As the leading Trust Services provider in Europe, we enable
the most innovative, digital business models.

Service description
Registration and
Signature Approval Methods

Swisscom Trust Services

Swisscom Trust Services Ltd

Konradstrasse 12
8005 Zurich

Switzerland

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

1 Content

1 Content 2
2 Service overview 4
3 Definitions 5
3.1 Service Access Interface Point (SAIP) 5
3.2 Service-specific definitions 6
4 Characteristics and options 10
4.1 Accesses to the registration procedures and/or approval procedures 10
4.2 Registration procedure 10
4.3 Signature approval procedures 13
4.4 Definition of the standard features and options 15
4.5 Procedure for identification and registration 19
4.5.1 General procedure of the registration process 19
4.6 Use of the Swisscom Trust Services registration portal 20
4.6.1 Registration procedure with voucher code or credit card payment 20
4.6.2 Payment 20
4.6.3 Optional: Installation of the signature approval device 20
4.6.4 Identification process 20
4.6.5 Terms of use 21
4.6.6 Signature 21
4.6.7 Refund 21
4.7 Use of the store offer within the framework of the Subscriber applications 22
4.8 Own identification and signature approval procedures 23
4.9 Service Desk 23
5 Performance presentation and responsibilities 24
6 Service Level 31
6.1 Service Level 31
6.1.1 General service level of Swisscom Trust Services for all services 31
6.1.2 Specific SLAs per procedure used 31
6.1.3 Validity of voucher codes 33
7 Invoicing and quantity report 33
8 Special regulations 33
8.1 Data processing by third parties from Switzerland or abroad, emergency accesses 33
8.2 Identification of persons residing outside the EU/EEA/Switzerland 33
8.3 Exchange of methods, deactivation of methods 33
8.4 Delimitation in the use of the identification service providers' identification data for further own purposes 34

2 Service overview

The Smart Registration and Signing Service is a server-based remote signature solution which, after registration and signature approval, enables signatures with signature certificates issued by Swisscom IT Services Finance S.E., Vienna (AT), hereinafter referred to as "Swisscom ITSF", and Swisscom (Switzerland) Ltd and optionally other Certification services. The Smart Registration and Signing Service is provided in the data centres of Swisscom (Switzerland) Ltd in Switzerland and partners in the EU and Swisscom Trust Services Ltd (hereinafter referred to as "Swisscom Trust Services") distributes the Services in its own name or grants third parties the right to distribute the Services in their own name.

The Smart Registration and Signing Service enables the integration of various registration and signature approval procedures, including those of Swisscom companies or third parties, which are described in this service description. Proper registration entitles the signatory to obtain signatures via a subscriber application. This requires the signatory to conclude a contract with a provider of a subscriber application who has integrated Swisscom Trust Services.. The Subscriber Application and its integration into the Remote Signature Solution is described in a separate service description. Swisscom Trust Services does not sell signatures for direct sale to private individuals.

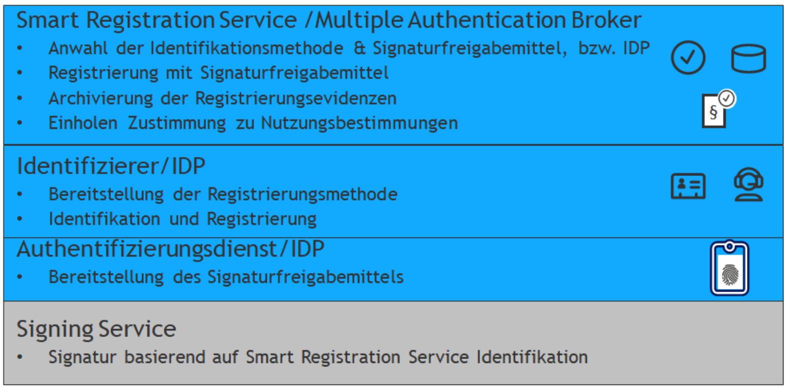
Registration requires a certified signature approval method, which is later used to approve the signature. This can be the Mobile ID App or a combination of password and one-time code via SMS or another signature approval or authentication solution. If an application or hardware token is used, it will usually need to be initialised beforehand. The Multiple Authentication Broker within the Smart Registration Service provides the signer with the appropriate and legally compliant processes for identification or signature approval.

Swisscom Trust Services works with partners to perform the identification and signature approval.

These partners are called "Identification service providers" if they only provide an identification method that can be combined with one or more signature approval methods.

If a user can authenticate with a partner using the identity data managed by this partner and this authentication is later used when signatures are approved, then this partner is referred to as an "IdP" (identity provider). In this case, registration consists only of authentication for the IdP's service and acceptance of the terms and conditions. An example of an IdP could be a bank.

After successful completion of the identification method, the Swisscom Certification and Trust Service archives the identification data for the legally prescribed period - unless otherwise agreed - and manages the acceptance of the Swisscom Certification and Trust Service Terms of Use. The signatories can then create advanced or qualified electronic signatures on the basis of the signature approval means (e.g. app, IdP app, mobile number) checked during the identification method until the validity of the identification expires. By this the user has not to undergo another identification procedure.



Smart Registration Service / Multiple Authentication Broker
- Anwahl der Identifikationsmethode & Signaturfreigabemittel, bzw. IDP
- Registrierung mit Signaturfreigabemittel
- Archivierung der Registrierungsevidenzen
- Einholen Zustimmung zu Nutzungsbestimmungen

Identifizierer/IDP
- Bereitstellung der Registrierungsmethode
- Identifikation und Registrierung

Authentifizierungsdienst/IDP
- Bereitstellung des Signaturfreigabemittels

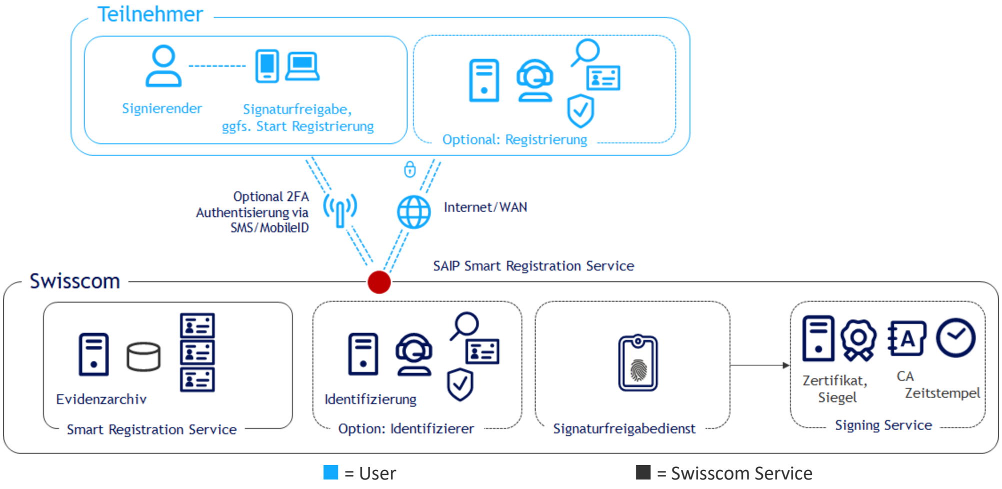
Signing Service
- Signatur basierend auf Smart Registration Service Identifikation

The User of the identification methods and signature approval procedures is either the subscriber who offers them as part of the signature workflow for its signatories or the signatory who uses these methods as part of a Swisscom Trust Services registration portal.

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 provided to the service recipient and User, is monitored and the service levels provided are reported.
The SAIP is either the enrolment portal https://srsident.trustservices.swisscom.com, where the User can select different identification methods, or the Multiple Authentication Broker of the Smart Enrolment Service, where the different signature approval procedures and optionally remote identification methods including registration are made available. The procedures on the registration portal can be paid for and carried out directly or with a voucher code.
Depending on the procedure, the User is then forwarded to the identification service provider, who identifies himself or herself, or to the signature approval service.
The following schematic diagram illustrates the services and service components of the Smart Registration Service:



In the case of the Multiple Authentication Broker, the User first communicates with the Swisscom Smart Registration Service (SRS) via the Internet and is offered various procedures for signature approval. If he is not registered, he is forwarded to the identification service provider. The latter provides the identification data for the Swisscom Certification and/or Trust Service. If SMS or Mobile ID is used for signature approval or registration, it is transmitted to the User's smartphone via the mobile phone interface.
Mobile services used for identification and signature approval and personally installed apps or passkeys and their availability under the private user´s environment on the smartphone or PC are not part of the Service Level Promise. The availability of the service is given when requests are received by the service and responded to correctly according to the interface description in the SAIP Reference Guide. The response may also be a documented error message.
The interface description for the Multiple Authentication Broker can be found at
https://trustservices.swisscom.com/downloads under the Reference Guide link:
https://documents.swisscom.com/product/filestore/lib/e2007490-6fd4-4012-801d-b104801a9abc/reference_guide_smartregistration_signing-en.pdf?idxme=pex-search and in the Multiple Authentication Broker Integration Guide in the Partner Area of the website:
trustservices.swisscom.com/hubfs/Website Files/Documents/Developer Documentation/MAB-IntegrationGuide-en.pdf.
In the past, for approval procedures based on mobile number, the identifications have also been offered on the identification portal and in the RA-App (with own service description).

3.2 Service-specific definitions

Term	Description
2-factor (signature approval)	Qualified electronic signatures offered via remote signatures or qualified/regulated seals must be approved with a signature approval procedure in which the signatory applies 2 factors. These 2 factors must come from the three areas of possession, knowledge and being (biometrics). For example, possession of a mobile number or app on a smartphone combined with knowledge of a password or PIN. Or alternatively, a biometric feature can be used, such as a fingerprint.
Access Token	The Access Token gives a User access to a resource. The token identifies the User to the resource. In the context of signatures, the identification and approval of the signature is done beforehand. The token then issued allows the User to issue and receive approval for a signature request. They are defined in the OAuth 2.0 standard and can also have various properties, such as a limited lifetime.
Audit	Conformity assessment bodies shall audit the conformity of the Certification or Trust Service in relation to the applicable law and standards.
CEN/TS 419 241	CEN is a European committee for standardisation, which published a standard for remote signatures with standard 419 241. This standard standardises the access to a signature and thus also the signature approval method. It is anchored in Swiss signature law and is also required by various supervisory bodies in Europe for the authorisation of remote signature providers.
Certificate	The certificate assigns the public key to a holder, e.g., a signatory or a seal requester. A Certification or Trust Service verifies the owner and signs this assignment itself. The certificate is assigned to a root certificate that belongs to the Certification or Trust Service and is classified as trustworthy in all validations.
Certification service	Term used in the Swiss Signature Act ZertES for the provision of signatures, seals, time stamps including certificates. The Trust Service is the provider of Certification services.
CH	Abbreviation for Switzerland or Swiss legal area.
Claimed ID	The Claimed ID is the access account to the Signing Service of the Swisscom Certification and Trust Service. It consists of a unique identification service provider for the Subscriber (e.g., the URL of his homepage) and the addition of which certificates are used for the signature.
Conformity Assessment Body	Conformity Assessment Bodies are nationally accredited and authorised to audit and certify Certification service providers or Trust Service providers. The report of a conformity assessment body shall be submitted to the Supervisory Body.
Document	For better comprehensibility, the term document is used synonymously with the term data. Both documents and data can be signed.
DSG	Federal Act on Data Protection in Switzerland. The version dated Sept. 1st, 2023 is largely aligned with EU data protection legislation (GDPR).
eIDAS Regulation	Regulation No. 910/2014 of the European Parliament and of the Council of July 23rd, 2014 on electronic identification and Trust Services for electronic transactions in the internal market and repealing Directive 1999/93/EC); also regulates electronic signatures in particular. At the national level, there are typically so-called "implementation laws" which, if necessary, still regulate aspects nationally that were not regulated in the regulation. In Austria, this is the SVG (Signature and Trust Services Act), which regulates, for example, the aspect of the archiving period for data.
Electronic seal	The electronic seal is technically based on exactly the same procedures as the electronic signature. Electronic seals are data in electronic form that are attached to or logically linked with other data in electronic form to ensure their origin and integrity. Under Swiss law, only regulated electronic seals for UID entities are regulated by law, but not advanced electronic seals. In the eIDAS Regulation, both qualified and advanced seals are regulated by law.
Electronic signature	The electronic signature allows the use of a technical procedure to verify the integrity of a document, an electronic message, or other electronic data as well as the identity of the signatory. It makes use of the technical possibilities of a certificate.

