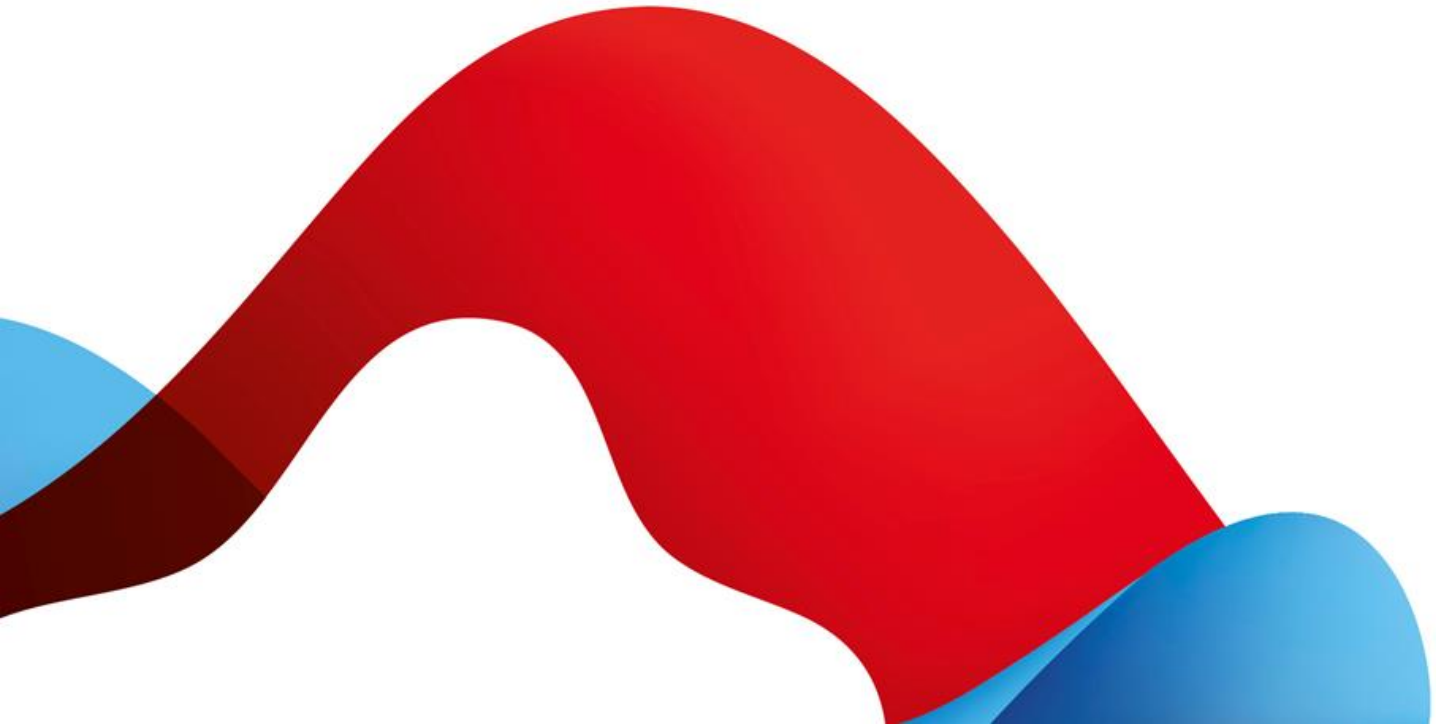


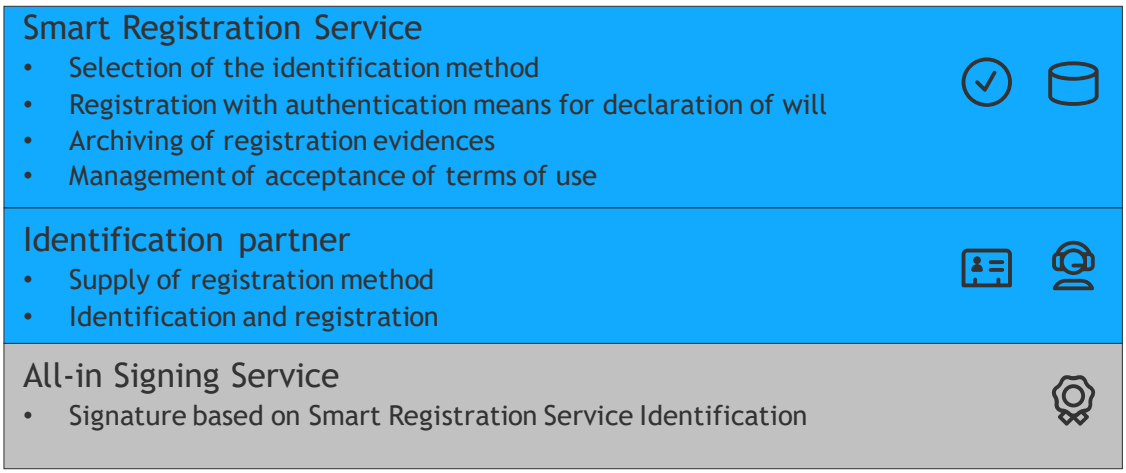
Table of contents

1 Service overview

Swisscom's facility for providing identification services (hereinafter "**Smart Registration Service**" or, for the sake of simplicity, "Service") enables customers to choose one or more identification procedures for the purpose of identifying persons authorised to use electronic signatures with Swisscom's All-in Signing Service (hereinafter "**AIS Service**".

The Smart Registration Service is based on the AIS Service and requires that the identified person later also signs using the AIS 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 AIS Service, the Smart Registration Service allows customers 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 customer 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 (mobile number) verified during the identification procedure and until the validity of the identification expires.



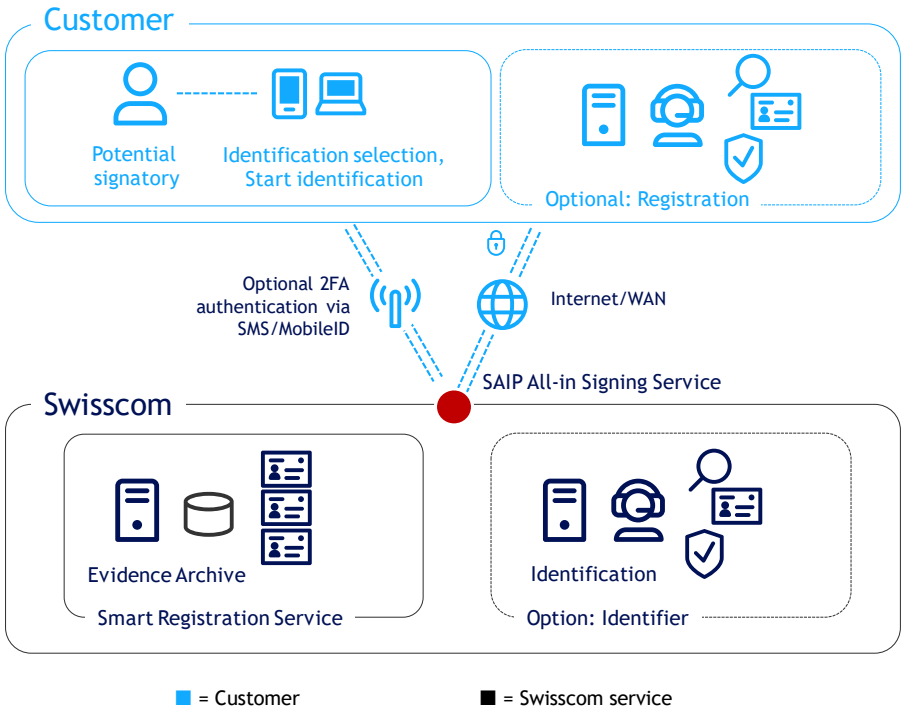
The Service provides the additional option of allowing the customer to perform the identification procedure in its own name with the respective identifier. In this case, the collected data are also supplied to Swisscom for the purpose of electronic signature. For example, the customer can instruct the 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 customer to conclude additional contracts and is not the subject of this service description (see Section 7.1).

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 service user. It is also the point at which a service is monitored and the provided service level is documented.

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 customer-specific part of the application to start the identification or optionally the transfer of the customer'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.

2.2 Service-specific definitions

Term	Description
Advanced Electronic Signature (AdES)	Advanced electronic signature provided by the All-in Signing Service in accordance with Swisscom's certification guidelines or those of Swisscom IT Service Finance S.E.
AIS Service	All-in Signing Service
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 customer does not provide its own identification and registration procedure, Swisscom offers identification and registration through an identification partner, known as an identifier.

Term	Description
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.
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 All-in 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 AIS Service.
Registration Authority (RA)	Authority responsible for identifying the signatories. Under an RA delegation agreement, Swisscom may outsource parts of the registration process to third parties.
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://www.swisscom.ch/de/business/enterprise/angebot/security/digital_certificate_service.html.
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).