Term	Description
ETSI EN 119 432	Protocol from 2021 of the Standardisation Organisation of the European Telecommunications Standards Institute (ETSI) for the connection of a signature application to a remote signature system.
ETSI EN 119 461	European norm for conformity of identification methods used by trust services.
EU	Abbreviation for European Union and thus the legal area of the European Union and the European Economic Area (EEA, i.e., Norway, Liechtenstein, and Iceland).
Evidence	Collection of data that can testify to the proof of a registration and to the identity of a signatory. This proof may also consist of a reference to a data set (evidence) managed by a delegated registration authority.
GDPR	EU General Data Protection Regulation. EU regulation on data protection.
Identification service provider (standard)	Provider of various standard identification methods, e.g., video identification, auto-identification, identification by means of a bank account, by means of an eID or chip information on the identity document.
IdP	Identity provider: An external registration authority that confirms a person's identity, typically through authentication and matching with an identity database. The authentication procedure can later be used for signature approval. In the Smart Registration Service, the IdP communicates with the Multiple Authentication Broker. After registration, the Authentication Broker learns from the RA / evidence database which IdP is responsible for which signatory. If the IdP can rely on already existing identity checks for authentication, which are audited and may be used for the electronic signature, the registration takes place with an initial authentication and acceptance of the terms of use. Example: a bank. However, an IdP can only provide the authentication means as a signature approval method and have this coupled with the results of an identity verifier, too.
Implementation concept	In the case of customer-own identification methods for registration or in the case of the use of customer-own signature approval methods, these methods and other regulatory relevant points must be described in an implementation concept and approved by Swisscom Trust Services. The implementation concept serves as the basis for the audit of these methods.
Key	An electronic signature is initially based on a key pair that is generated in the HSM. Furthermore, a hash is created from the document. This hash is encrypted with the private key so that it can later be decrypted with the public key. The signature check is then carried out in reverse: A hash is again created from the document. The encrypted hash is decrypted with the public key and checked to see if it matches the freshly formed hash of the document. If this is not the case, the document has either been changed or the public key does not match the private key, i.e., the document has been signed by someone else.
Liveness detection	Liveness detection is used to determine that a video session is being conducted by a live person on site and is not faking a person through a pre-recorded video. This is typically done by giving random instructions to the User in the video session to follow.
Mobile ID	Managed service for secure User authentication. Mobile ID can be obtained from various Swiss providers, including Swisscom (Switzerland) Inc.
Mobile ID App	Managed service app (application) that can be downloaded from the Google Play Store or Apple Store for secure User authentication. This is based on authentication capabilities of the mobile device such as fingerprint or face recognition. The Mobile ID App is initialised via an international mobile number and works with a running internet connection.
Multiple Authentication Broker	Based on the logic of the registration authority and its RA database, the Multiple Authentication Broker decides which signature approval method or which external IdP must be addressed for signature approval. It ensures the signature approval - if necessary, by calling a registration for unregistered signers. After signature approval, the broker enables the Subscriber to obtain an access token to request the signature from the signing service.

Term	Description
NFC	Near Field Communication (NFC) is a wireless communication that, for example, a smartphone can establish with an identity document that contains a chip. This allows the ID data to be read directly via a secure protocol by holding the document against the back of the smartphone, where the NFC reader is typically located.
OAuth	OAuth 2.0 stands for Open Authorisation and is a standard that allows a website or application to access resources offered by another service. It is the authoritative industry standard for online authorisation.
One-Shot Signing	In cases user very rarely sign documents it could be better to design a process without signature approval means consisting only of a identification process and signing in one session. The disadvantage is that in future the user must register again for the next signature.
Open ID Connect	Is an authentication layer based on the OAuth 2.0 framework and used to verify the identity of a User with the help of authentication servers, for example via an IdP. The standard is published by the OpenID Foundation.
OTP	One-time code that is transmitted to a mobile device via SMS for easy use. This verifies the "ownership" factor of a mobile device with the specified mobile number.
PAR	Pushed Authentication Request OAuth 2.0 extension describes a technique of initiating an OAuth flow from the backchannel instead of by building a URL, providing better security and more flexibility for building complex authorization requests. The protocol is standardized in RFC 9126.
Person to be identified	Natural person who must be identified in advance to sign a document electronically with authentication and declaration of intent.
Personal signature	Signatures by natural persons as opposed to seals.
PWD	Password (-entry), password to be used for authentication at the service or signature approval, which offers the factor "knowledge".
QR Code	The "Quick Response" code is a two-dimensional code that was developed by the Japanese company Denso Wave in 1994 and is now standard for process triggering on the smartphone.
RA	Registration Authority
RA Agency	Organisation providing the RA agents
RA Agent	Authorised operator of the RA app
RA app	App (application) downloaded from the Android or iOS store. This enables a trained RA agent to identify for advanced and qualified signatures and transmits the data to the RA service of Swisscom Trust Services. The RA agents here act on behalf of the registration office of the Swisscom Certification and Trust Service.
RA-Service	Service for receiving and archiving evidence, operation in connection with the RA App
Recognition Authority	According to ZertES, the recognition authorities are responsible for recognising Certification services. In Switzerland, KPMG is currently the only Recognition Authority. The counterpart in the eIDAS Regulation to this is the supervisory body.
Registration	Registration always consists of identification, acceptance of the terms of use and assignment and verification of a signature approval device.
Registration Authority (RA), RA Authority	Internal or (partly) external delegated body that takes over the registration.
Signatory	Natural person who electronically signs a document with prior identification and signature approval.
Signature approval means or signature approval method	Technically, an authentication means, or method verified during enrolment. It uses One factor (advanced) or two different factors from two of three types (possession, knowledge, biometrics) (qualified) to ensure the identity verified during enrolment. It is used to ensure that the signer has sole access to the key to the signature certificate ("sole control" or SCAL). SCAL2 is used to describe sole access control based on two factors, SCAL1 is used to describe access control

Term	Description
	based on one factor. With the signature approval, the signatory expresses his will to sign. SCAL 1 and SCAL 2 are defined in CEN/TS 419 241.
Signature certificate or seal certificate	Certificate issued to the signatory or seal requester, administered in trust by Swisscom Certification and Trust Services and used for signature or seal creation
Signature level	Variant of electronic signature according to the regulations: advanced electronic signature or qualified electronic signature.
Signing Service	Part of the service that applies the signature, seal, or time stamp to the hash of a document based on the ETSI EN 119 432 standard, provided that the request contains an access token provided by the Smart Registration Service via the Multiple Authentication Broker.
Smart Registration Service	Service from Swisscom Trust Services that controls and manages the signature approval, archives the evidence, and provides information about the signature approval and registration from the RA database. The Smart Registration Service communicates externally via the Multiple Authentication Broker and the import interface of the RA database. Within the scope of the signature, the Smart Registration Service offers the signature approval procedures suitable for regulatory purposes and optionally also the suitable registration procedures, if a signatory is not registered. It makes use of external IdPs and services. For personal signatures, the access token for the signature request at the Signing Service is made available via communication with the Multiple Authentication Broker.
Store (registration methods or signature approval methods)	During the signature workflow, the various regulatory options for signature approval and/or registration can - optionally - be offered within the scope of a webview, if these are not already known in advance. The selection is made in a window ("store") offered by Swisscom Trust Services within the scope of a webview. Alternatively, all methods of the Store can be accessed via the OIDC PAR protocol.
Subscriber	Swisscom Trust Services provides the services in accordance with this service description for the benefit of the Subscriber. The Subscriber is either a direct customer of Swisscom Trust Services with a Signing Service contract (including a declaration of acceptance vis-à-vis Swisscom (Switzerland) Ltd.) or has a commercial contract with a reseller of the Swisscom Trust Services service with a declaration of acceptance vis-à-vis Swisscom (Switzerland) Ltd. If, in the case of seal applications, the Subscriber is not identical with the Seal Requester due to the lack of individual signature approvals, the Subscriber requires authorization by the Seal Requester sending or handing over the access certificate electronically to Swisscom Trust Services or accepting the access certificate authorized by the Subscriber to Swisscom Trust Services.
Subscriber application	The Subscriber gives signatories and signature creators access to an application with which they can create electronic signatures, seals, and time stamps in accordance with the terms of use of Swisscom (Switzerland) Ltd or Swisscom ITSF and, in addition to approval, the Subscriber ensures transmission of the signature data to the remote Signing Service of Swisscom Certification and Trust Services ("Subscriber Application"). The Subscriber Application receives the signed data (hash) and prepares the document for the Signatory. The Smart Registration & Signing Service provides an interface that is connected to a Subscriber Application to trigger the signature. The Subscriber Application is not part of this service description; it is provided outside the Signing Service, e.g. by partners.
Supervisory body	According to the eIDAS Regulation, a supervisory body´s task is to ensure the qualification of the corresponding Trust Services and thus ensure a comparable level of security. It uses the audit report of the conformity assessment bodies for this purpose. The Swiss Signature Act ZertES contains the counterpart of the Recognition Authority.

Term	Description
Terms of Use (Subscriber Agreement)	Provisions that - required by law - every User must accept before cooperating with a trust or Certification service. They do not necessarily have to be signed, but acceptance must be verifiably ensured as part of the registration process. The terms of use regulate the conditions for the use of the signature certificates and signature service in the direct relationship between Swisscom (Switzerland) Ltd and the signatory or Swisscom ITSF and the signatory on a Subscriber application. These are provided at https://trustservices.swisscom.com/repository/..
Token	See Access Token.
Trust Service	Term used in the eIDAS Regulation for the provider of trusted signatures, seals, and time stamps as well as certificates. In the Swiss Signature Act, the term "Certification Service Provider" is used analogously.
URL	Uniform Resource Locator typically refers to the http(s) address called in the browser for a web page.
User	Swisscom Trust Services provides the services in accordance with this service description for the benefit of the User. The User is either a direct customer of Swisscom Trust Services with a Smart Registration & Signing contract (including declaration of acceptance vis-à-vis Swisscom (Switzerland) Ltd.), a voucher contract, a commercial contract with a reseller of Swisscom Trust Services or directly uses the registration portal offered by Swisscom Trust Services on its website.
webauthn	WebAuthn is a standard for a programming interface (API) published by the World Wide Web Consortium (W3C) with the close involvement of the FIDO Alliance as part of the FIDO2 project, with which users of web applications can use direct authentication by means of a public key procedure in the web browser.
Webview	With the help of a webview, a view is shown or embedded in an app/application that displays web content - in this case from Swisscom Trust Services.
ZertES	Swiss Federal Act on Certification Services in the Field of Electronic Signature and Other Applications of Digital Certificates

4 Characteristics and options

4.1 Accesses to the registration procedures and/or approval procedures

The registration procedures are made available via several access points:

Standard version	Offer
Registration portal: The person to be identified visits the website https://srsident.trustservices.swisscom.com and selects the appropriate procedure for registration against redemption of a voucher code or against payment by credit card. The portal solution is described below.	●
Access to Stores: In parallel there is a concept of so-called "stores" where the procedures are offered in the signature flow itself. Based on the customer’s order the selected procedures with which a signatory can register are configured. With the procedures in the store, other signature approval methods can also be used that are not based on the mobile number.	●

● = Standard (included in the price) ○ = Against surcharge

Additionally persons can be registered via the RA app. This is described in a separate service description. The RA app is also used in numerous Swisscom shops and other on-site identification points.

4.2 Registration procedure

All identification and registration procedures are listed in tabular form below:

- Feature: method of the identification
- Partner: Partners of Swisscom Trust Services who provide this service as a delegated Registration Authority of Swisscom Trust Services.

- Valid: Maximum validity period in years (Y). Procedures that rely on identification documents during registration shall determine the maximum validity up to this period of years, or shorter if the identification document presented expires before then. An identity document is considered valid if the date printed on the document documents this validity. Special decrees or laws from some national states, which also declare expired ID cards / passports to be valid, cannot be recognised.
- Legal area for this signature type: Approval of the procedure in use for the Qualified Electronic Signature (QES) or Advanced Electronic Signature (AES) in the legal area of the eIDAS Regulation (EU) or in the legal area of Switzerland (CH).
- Languages: User experience in the languages: D=German, E=English, F=French, I=Italian, PL=Polish

The procedures are offered as follows:

- Via the registration portal on the homepage ("Portal").
- Via the store depending on the order and configuration ("Store").

All identification methods 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. Per ClaimedID different methods can be configured.

Feature	Partner	Valid	Notes	Legal area Languages	Portal / Store
Confirmation of the terms of use	Swisscom (Switzerland) Ltd and Swisscom IT Services Finance S.E., Austria			EU: QES/AES CH: QES/AES EU: D,E CH: D,E,I,F	●
Standard identification service provider					
Video identification, app based	IDNow Gmbh, Germany	5Y	**Via Store:** all signature approval methods in the signature approval store, **via Portal:** Mobile ID, Mobile ID App or PWD/OTP as signature approval only	EU: QES/AES CH: AES D, E, others	○ (Store, Portal)
		Allowed documents under https://go.idnow.de/bafin2017/documents			
eID Identification (Germany), App based	IDNow Gmbh, Germany	5Y	**via Portal:** only Mobile ID, Mobile ID App or PWD/OTP as signature approval	EU: QES/AES CH: AES D, E	○ (Portal)
		Allowed documents: German ID, German Residence Permit and German EU citizen ID card			
Auto- and NFC Identification, browser based	Fidentity AG, Switzerland	2Y	**Via Store:** all signature approval methods in the signature approval store	EU: QES/FES CH: QES/FES D,E,F, others	○ (Store)
		Allowed documents under: https://fidentity.ch/fidentity/wp-content/uploads/2023/11/List-of-allowed-documents-v13_neu.pdf			
Autoidentifikation, browser based	Fidentity AG, Switzerland	2J	**Via Store:** all signature approval methods in the signature approval store	EU: QES/FES CH: QES/FES	○ (Store)

<table>
<tr><th>Feature</th><th>Partner</th><th>Valid</th><th>Notes</th><th>Legal area
Languages</th><th>Portal / Store</th></tr>
<tr><td></td><td></td><td colspan="3">Allowed documents under:
https://fidentity.ch/fidentity/wp-content/uploads/2023/11/List-of-allowed-documents-v13_neu.pdf</td><td></td></tr>
<tr><td rowspan="2">NFC identification, browser based</td><td rowspan="2">Fidentity AG, Switzerland</td><td>2J</td><td><b>Via Store:</b>
all signature approval methods in the signature approval store</td><td>EU: QES/FES
CH: QES/FES</td><td rowspan="2">○
(Store)</td></tr>
<tr><td colspan="3">Allowed documents under:
https://fidentity.ch/fidentity/wp-content/uploads/2023/11/List-of-allowed-documents-v13_neu.pdf</td></tr>
<tr><td rowspan="2">Auto identification, app based</td><td rowspan="2">Nect GmbH, Germany</td><td>2Y</td><td><b>Via Store:</b>
all signature approval methods in the signature approval store
<b>via Portal:</b>
Mobile ID, Mobile ID App or PWD/OTP as signature approval only</td><td>EU: QES/AES
CH: AES
D, E, PL</td><td rowspan="2">○
(Store, Portal)</td></tr>
<tr><td colspan="3">Allowed documents under:
https://nect.com/support/faqcontent/documents/general?</td></tr>
<tr><td rowspan="2">Video identification, app based</td><td rowspan="2">Intrum AG, Switzerland</td><td>5Y</td><td><b>Via Store:</b>
all signature approval methods in the signature approval store,
<b>via Portal:</b>
Mobile ID, Mobile ID App or PWD/OTP as signature approval only</td><td>EU: AES
CH: QES/AES
D, E, F, I</td><td rowspan="2">○
(Store, Portal)</td></tr>
<tr><td colspan="3">Allowed documents under:
https://go.online-ident.ch/swisscomsrsch/documents</td></tr>
<tr><td rowspan="2">Auto identification, app based</td><td rowspan="2">Intrum AG, Switzerland</td><td>2Y</td><td><b>Via Store:</b>
all signature approval methods in the signature approval store,
<b>via Portal:</b>
Mobile ID, Mobile ID App or PWD/OTP as signature approval only</td><td>EU: AES
CH: QES/AES
D, E, F, I</td><td rowspan="2">○
(Store, Portal)</td></tr>
<tr><td colspan="3">Allowed documents under:
https://go.online-ident.ch/swisscomsrsch/documents</td></tr>
<tr><td rowspan="2">Auto Identification, App based</td><td rowspan="2">ti&m AG, Switzerland</td><td>2J</td><td><b>Via Store:</b>
all signature approval methods in the signature approval store</td><td>EU: QES/FES
CH: QES/FES
D, E, F, I</td><td rowspan="2">○
(Store)</td></tr>
<tr><td colspan="3">All ICAO 9303 identity documents admitted for ZertES registration.</td></tr>
<tr><td rowspan="2">NFC Identification, App based</td><td rowspan="2">ti&m AG, Switzerland</td><td>2J</td><td><b>Via Store:</b>
all signature approval methods in the signature approval store</td><td>EU: QES/FES
CH: QES/FES
D, E, F, I</td><td rowspan="2">○
(Store)</td></tr>
<tr><td colspan="3">All ICAO 9303 identity documents admitted for ZertES registration and offering a chip to read out the information, (www.icao.int)</td></tr>
<tr><td>Customer Own Identification</td><td>Customer or service provider of this IDP</td><td colspan="3">Only based on an implementation concept accepted by Swisscom Trust Services and approval of the conformity assessment body and supervisory body. Validity and legal areas will be determined in the implementation concept.</td><td>○
(Store)</td></tr>
<tr><td colspan="6"><b>IdP identifications</b></td></tr>
</table>

Feature	Partner	Valid	Notes	Legal area Languages	Portal / Store
IdP identification with Postfinance App	Postfinance AG, Switzerland	1Y	Only in connection with the signature approval method of Postfinance for Postfinance customers	EU: AES CH: QES/AES D, E, F, I	○ (Store)
Customer Own IdP	Customer or service provider of this IDP	Only based on an implementation concept accepted by Swisscom Trust Services and approval of the conformity assessment body and supervisory body. Validity and legal areas will be determined in the implementation concept.			○ (Store)
Further services					
Use of the Self-Service Portal	Swisscom (Switzerland) Ltd		Mobile ID, Mobile ID App or PWD/OTP as signature approval only	D, E	○ (SRS)
Visualisation of the registration process by store views of Swisscom	Swisscom (Switzerland) Ltd		Views configured and displayed by Swisscom for the selection of ordered and configured registration methods. No prices will be shown.	D, E	○ (Store)
Implementation of subscriber´s own view of the store in own look & feel (UX)	By subscriber		Subscriber specific UX for the visualization of the selected and configured registration methods via OIDC-PAR interface, for example also to be used to display subscriber specific prices	N/A	○ (Store)

● = Standard (included in the price) ○ = Available for an additional charge only in the SRS, only in the Store or in the SRS and Store.

Please note that historic identifications by deprecated SRS Service sold till 2023 still work in combination with the signature approval methods of Mobile ID and PWD/OTP within the broker flow.

4.3 Signature approval procedures

In the following table all signature approval procedures are listed. These must have already been used or checked at least once during registration:

- Feature
- Partner: Partner of Swisscom Trust Services, which provides this service as a delegated signature approval service of Swisscom Certification and Trust Services.
- Legal area for signature type: Approval of the procedure in use for the Qualified Electronic Signature (QES) or Advanced Electronic Signature (AES) in the legal area of the eIDAS Regulation (EU) or in the legal area of Switzerland (CH).
- Languages: UX in the languages: D=German, E=English, F=French, I=Italian

The signature approval procedures are offered in the Store during the signature flow depending on the order and configuration. Per ClaimedID different methods can be configured.