3 Variants and options

Standard variant	Smart Registration Service
Identification by identifier:	
Video identification	○
Bank identification	○
Identification through customer's own procedure	○
Restriction of the identification provided only to certain signature application installations ("Claimed IDs") of the All-in Signing Service	○
Advice on integrating the interface and service	○

○ = For an additional fee

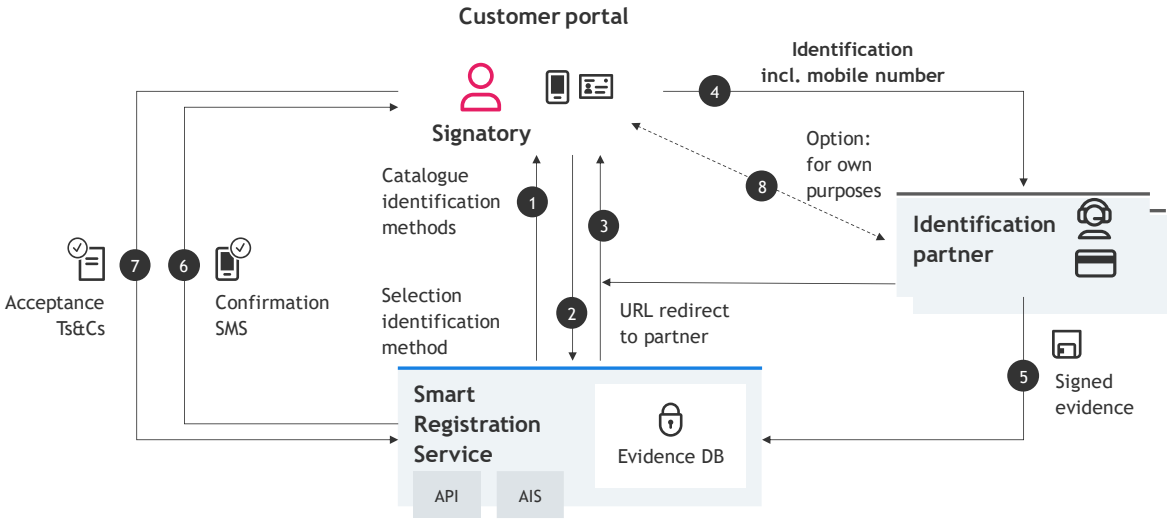
3.1 Definition of service specifications and options

Specification/Option	Definition
Video identification	In the case of video identification, the customer 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. 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.
Bank identification	In the case of bank identification, the customer receives a URL to a website, which it passes on to the person to be identified. The person to be identified now accesses the bank identification service, which first asks for the customer's main bank. The customer then logs into its bank account and confirms the authentication requests made by the bank. After this login, the person to be identified exits their bank account again and is thus identified. The person to be identified now additionally enters their mobile phone number for future declarations of intent connection with the signature. The identification data, mobile number and reference to the bank login process are transmitted to Swisscom. In this case, the identifier keeps the detailed transaction data as delegated registration authority.
Identification by customer's own identification procedure	The person to be identified is identified by the customer'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 customer's own identification procedure by a recognised auditor.
Restriction of the identification provided only to certain signature application installations ("Claimed IDs") of the All-in 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 All-in Signing Service is used. There is the additional option of restricting the signature options for identified persons so that they are only allowed to sign for a specific signature application (i.e. specific access to the All-in 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.

3.2 Procedure for identification and registration

3.2.1 Process description for identification and registration with procedures offered by Swisscom

The customer 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.



If the customer does not use its own identification procedure, the customer submits a request via this interface asking which identification options are available. In the reply from Swisscom, the customer 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 customer now selects an identification procedure (2) and receives a URL (3) in response, which the customer can pass on to the person to be identified.

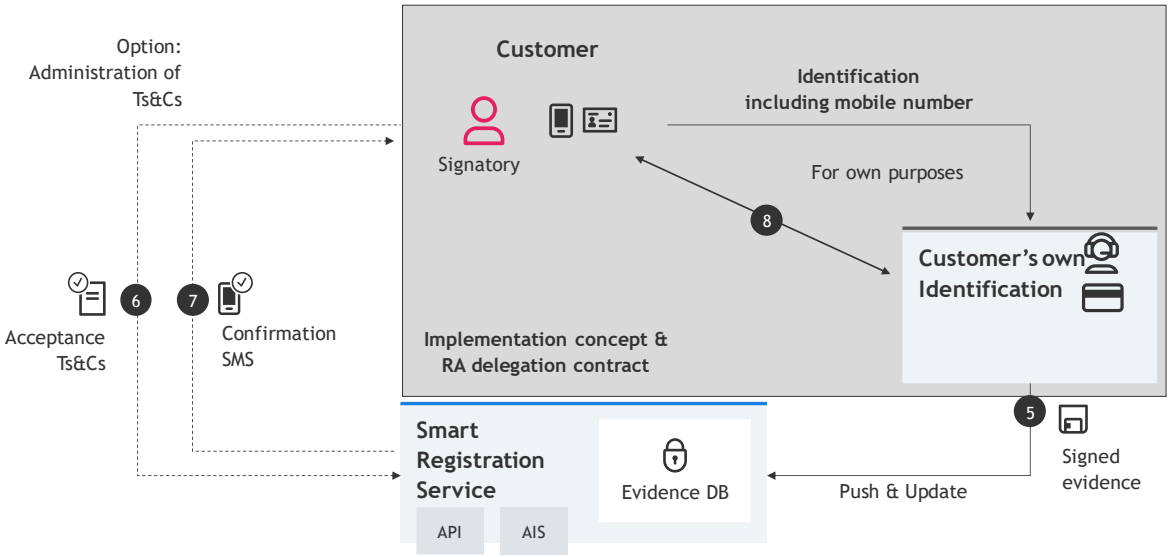
The person to be identified accesses the URL (4) and is directed the identifier's website. They then follow the instructions necessary for identification.

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. Swisscom sends an SMS to this mobile number containing a URL to a website that requests the user to accept Swisscom's terms and conditions of use for the Swisscom Signature Service (6). As soon as the customer 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 as a trusted service provider.

In contrast to the customer-specific procedure outlined below, Swisscom is the responsible registrar in this case. An implementation concept is not required for this.

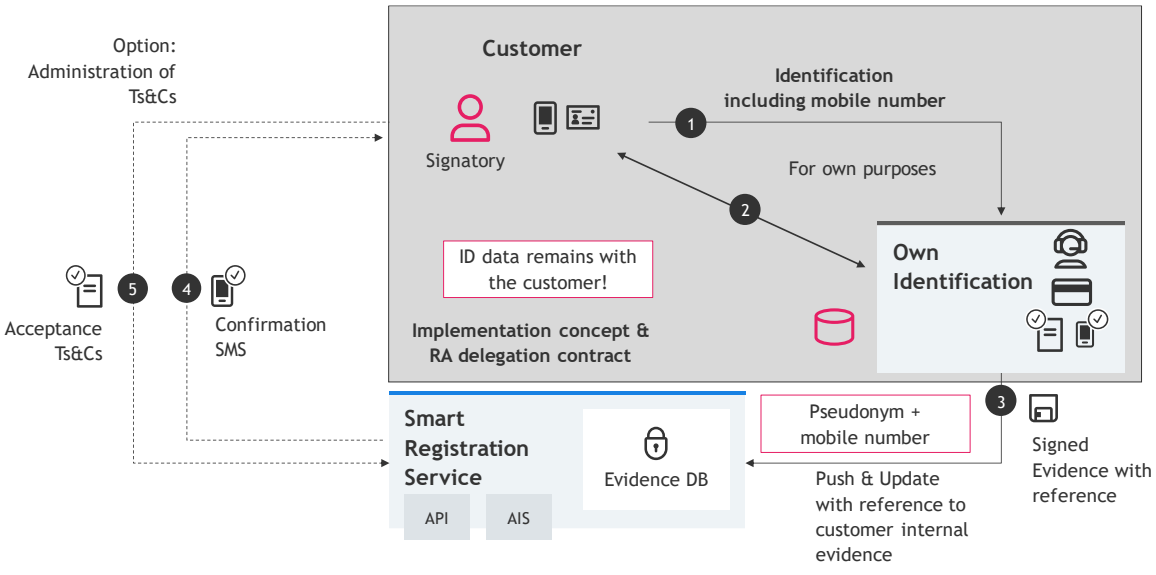
3.2.2 Process description for identification and registration with customer-specific procedures

In the case of customer-specific identification procedures, steps (1) to (4) are omitted and the potential signatory performs identification and registration of the mobile number using the customer-specific procedure described in the implementation concept. The customer thereby assumes the role of registrar.