Feature	Partner	Notes	Legal area Languages	Store
Standard signature approval procedure in conjunction with standard identification:				
Password / one-time code via SMS	Swisscom (Switzerland) Ltd	Only in countries with SMS reception and roaming agreement with CH/Germany. Usable with all Store, Portal, Shop and RA-App identificaitons.	EU: QES/AES CH: QES/AES D, E, F, I	○ (Store, Portal, RA-App)
One-time code via SMS	Swisscom (Switzerland) Ltd		EU: AES CH: AES D, E, F, I	○ (Store, Portal)

Feature	Partner	Notes	Legal area Languages	Store
Mobile ID	Swisscom (Switzerland) Ltd		EU: QES/AES CH: QES/AES D, E, F, I	○ (Store, Portal, RA-App)
Mobile ID App	Swisscom (Switzerland) Ltd		EU: QES/AES CH: QES/AES D, E, F, I	○ (Store, Portal, RA-App)
Swisscom Signature Approval App	Swisscom (Switzerland) Ltd	Only in combination with Store identifications	EU: QES/AES CH: QES/AES D, E, F, I	○ (Store)
Passkeys	Android, Apple, Microsoft, yubikey and other FIDO Alliance Members	Only in combination with Store identifications	EU: QES/AES CH: QES/AES All local languages	○ (Store)
Signature Approval SDK	Swisscom (Switzerland) AG in conjunction with Futurae AG	Configurable SDK for an app-controlled signature approval (biometrics/PIN) within the scope of an own app, e.g. for account management in combination with own audited identification methods.	EU: QES/AES CH: QES/AES Language configurable	N/A
Customer Own Signature Approval	Customer or service provider of this IDP	Only based on an implementation concept accepted by Swisscom Trust Services and approval of the conformity assessment body and supervisory body. Validity and legal areas will be determined in the implementation concept.		○ (Store)
Fasttrack Method	Swisscom (Switzerland) Ltd	This method is based on the legal regulation that all Swiss mobile numbers can only be issued after identification of the mobile SIM card subscriber. FES can only be issued within Switzerland; these signatures only contain the mobile number.	CH: FES	○ (Store)
One Shot Signature without signature approval method				
Approval by one of the Store methods listed in chapter 4.2	Corresponding supplier of 4.2	The signature approval is done in the same registration session including the acceptance of the terms of use. The application of a special signature approval method is not necessary. The user is obliged to register again if he/she wants to sign another document.	EU: AES CH: QES/AES D, E, F, I	○ (Store)
Signature approval by the IdP:				
Authentication with the Postfinance app	Postfinance AG, Switzerland	Only in conjunction with registration with the same IdP	EU: AES CH: QES/AES D, E, F, I	○ (Store)
Visualization of the signature approval method selection by store views of Swisscom	Swisscom (Switzerland) Ltd	Views configured and displayed by Swisscom for the selection of ordered and configured signature approval methods. No prices will be shown.	D, E	○ (Store)
Implementation of subscriber´s own view of the signature approval method selection in own look & feel (UX)	By subscriber	Subscriber specific UX for the visualization of the selected and configured signature approval methods via OIDC-PAR and/or CIBA interface, for example also to be used to display subscriber specific prices	N/A	○ (Store)

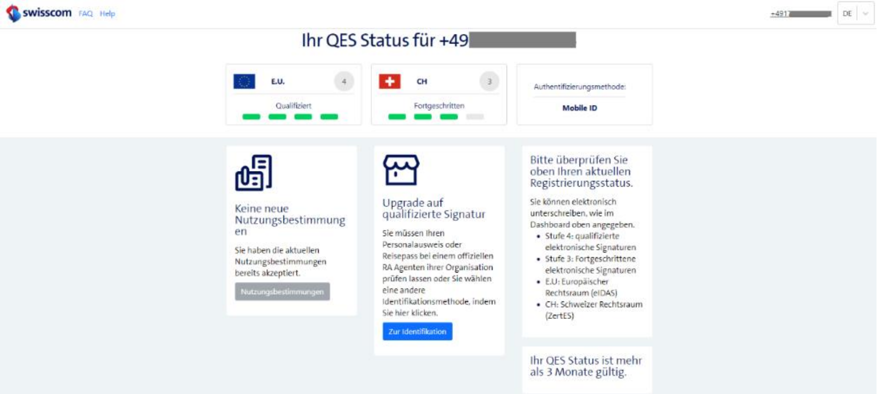
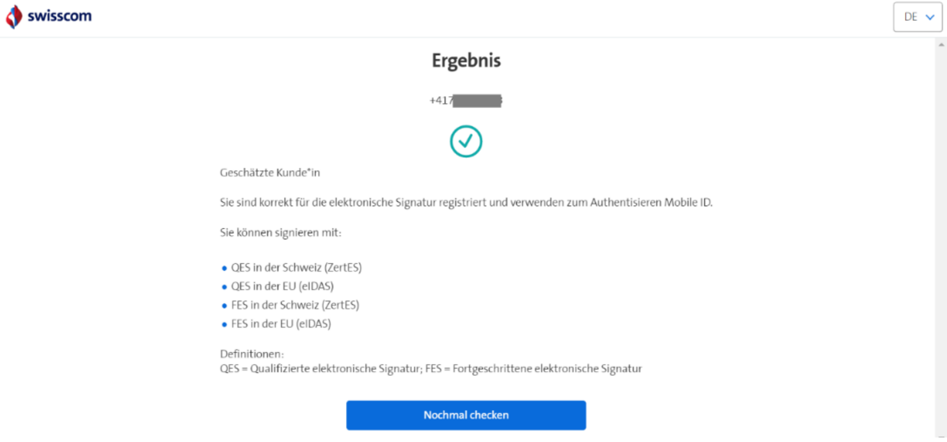
● = Standard (included in the price) ○ = Available in the store for an additional charge.

4.4 Definition of the standard features and options

Possible legally authorized procedures are explained below. Only the procedures named in the order form or contract can be ordered or are offered by an identification service provider at the time of ordering.

Feature	Definition
Acceptance of the terms of use	The terms of use of the Trust Services must be confirmed prior to registration. The signatory shall accept the terms of use of Swisscom (Switzerland) Ltd. and/or Swisscom IT Services Finance S.E. for one or both jurisdictions. The terms of use apply in each case to both advanced and qualified electronic signatures. The confirmation of the terms of use takes place: • Either in the registration process itself, where the corresponding terms of use are displayed and must be confirmed with ticks. For this purpose, Swisscom Trust Services or its identification partner offers a "webview" that a Subscriber application can embed in its workflow. • Or in case of portal or RA-App registration after registration by sending an SMS with a URL to a website where the confirmation must take place. This SMS is sent out by Swisscom Trust Services after the registration evidence has been submitted and no terms of use have been confirmed beforehand. • Or in the self-service portal https://smart-flow.trustservices.swisscom.com/ where the terms of use for mobile number-based signature approval procedures can be checked after verifying the mobile number.
Video identification, app based	With video identification, the User receives a URL to a website and a reference to an app (QR code) to download and install on their smartphone. With the app installed, the User accepts another QR code on the website or enters the specified parameters to start the identification process. If necessary, additional information (e.g., name) must be entered beforehand. The video identification service then starts, with an operator visibly guiding the User through the process in a dialogue. This requires a smartphone with a camera. During a web session, the person to be identified must show his or her ID card under the guidance of a video identification operator and answer questions to confirm the ID card data and prove that he or she is alive. The data obtained in this way is then transmitted to Swisscom's Certification and Trust Service.
eID identification, app based	The User receives a URL to a website where he or she is asked to install and use an app on his or her Android or Apple smartphone with which the following steps have been carried out: • Photo of the front and back of the German identity card or an electronic German residence title/eID card with eID function • The ID card is held up to the NFC interface of the smartphone and the chip information of the ID document is read via NFC. • The mobile number is confirmed by means of a one-time password, which is transferred by SMS. The result data set of the identity check is then made available to the Swisscom Certification and Trust Service.
Auto identification, app based	The person to be identified is redirected to a website and must first download and install an app for auto-identification and follow the app's instructions: • The front and, if applicable, the back of the authorised ID document must first be captured with the smartphone's rear camera. • The identity document must be tilted and moved in such a way that all optical security features (e.g., holograms) can be recognised in the light. • The photo of the ID card is compared with a self-taken picture of the person to be signed using the front camera. • Liveness detection takes place, for example, by speaking two predefined random words in a video recording or by demanding a certain movement. • The verification of the identification data takes place in the background with the help of AI algorithms (duration up to 15 minutes). The result data set is then transmitted to the Swisscom certification and trust service. As there is no personal user guidance, the user is responsible for showing the correct credentials, a passport or ID document according to the country list displayed at the time of purchase. (e.g., no driving license). Furthermore, sufficient illumination and sharpness of the lens is necessary. For example, driver licenses are not sufficient to get registered for a QES.
NFC identification, app based	Works like the app-based auto-identification described above with the following differences:

Feature	Definition
	• Instead of the ID card check (e.g. hologram etc.), the NFC chip of the ID card is read. The ID card is held over the NFC reader of the smartphone for a few seconds so that all information can be read. • The manual background check can generally be omitted, thus shortening the process.
Auto- and NFC Identification, browser based	The person to be identified is redirected to a session on the smartphone browser and must follow the steps within this smartphone browser session: • A QR code must be scanned by the smartphone camera and a browser based session on the smartphone will be started. • In case a chip based identification document is used and the method supports NFC identification a NFC browser extension will be installed. In this case the document must be placed on the back of the smartphone to read out all chip data via NFC • Otherwise, if NFC is not possible, the front and, if applicable, the back of the authorized ID document must first be captured with the smartphone's rear camera. ○ During this process, the identity document must be tilted and moved in such a way that all optical security features (e.g., holograms) can be recognised in the light. • The photo of the ID card is compared with a self-taken picture of the person to be signed using the front camera. • Liveness detection takes place, for example, by demanding a certain movement. • In case NFC was not applicable the verification of the identification data takes place in the background with the help of AI algorithms (duration up to 15 minutes). The result data set is then transmitted to the Swisscom certification and trust service. As there is no personal user guidance, the user is responsible for showing the correct credentials, a passport or ID document according to the country list displayed at the time of purchase. (e.g., no driving license). Furthermore, sufficient illumination and sharpness of the lens is necessary.
Customers' own IdP	Customers' own IdPs managing user data that has already been sufficiently identified in accordance with the signature legislation can be included in the store. It could exclusively be used for the customer's own signature operation, or it can be offered to other signature services (for a fee). The underlying identification must fulfil the requirements of EN 119 461. Proof that a person has been registered with an IdP is always provided by the means of authentication issued by the IdP. The means of authentication is therefore also the only way to approve signatures and must fulfil the requirements of the CEN/TS 419 241 standard.
Customers' own Identification	Customers' own identification methods, e.g., other auto or video identification methods, can be integrated into the broker flow, provided they are conformity assessed. For this purpose, they must fulfil the requirements of EN 119 461. The identification method can be combined with other standard methods for signature approval or Customer's own signature approval method. It could exclusively be used for the customer's own signature operation, or it can be offered to other signature services (for a fee).
Use of the Self-Service Portal	The Self-Service Portal is particularly suitable for Users of the registration portal and the Smart Registration Service who have carried out their registration offline and would like to be sure before signing whether the registration has proceeded properly or whether they are capable of signing. It is currently operated by Swisscom but could be outsourced to a Swisscom partner in future. **Checking the registration status** The Self-Service Portal enables 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 on this portal in case e.g., a SMS did not arrive properly with the Terms of Use links. The portal can be accessed at: https://smart-flow.trustservices.swisscom.com/

Feature	Definition
	 swisscom FAQ Help +4917[redacted] DE Ihr QES Status für +49[redacted] E.U. 4 Qualifiziert CH 3 Fortgeschritten Authentifizierungsmethode: Mobile ID Keine neue Nutzungsbestimmungen Sie haben die aktuellen Nutzungsbestimmungen bereits akzeptiert. Nutzungsbestimmungen Upgrade auf qualifizierte Signatur Sie müssen Ihren Personalausweis oder Reisepass bei einem offiziellen RA Agenten ihrer Organisation prüfen lassen oder Sie wählen eine andere Identifikationsmethode, indem Sie hier klicken. Zur Identifikation Bitte überprüfen Sie oben Ihren aktuellen Registrierungsstatus. Sie können elektronisch unterschreiben, wie im Dashboard oben angegeben. • Stufe 4: qualifizierte elektronische Signaturen • Stufe 3: Fortgeschrittene elektronische Signaturen • E.U: Europäischer Rechtsraum (eIDAS) • CH: Schweizer Rechtsraum (ZertES) Ihr QES Status ist mehr als 3 Monate gültig. 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 jurisdiction (Switzerland = CH, or eIDAS states EU/EEA). In addition, the signature approval method is displayed and the expiry date of the validity of the registration. If the terms of use have not yet been accepted or if they have been updated, they can be accepted by pressing the button "Terms of use". The online identification page can be reached by clicking on the button "For identification". **Verification of the signature capability** In addition, a second portal can be used to check whether a signature is possible: https://check-signature.scapp.swisscom.com/ For this purpose, a text "Hello World" is to be signed with the register signature approval procedure for test purposes. After the signature, the result is displayed:  swisscom DE Ergebnis +417[redacted] Geschätzte Kunde*in Sie sind korrekt für die elektronische Signatur registriert und verwenden zum Authentisieren Mobile ID. Sie können signieren mit: • QES in der Schweiz (ZertES) • QES in der EU (eIDAS) • FES in der Schweiz (ZertES) • FES in der EU (eIDAS) Definitionen: QES = Qualifizierte elektronische Signatur; FES = Fortgeschrittene elektronische Signatur Nochmal checken The use of the portals is free of charge.
IdP identifications	Different IdPs allow registration with their own applications and accesses. Users must first authenticate to the IdP's own application or logins and confirm that they are registered with the IdP. Depending on the type of registration, the User may be denied access to the signature service (e.g., if identification has been carried out correctly according to the Banking Act, but the identification document is not sufficient according to the Signature Act). I.e., the user is analysed by the IdP, matched and filtered out if necessary. If the signature is possible, the User must confirm the terms and conditions of use of the relevant Swisscom Certification or Trust Service and can then approve signatures with an authentication or approval set up for this purpose at the IdP. The use of other signature approval methods is then generally not possible with an IdP registration.
Visualization of the registration process in the store with Swisscom Views	For quick integration of the registration method selection inside a browser flow, Swisscom offers views with the Swisscom logo and its own UX design for selecting the appropriate registration method. In the web-guided browser flow, the signatory is then shown a page hosted on a Swisscom system with the Swisscom look and feel. No prices for the different registration methods are displayed here, i.e., the person ordering the services receives an invoice according to the order, depending on the identification method selected by the customer. Only those procedures are displayed that the person ordering the service has ordered and that make sense

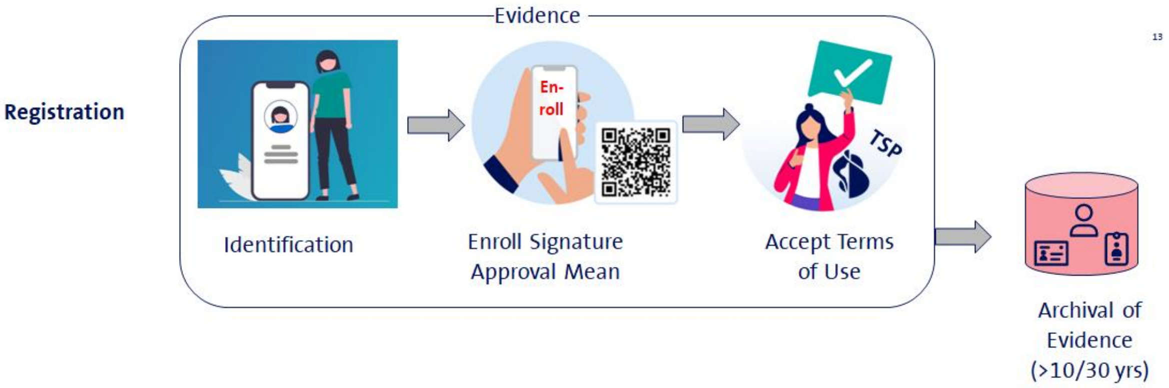
Feature	Definition
	for the signature order (e.g., advanced, or qualified, jurisdiction EU or Switzerland). Individual icons show the different procedures and offer further information via help symbols (e.g., type of procedure, etc.). The jurisdiction for which the procedure is applicable is also displayed.
Integration of the store's registration methods in its own look & feel (UX)	If the subscriber-specific UX is to be used for the selection of registration methods and, for example, additional information is to be placed on the individual procedures, such as different price information, the OIDC-PAR interface is a good way of integrating the available and ordered procedures. This requires integration effort on the part of the subscriber application as well as testing effort on both sides.
Password / one-time code via SMS	Password (-entry), password to be used for authentication at the service or signature approval, which offers the factor "knowledge". This password entry is combined with a one-time code that is transmitted to a mobile device via SMS for easy use. This verifies the "ownership" factor of a mobile device with the specified mobile number.
One-time code via SMS	One-time code that is transmitted to a mobile device via SMS for easy use. This verifies the "possession" factor of a mobile device with the specified mobile number. Thus, only one factor is checked - the procedure is accordingly only usable for advanced electronic signatures.
Mobile ID	Managed service for secure User authentication based on a push message and PIN entry. Mobile ID can be obtained from various mobile phone providers in Switzerland, including Swisscom (Schweiz) AG, for Swiss SIM cards. It requires an SMS for initialization. See https://mobileid.ch
Mobile ID App	Managed service app (application) that can be downloaded from the Google Play Store or Apple Store for secure User authentication. This is based on authentication capabilities of the mobile device such as fingerprint or face recognition. The Mobile ID App is initialized via an international mobile number by SMS and works with a running internet connection. https://mobileid.ch
Swisscom Signature Approval App	App in the Google or Apple Store for the smartphone, which enables signature approval with biometric features (e.g., fingerprint or face recognition) and has a 6-digit PIN as a fallback solution. This signature approval device is not linked to a mobile number nor SIM card and therefore does not depend on the receipt of an SMS.
Passkeys	Passkeys are an extension of the FIDO standard for 2-factor authentication, which is typically also used by web services for logging in. These are pairs of private and public keys that are stored on the respective device and are also synchronized in the respective environment on multiple devices within an Android/Apple or Windows environment. Typically, the method to unlock the screen (e.g. fingerprint, face recognition or PIN) is also used to authenticate by passkey. Alternatively, FIDO2-compatible USB or NFC sticks via WebAuthn API can also be used. This makes it possible to approve signatures independently of a mobile number or even a smartphone.
Signature approval SDK	Software development kit for the use of the signature approval options of the signature approval app within the framework of an own app. This means that signature approval can be integrated into a customer's own app with only small audit costs, as the corresponding approval process is basically audited and runs on Swisscom systems integrated in the customer app. A usage concept must be elaborated together with Swisscom Trust Services and the concept must be approved by the conformity assessment body.
Fasttrack method	The Fasttrack method refers to signature approval without prior registration with Swisscom Trust Services. This is based on Swiss legislation, which obliges subscribers to mobile phone services to identify themselves in advance. The mobile phone providers store the subscriber data behind a mobile phone number. As part of the Fasttrack procedure, no further identification or registration is necessary, and the signature can be authorized directly by means of a one-time code sent by SMS to a mobile number registered in Switzerland. Only advanced electronic signatures can be issued because of this procedure and the certificate for these signatures only contains the mobile number as the verified date and the country Switzerland.
Customer's own signature approval method	In addition to customer signature approvals that are based on the signature approval SDK, other customer signature approval means that do not use the SDK can also be integrated into the signature flow. The method can either only be used for the customer's own signature operation or it can also be offered to other signature services (for a fee). The underlying approval method (authentication) must fulfil the requirements of CEN/TS 419 241.
Authentication with Postfinance App	The login to the Postfinance eBanking app can be used to approve a signature. See IdP Identifications.
Approval by one of the Store methods	The so-called one-shot signature enables signature approval without installation, initialization and use of a signature approval means. Identification and signature approval (an "OK" button is

Feature	Definition
listed in chapter 4.2	sufficient for this) with the signature takes place in a session that is initiated by the broker. All store methods from chapter 4.2 can be used for this.
Display of signature approval procedures in the store with Swisscom Views	For quick integration of the registration and signature approval method selection, Swisscom offers views with Swisscom logo and UX design for selecting the appropriate signature approval method. In the web-guided browser flow, the signatory is then shown a page hosted on a Swisscom system with the Swisscom look and feel. No prices are displayed for the different procedures, i.e., the party ordering the services receives an invoice according to the selected signature approval method, if fees are charged for the procedure at all. Only those procedures are displayed in a decision-based way that the party ordering the service has ordered and that make sense for the signature order (e.g., advanced, or qualified, jurisdiction EU or Switzerland). Individual icons show the different procedures and offer further information via help symbols (e.g., type of procedure, etc.). The jurisdiction for which the procedure is applicable is also displayed.
Integration of the store's signature approval methods in its own look & feel (UX)	If the subscriber-specific UX is to be used for the selection of signature approval methods and, for example, additional information on the individual procedures is to be placed, such as different price information, the OIDC-PAR interface is suitable for integrating the available and ordered procedures. QR Code elements could be integrated via the OpenID Connect Client Initiated Backchannel Authentication Flow (OIDC CIBA). This requires integration effort on the part of the participant application as well as testing effort on both sides.

4.5 Procedure for identification and registration

4.5.1 General procedure of the registration process

Registration is either offered to Subscribers as part of the Subscriber application offering and embedded in the workflow of the signature application. Additionally, Signatories also have the option of registering directly online using payment via credit card or voucher code on the Swisscom Trust Services website.
https://srsident.trustservices.swisscom.com
to carry out the registration.



Registration always consists of the following steps:

- A signature approval medium/procedure must be selected and, if necessary, installed in advance, e.g. the Mobile ID App. The possible signature approval means and procedures are to be selected from the offer above. Not every registration procedure works with all signature approval methods. An IdP, such as a bank, will usually only allow its own signature approval app.
- The terms of use of the respective Swisscom Certification service or Trust Service must be accepted. This is done either during registration or afterwards by sending an SMS with a link to a website with the terms of use.
- The signature approval means must be used for the first time, i.e., you must prove that you have a signature approval method or that you own the mobile phone number. This generates a unique ID for the signature approval procedure, which is then assigned to the User (e.g., smartphone registration number or mobile phone number, etc.).
- The identification itself, which in the case of the standard identity checkers is carried out, for example, by means of video identification or by checking against a bank account. In the case of the IdP, you authenticate yourself, i.e., you log in to the IdP and confirm that you have already been identified by the IdP. As part of the identification, it is checked whether you can be approved for the electronic signature procedure and whether all legal requirements for this are met (e.g. possession of the correct identity document, etc.).