In the case of customer-specific identification procedures, the terms and conditions of use can alternatively be managed by the customer. 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 customer 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 customer. 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.

3.3 Use of Smart Registration Service identities in the signature process

If a signature is requested from any signature portal in the AIS Service, the AIS 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.

3.4 Advance submission of customer data

When selecting and activating an identification method offered by Swisscom, it is possible to provide pre-existing identification data, 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.).

3.5 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 customer is responsible for observing these conditions when selecting the identification procedure. The customer 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.

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
Own identification procedure		Project-specific – is defined in the implementation concept
EU video identification (VideoIdent by identity.tm)	EU: QES EU: AdES Switzerland: AdES	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 guidance: at least English and German.
Bank identification (KlarnaIdent by KlarnaAB)	EU: QES EU: AdES	This requires a bank account with a German or Austrian banking institution. 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.

3.6 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 customer.

3.7 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.

4 Service provision and responsibilities

Non-recurring services

Activities (S = Swisscom / C = Customer)	S	C
Service provision		
1. If the customer 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 customer-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 customer-specific identification procedure, the customer 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.	✓	

Recurring services

Activities (S = Swisscom / C = Customer)	S	C
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 3.4.	✓	
3. Selecting the suitable identification procedure that is compatible with the desired electronic signature according to Section 3.4.		✓
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 customer 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 customer-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.		✓

Activities (S = Swisscom / C = Customer)	S	C
10. Triggering identification based on the URL sent.		✓
11. Providing evidence data in the Smart Registration Service when using a customer-specific procedure.		✓
12. Obtaining acceptance of the terms and conditions of use for the Swisscom Signature Service.	✓	
13. Lifecycle management of the customer'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 customer-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.	✓	
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.	✓	
21. Assuming the costs of aborted identifications (e.g. video identification) and expenses incurred by the identifier in connection with these.	✓	

5 Service levels and reporting

5.1 Service levels

5.1.1 Smart Registration Service

The following service levels generally relate to the agreed Support Times. Definitions of terms (Operation Time, Support Time, Availability, Security and Continuity) and the description of the measurement procedure and reporting can be found in the other contractual elements (e.g. SLA definitions).

The following service levels are provided for the service variants (see Section 3). If more than one service level is available per variant, the service level is defined 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-Sw: with advance notice for security and system-critical updates	Daily 19:00-07:00, only for announced maintenance	●
Support Time			
Support Time [1]	Mo-Su	00:00-24:00	●
Fault Acceptance	Mo-Su	00:00-24:00	●

[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.

Service levels & target values		Smart Registration Service
Availability		
Service Availability		
▪ Access to the Smart Registration Service	99.5%	●
Security		
	Basic (ITSLB)	●
	Advanced (ITSLA)	●
	Customised (ITSLC)	○
Continuity		
ICT Service Continuity (ICTSC)	Best Effort	●
	RTO 48 h | RPO 24 h	○
ICT Business Continuity (ICTBC) [2]		○

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

5.1.2 Partner identification service level

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

Service levels & target values		Video identification (EU)	Bank identification
Support Time			
Support Time	Mo-Su 00:00-24:00		●
	Mo-Su 07:00-24:00	●	
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	●	–
	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: 1 minute	–	●

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

[2] The AIS Service cannot be combined with the Swisscom ICT Business Continuity Service for a business continuity solution.

5.1.3 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. Customer-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.

5.2 Service level reporting

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

6 Billing and quantity report

6.1 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

6.2 Quantity report

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

7 Special provisions

7.1 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 are not covered by this service description. If the customer wishes to use these identification procedures, they must be contractually agreed taking into account other Swisscom service descriptions (in particular, AIS Service).

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 customer wants support in this regard, this must be ordered separately within the framework of an Onboarding Support contract.

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

The customer 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 customer, 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 customer and Swisscom imports the evidence record. The customer 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 customer 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.

If the customer makes use of this possibility and these contracts are concluded:

- the customer 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 customer is obliged to inform Swisscom of the existence of any contract with an identifier before the Smart Registration Service is activated.

7.3 Sending preliminary data

If Swisscom's identifiers receive data of the person to be identified in advance when the identification method is accessed, the customer 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.

7.4 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 customer 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 customer 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 customer of this in good time, if possible at least three months before the restriction comes into effect. The customer 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.

7.5 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 customer, identifiers from the EU and Switzerland are enlisted in order to perform the respective identification. 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.