- Finally, a result data set is made available as "evidence" to the Swisscom registration database (RA system) and archived by the Swisscom Certification and Trust Service within the legal retention period. This result data set is also used, for example, in court proceedings concerning the electronic signature or other verifications in the event of doubts about the signature.

Swisscom offers its own webviews for the registration process, which can be integrated into the respective workflow of the subscriber application. Alternatively, the user can create webviews that carry out the individual steps one after the other using OIDC PAR or OIDC CIBA API.

Identification procedures can be combined, i.e. an attempt can first be made, for example, to identify a person using an NFC-enabled ID document. If this is not available or is unsuccessful, the person is then forwarded to an auto-identification process.

4.6 Use of the Swisscom Trust Services registration portal

4.6.1 Registration procedure with voucher code or credit card payment

The person to be identified visits the website
https://srsident.trustservices.swisscom.com

It selects a suitable procedure according to 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 according to Swiss law, a procedure must be selected which is approved under the Swiss Signature Act ZertES.
- The signature level must be correct: Qualified electronic signatures, generally require more elaborate registration than advanced electronic signatures. The User is responsible for complying with these conditions when selecting the identification method. 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 means of identification must match. Each identification method specifies the requirements that must be met. For eID or NFC identification, the person must have a government-approved eID solution and, for example, a smartphone with NFC and/or government-approved app. For video and auto-identification methods, a machine-readable ID (passport or EU/CH ID card) must be available. For identification at an IdP/bank, a customer relationship must also exist with this IdP.
- Language: Not all procedures use all languages for User communication.
- The validity of the registrations, i.e., the period of time during which a signature can only be signed with the signature approval without further registration, varies from procedure to procedure.
- Price/voucher code: The procedures have different prices depending on the effort involved. If payment is made by voucher code rather than credit card, the voucher code may be restricted to a particular procedure. In this case, it may be necessary to check with the party that provided the voucher code.

4.6.2 Payment

Once the appropriate procedure has been selected, the User can pay for the identification using the credit card or voucher code provided. Credit card sales result in contracts with private customers, who then receive a payment voucher. Legal entities should contractually purchase individual vouchers via Swisscom Trust Services partners or a voucher package (minimum 200 registrations) via direct sales. Only voucher customers will receive an invoice.

4.6.3 Optional: Installation of the signature approval device

Before starting the installation process, the signature approval device to be used later for signature approval must be installed. Please note, that only Mobile ID or password in combination with one-time code via SMS is possible for these registration methods. If no signature approval method is installed, the User could be forced to use a combination of self-selected password and one-time code via SMS.

4.6.4 Identification process

To start the identification process, the User is redirected to the identification service provider or IDP. At the same time, the User is sent a link to the specified email address to start the identification process with the relevant provider. The links/redirections have an expiry date (see below).
The identification process is then carried out according to the instructions on the screen with the external identification service provider. You may need to enter data beforehand, which will then be requested as part of the process. In some cases, an application from the provider must be installed, or the process can be carried out entirely in the browser.
This needs to be considered during the identification process:

- Depending on the procedure, have the necessary means at hand, e.g., a sufficient camera, sufficient lighting or an NFC reader of NFC access module in the mobile device, etc.
- When presenting an ID document, always present the correct document (passport or EU/CH ID) and not, for example, a foreign ID card, driving licence, etc.
- If necessary, wait for the application or process to send the data to the Swisscom Certification and Trust Service and do not cancel the process prematurely.

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

In principle, an identification service is provided based on the material offered and the quality of the equipment used by the User. For example, if the ID images are washed out or unreadable, or if a (suspected) false ID has been presented, or if the IDs are not considered sufficiently secure, registration may be refused. A registration that has been started does not necessarily lead to success. Therefore, payment does not automatically imply a claim to successful registration, but merely legitimizes the buyer for an attempt within the framework of an identification procedure.

4.6.5 Terms of use

The terms of use of Swisscom Trust Services must be accepted. The signature approval procedure is used for the first time for acceptance. If this includes a password, the password shall be set for the first time. Often the terms of use are already displayed and accepted in the external identification process. If not, an SMS containing the terms and conditions will be sent to the mobile number provided during registration. The link in the SMS must then be opened and the terms of use confirmed using the authentication method provided. If the instructions in the SMS are not followed, the SMS will be sent again all three days within 15 days. If no consent is given after this period, the registration process will be cancelled, and a new registration will be required for signature. If only one of the terms of use is accepted instead of both (CH/EU), signing will only be possible in the relevant jurisdiction.

4.6.6 Signature

Only after accepting the terms of use and providing proof of identity can the User sign with the Subscriber and Signature applications.

Depending on the procedure used, the registrations have an expiry date, e.g. they can be linked to the expiry date of the ID card or they are generally only valid for 1, 2 or 5 years (see above). Before the expiry date, the User is reminded via SMS to re-register if the mobile phone number is known.

4.6.7 Refund

If an error has occurred due to mistakes in the registration process, you will be entitled to either a refund in the case of card payment or a replacement voucher in the case of a voucher.

Reasons are in particular:

- SMS not received on mobile numbers within the EU, Switzerland, and EEA
- Aborts of the app or process due to misbehavior.
- "Hanging" of the process for longer than 15 minutes.

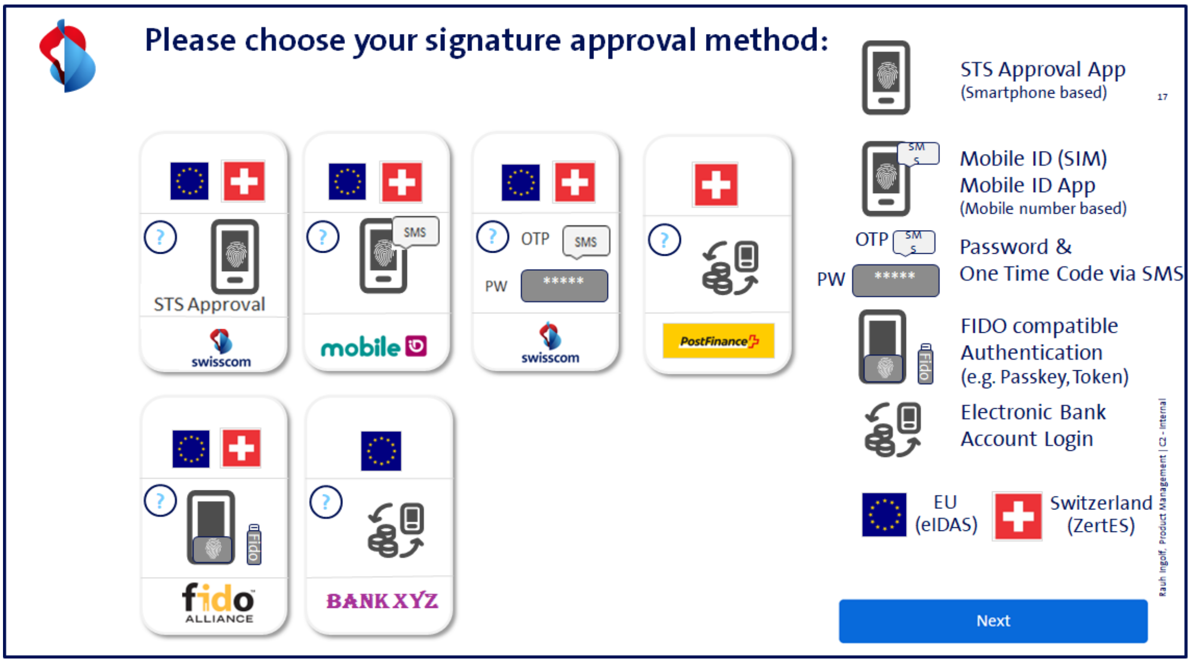
Furthermore, vouchers can be refunded for procedures that have been removed from the offer after purchase of the voucher.

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

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

4.7 Use of the store offer within the framework of the Subscriber applications

Subscribers who offer a signature workflow within the scope of the signature applications (sub-subscriber applications) are offered all registration procedures in the store (marketplace) according to order and configuration. The registration and selection of the signature approval procedure in the signature workflow is thus carried out by the signer himself if his signature approval procedure is not known and does not have to be checked separately in advance.

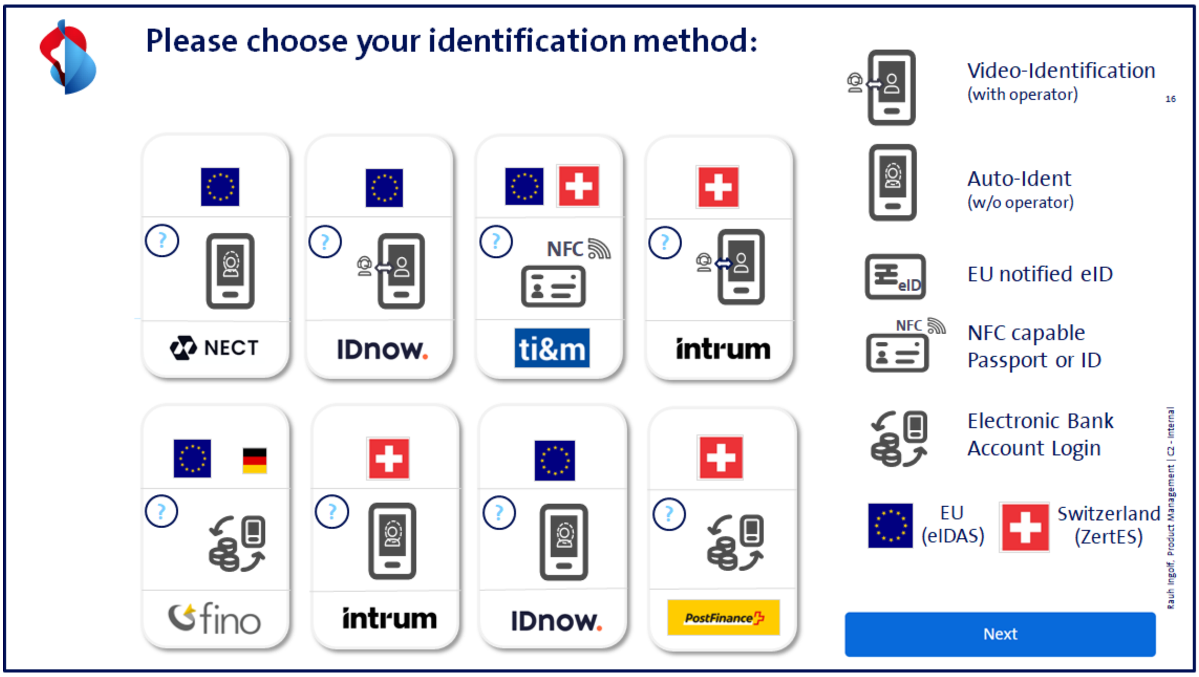


Please choose your signature approval method:

(Principle image - some of the procedures are not yet available in the Store)

These procedures must be ordered and are configured according to the order. The order form shows which procedure can be configured for a store. A monthly provision fee or a fee per identification can be charged, which is paid to Swisscom Trust Services as far unless a flat-rate fee is charged. Swisscom Trust Services acts here as a reseller of the identification service. The partner prices the costs into its offer to the end customer.

In the same way, the registration procedures are also offered in the signature flow:



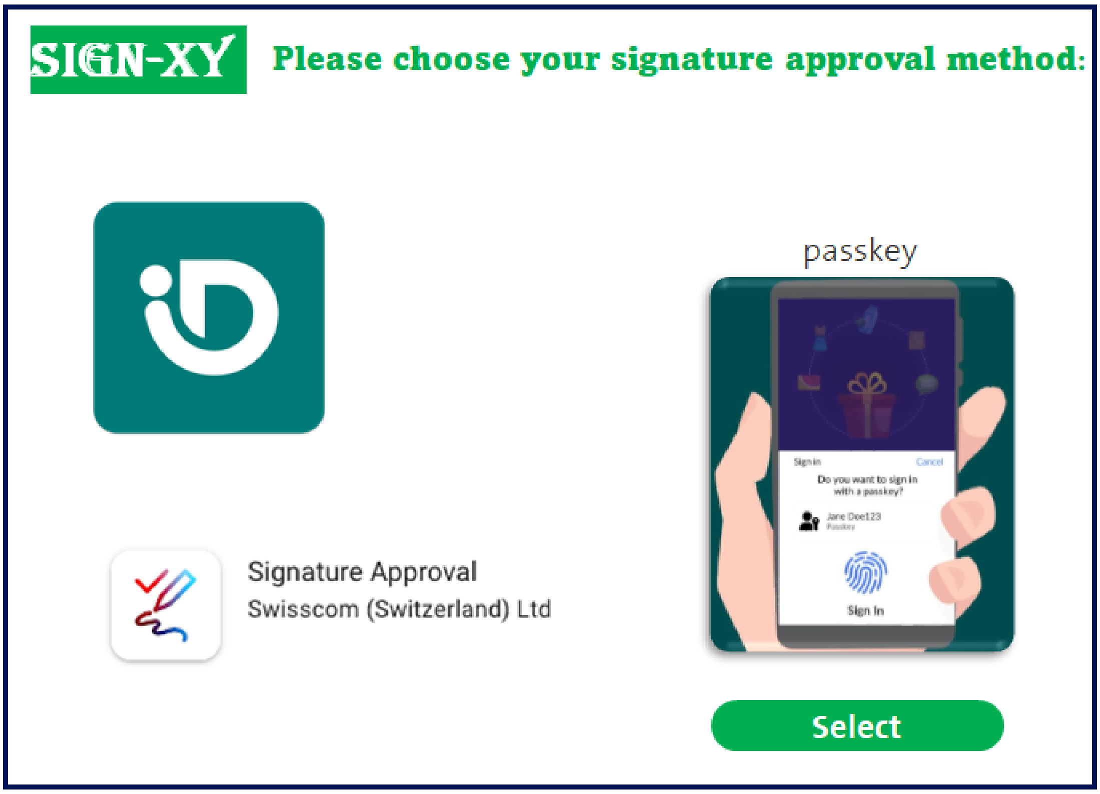
Please choose your identification method:

(Principle image - some of the procedures are not yet available in the Store)

Again, only the desired and ordered methods are configured in the selection. Swisscom Trust Services ensures in the signature flow that persons who are not registered with the selected signature approval method, or whose signature authorization fails, are forwarded to the registration methods store. The appropriate registration methods are offered here, depending on the jurisdiction and signature level.

Signature flows can also be configured to allow only one signature approval or registration method, for example. The so-called one-time signature is also possible as a special configuration. In this case, only identification methods are displayed, and the signature is also created in the same session. There is no need for a special signature approval, but this means that registration is required again for future signatures.

Via OIDC-PAR API and/or OIDC-CIBA the user can design its own flow using own brand instead of the webviews shown above. This could be an example:



SIGN-XY Please choose your signature approval method:

4.8 Own identification and signature approval procedures

IdPs who wish to integrate their own identification or signature approval procedures can do so. This requires an implementation concept and an audit by a conformity assessment body, and possibly a notification to the supervisory authority. The individual steps are offered as part of the onboarding support and are described in the corresponding onboarding support service description. Once approved, the procedures can then be offered to other subscribers in the market, if desired.

4.9 Service Desk

Swisscom Trust Services provides a service desk (1st level support) for identifications acquired by credit card or for Users who use the above-mentioned interfaces to Swisscom systems in their applications. Users who carry out identifications by voucher should contact the partner that issued the vouchers. According to the requests, Swisscom Trust Services will solve the incidents directly with the service points of the identification service providers, if necessary, provided that no own identification method is used.
Identifications acquired via the registration portal do not guarantee registration. If a registration does not work, the user will be offered another attempt using the same and finally another method. If this is unsuccessful, users with credit card payment are entitled to a refund.

5 Performance presentation and responsibilities

One-off benefits

Activities (S = STS/U = User, i.e. customer of this service)	S	U
Provision of the registration method within the framework of the registration portal		
1. Registration via the online portal of Swisscom Trust Services: The User can call up the appropriate registration at https://srsident.trustservices.swisscom.com and pay by voucher code or credit card	✓	
2. Purchase of the registration option via the online portal either by concluding a contract via one or more vouchers or directly by credit card payment.		✓
Provision of registration methods and signature approval methods in the framework of stores (in the signature flow)		
3. Users (in this case Subscribers) who provide signature applications for the signature service can include the stores for selecting the registration method and for selecting the signature approval. Swisscom Trust Services provide the processes for calling up the signature approval means and for accepting the terms of use as a configurable webview within the scope of registration.	✓	
4. Integration of the webviews in the signature flow. Establishment of a separate accounting system and billing of the services to the identified persons (signatories).		✓
Provision of registration and signature approval method in the store via OIDC APIs (PAR/CIBA)		
5. Implementation of views based on the offered APIs		✓
6. API test	✓	
Termination of the service		
1. Deleting the permissions and accesses to the Smart Registration Service	✓	
2. Operation termination of identification methods or signature approval methods that no longer meet regulatory or legal requirements or are no longer supported by the provider.	✓	

Recurring services

Activities (S = STS/U = User, i.e., customer of this service)	S	U
Standard services in general		
1. Provision and maintenance of the service infrastructure and access and operation of the service.	✓	
2. Ensuring the conformity of the identification methods to the respective types of electronic signature offered and the offered legal area for this procedure.	✓	
3. Selection of the appropriate identification method compatible with the desired electronic signature and other requirements in accordance with section 4.		✓
4. Provision and maintenance of the interface to the partners selected by Swisscom Trust Services to carry out the identification process.	✓	
5. Informing the person to be identified about the pending identification, the purpose of the identification and the procedure to be followed during the identification in case of use of the Swisscom Webviews.	✓	
6. Informing the person to be identified about the pending identification, the purpose of the identification and the procedure to be followed during the identification in case of use OIDC PAR and/or CIBA APIs		✓
6. Provision of access to the identification service provider or IdP for the person to be identified	✓	
7. Collecting the evidence data or results from the external identification service providers or IdPs.	✓	
8. Reporting security incidents involving identification or signature approval.		✓
9. Legally compliant archiving of the received identification evidence, the signature approval procedure used and consents to the terms of use	✓	
10. Support and coordination and commissioning of support cases with the respective identification service provider, stating the contract number, Multiple Authentication Broker Transaction ID (so-called rax_id), if available mobile number or UUID, time of identification and identification method used as well as mobile number.	✓	
11. Mention of the order reference (if available), time of identification, identification method used, and signature approval medium used or other necessary data in the case of a support case.		✓

Activities (S = STS/U = User, i.e., customer of this service)	S	U
12. The person to be identified ensures that he/she is permanently resident in Switzerland, the EEA or a country of the EU or another country which was explicitly stated in the order given to Swisscom Trust Services		✓
13. User's own communication costs for using support services (e.g., telephone, postage, etc.)		✓
14. The User accepts that he or she or the person to be identified is not entitled to registration. This may be refused for different reasons e.g., due to a risk assessment. The only compensation here is a refund of the costs that he or the person concerned has paid for this registration. Alternatively, Swisscom Trust Services can also send a voucher for another registration method.		✓
15. Billing of the services to the customer of the services, listing the summary utilization of the methods used. (B2B billing)	✓	
16. User or end customer-specific usage recording and billing, which method was used and how often		✓
17. Communication with the apps, browsers, keys (e.g., passkeys) and end devices of the signatory or the person to be identified, provided that • the devices and apps are accessible via the Internet with sufficient bandwidth or mobile phone functionalities via mobile phone, • SMS messages can be received by the local Swisscom provider for one-time codes, • no viruses or disruptive software installed locally on the signatory or the person to be identified interferes with communication, • the latest versions of the required apps and browsers are always used, • the latest versions of the operating systems or corresponding software are always used for operating system functions (e.g., passkeys).	✓	
Standard services in case the registration and/or signature approval methods in the store are called via OIDC PAR		
1. Notification to the person to be identified that he or she will be redirected to a portal of an identification service provider (example: "By calling up the URL http://xxx you will be redirected to the identification portal of our identification partner where you can identify yourself"). Obtaining consent within the meaning of the applicable data protection legislation, insofar as advance data is sent.		✓
2. Responsibility for preparation of the identification of the person to be identified before providing access to the identification partner by means of a prompt or User guidance in the relevant portal and compliance with all regulations for the selected identification method, i.e. in particular hints concerning the 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, etc.), acceptance of the terms of use, sufficient illumination in the case of video procedures, installation of the necessary identification apps/programs, necessary entries or answers to the questions asked.		✓
3. Provision of error handling in case a registration or signature approval was not successful, e.g., by offering a second try or alternative method for registration and/or signature approval.		✓
Standard services when providing the methods via the registration portal		
1. Provision of the voucher system and redemption options for vouchers as well as processing credit card payments via payment service providers.	✓	
2. Enter the exact personal data for proper invoicing or payment receipt.		✓
3. Invoicing (by e-mail) to corporate customers or payment receipt to the private User	✓	
4. Compensation of costs for aborted identifications (e.g., video identification) if this is due to a faulty process at Swisscom Trust Services, provided that the User fulfils his obligations to cooperate.	✓	
5. Online identification via the Swisscom Trust Services portal: Support exclusively via web form or e-mail and attempt to resolve the problem by voucher for alternative procedure, or repayment. Telephone support, personal support and personal analysis of the respective problem case are not provided. Identification within the scope of the stores: Support via the options mentioned in the order form/contract. A registration problem is generally solved via reimbursement of costs or substitute identification. There is generally no entitlement to a detailed analysis of an identification problem.	✓	
6. International payment of statutory levies in the private customer business.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
Video identification via app		
1. Download of the specified app from the smartphone app store and installation on the smartphone. The app may not be available in every country-specific app store.		✓
2. Download and installation/activation of the signature approval means if necessary.		✓
3. Use on a smartphone with a sufficient equipped camera (minimum resolution 1024 x 768 pixels) in decent lighting conditions (lamp, daylight).		✓
4. Use of ID from selected EU/EEA countries and Switzerland or passports. No residence permits or driving licenses. See clause 4.2 for the list of accepted documents.		✓
5. Selection of the language to be spoken by the operator by the language selection of the User interface/smartphone, if no extra language selection is specified.		✓
6. Answer all questions asked by the operator in the specified authorised languages of the language selection or according to the operator's instructions. These serve as an additional security check of the document or to ensure that a previously unrecorded video session is played during registration (so-called life detection).		✓
7. Execution of the identification and transmission the evidence data to the Swisscom Certification and/or Trust Service.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
Auto-identification via app		
1. Download of the specified app from the smartphone app store and installation on the smartphone. The app may not be available in every country-specific app store.		✓
2. Download and installation/activation of the signature approval means if necessary.		✓
3. Use on a smartphone with a sufficient equipped camera (minimum resolution 1024 x 768 pixels) in decent lighting conditions (lamp, daylight).		✓
4. Use of ID from selected EU/EEA countries and Switzerland or passports. No residence permits or driving licenses are allowed. See clause 4.2 for the list of accepted documents.		✓
5. Language selection of the User guidance by the language selection of the User interface/smartphone unless an extra language selection is specified.		✓
6. Answer all questions asked by the app or following app instructions. These serve as an additional security check of the document or to ensure that a previously unrecorded video session is played during registration (so-called life detection).		✓
7. Execution of the identification and transmission the result data to the Swisscom Certification and/or Trust Service.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
NFC identification via app		
1. Download of the specified app from the smartphone app store and installation on the smartphone. The app may not be available in every country-specific app store.		✓
2. Download and installation/activation of the signature approval means if necessary.		✓
3. Use on a smartphone with a sufficient equipped camera (minimum resolution 1024 x 768 pixels) in decent lighting conditions (lamp, daylight). The smartphone must provide a NFC tag reader and prepared to read out NFC tags.		✓
4. Use of chip-based ID from selected EU/EEA countries and Switzerland or passports. No residence permits or driving licenses are allowed. See clause 4.2 for the list of accepted documents.		✓
5. Language selection of the User guidance by the language selection of the User interface/smartphone unless an extra language selection is specified.		✓
6. Answer all questions asked by the app or following app instructions. These serve as an additional security check of the document or to ensure that a previously unrecorded video session is played during registration (so-called life detection).		✓

Activities (S = STS/U = User, i.e., customer of this service)	S	U
7. Execution of the identification and transmission the result data to the Swisscom Certification and/or Trust Service.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
Auto- and NFC identification via browser		
1. Activation of a browser session on the user's smartphone, e.g., via QR code.		✓
2. Download and activation of the signature approval method if necessary.		✓
3. Use on a smartphone with a sufficient equipped camera (minimum resolution 1024 x 768 pixels) in decent lighting conditions (lamp, daylight). In case NFC identification should be used the smartphone must provide a NFC tag reader and prepared to read out NFC tags.		✓
4. Installation of the browser extension for NFC read-out in case NFC and chip-based identification document should be used		✓
5. Answer all questions asked by the app or following app instructions. These serve as an additional security check of the document or to ensure that a previously unrecorded video session is played during registration (so-called life detection).		✓
6. Execution of the identification and transmission the result data to the Swisscom Certification and/or Trust Service.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
eID identification		
1. Download the specified app from the app store of the smartphone and install it on the smartphone. Additional national apps may have to be installed (depending on the country). The app may not be available in every country-specific app store.		✓
2. Download and installation/activation of the signature approval means unless the signature will be approved by the password/one-time code procedure.		✓
2. Use on a smartphone with an NFC interface.		✓
3. Use of IDs from selected EU/EEA countries and Switzerland. See clause 4.2 for the list of accepted documents.		✓
4. Language selection of the User guidance by the language selection of the User interface/smartphone unless an extra language selection is specified.		✓
5. Answer all questions asked by the app or following app instructions. These serve as an additional security check.		✓
6. Execution of the identification and transmission of the result data to the Swisscom Certification and/or Trust service.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
IdP identification		
1. Business relationship with the providing IdP and possession and use of the necessary access means to authenticate with the IdP. The way to authenticate must be requested from the IdP if necessary.		✓
2. The (first) identification at the IdP has been made in such a way that it is also compatible with the regulations and laws of the required electronic signature.		✓
3. IdP must filter out and reject identifications that do not comply with the law.	✓	
4. The terms of use of Swisscom Trust Services must be accepted when registering for the signature service for the first time.		✓
5. Execution of the identification and transmission of the result data to the Swisscom Certification and/or Trust service, unless archived by the IdP.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U

Activities (S = STS/ U = User, i.e., customer of this service)	S	U
Customer's own IdP, identification method and/or signature approval method		
1. Order of the appropriate onboarding services to reach the conformity of the method for the required jurisdiction and level of signature. Conclusion of a contract for the delegation of registration authority activities.		✓
2. Preparation of an implementation concept and notification of all concept changes and, in this case, order of a new review for the amended implementation concept.		✓
3. Review of the implementation concept, preparation of the audit request, planning of the audit, discussion of the final audit report, submission of the new method to the supervisory body(ies) to obtain approval for use.	✓	
4. Elimination of all non-conformities, compliance with all regulations and laws applied to this process, ongoing adaptation to new standards and regulations, regular repeat audits and full audits (every two years). Order via Swisscom Trust Services.		✓
5. Provision of all information by the provider of this method as a supplier to the certification and trust service as a critical infrastructure within the framework of the NIS2 directive and corresponding national laws. Self-audit of the relevant cybersecurity audit items and participation in the joint annual audit with Swisscom Trust Services.		✓
6. Common audits with the provider of the method according to the requirements for critical infrastructures.	✓	
7. Responsibility for the compliant implementation of the identification and provision of evidence, reporting all violations and anomalies to Swisscom Trust Services in a very timely manner.		✓

Activities (S = STS/U = User, i.e., customer of this service)	S	U
Password - one-time code signature approval procedure		
1. Set and securely note the password to be used for the signature. This cannot be reset during the period of use! In this case, a new registration is necessary.		✓
2. Use of a SIM card from a network operator that can receive SMS (roaming if necessary) from the network of Swisscom (Switzerland) Ltd or the provider seven.io or Horisen. This can be problematic in some foreign countries; certain countries do not allow SMS reception from abroad without registration. The one-time code is sent via the mobile number of the SIM card.		✓
3. Enter the password and one-time code in the input windows provided.		✓
4. Provision of the input windows. Within the framework of a workflow of the Subscriber application, the windows are offered as parameterizable iFrames. The parameterization can be viewed at https://github.com/SwisscomTrustServices/AIS/wiki/SAS-Documentation.	✓	
5. Use of the two-factor entry of password and one-time code to trigger the signature, as well as logging and archiving of this declaration of intent to sign.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
Mobile ID procedure		
1. Use of a Swiss SIM card that enables Mobile ID		✓
2. Initialization of the Mobile ID on the smartphone with the Mobile ID-enabled SIM card via https://mobileid.ch . Securely archive the recovery code displayed during activation for activation on another smartphone. If Mobile ID is used on another smartphone without the recovery code, the User must re-register.		✓
3. Set and securely remember/keep the 6-digit PIN that must always be entered when calling up the Mobile ID.		✓
4. Use of a network operator that can receive SMS (roaming if necessary) from the network of Swisscom (Switzerland) Ltd or the provider seven.io or Horisen. This can be problematic in some foreign		✓

Activities (S = STS/U = User, i.e., customer of this service)	S	U
countries; certain countries do not allow SMS reception from abroad without registration. The one-time code is sent via the mobile number of the SIM card. The SMS is used to initialize the Mobile ID. Swiss operators do all accept Swisscom SMS.		
5. Enter the PIN for signature approval.		✓
6. Call the Mobile ID application on the signatory's device to trigger the signature, as well as logging and archiving this declaration of intent to sign.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
Mobile ID App Procedure		
1. Download of the Mobile ID app from the smartphone app store and install it on the smartphone. The app is not available in the App Store in every country.		✓
2. Initialization of the Mobile ID app on the smartphone and setting up a second factor, e.g. facial recognition or fingerprint. Securely archive the recovery code displayed during activation for activation on another smartphone. If Mobile ID App is used on another smartphone without the recovery code, the User must re-register.		✓
3. Use of a SIM card from a network operator that can receive SMS (roaming if necessary) from the network of Swisscom (Switzerland) Ltd or the provider seven.io or Horisen. This can be problematic in some foreign countries; certain countries do not allow SMS reception from abroad without registration. The one-time code is sent via the mobile number of the SIM card. The SMS is used to initialize the Mobile ID App.		✓
5. Activation of the biometric factor for signature approval.		✓
6. Call the Mobile ID application on the signatory's device to trigger the signature, as well as logging and archiving this declaration of intent to sign.	✓	

Activities (S = STS/U = User, i.e. customer of this service)	S	U
FIDO2 methods (e.g., Passkey)		
1. Use of a device (PC, smartphone, USB stick FIDO2 compatible, etc.) or software on a device that supports the FIDO2 standard or passkey.		✓
2. Initial creation of the FIDO2 key/passkey. Then use on all devices on which this key is available (possibly synchronized by system services of the operating system manufacturer or software manufacturer). Responsibility for the safeness of the passkey, FIDO2 private key and eventual synchronization.		✓

Activities (S = STS/U = User, i.e., customer of this service)	S	U
IdP signature approval		
1. Business relationship with the providing IdP and possession and use of the necessary access means to authenticate with the IdP. The call and the use must be requested from the IdP if necessary.		✓
2. To use the IdP signature approval, registration with the IdP is mandatory.		✓
3. Calling and using the selected IdP signature approval for signature initiation, as well as logging and archiving this expression of will.	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
Signature approval SDK		
1. Embedding the software development kit in a self-designed app for signature approval. Consideration of the requested initialization parameters (e.g., PIN length, biometric factors, etc.). These are provided by Swisscom Trust Services.		✓
2. Creation of an implementation concept for the SDK, which shows the conform use and publication of the app (template delivered by Swisscom)		✓
3. Approval of the implementation concept and configuration for use	✓	

Activities (S = STS/U = User, i.e., customer of this service)	S	U
4. Initializing the app and thus the SDK on the smartphone and setting up a second factor, e.g., facial recognition or a fingerprint, as well as a PIN as a fallback solution. If necessary, securely archive the recovery code displayed during activation for activation on another smartphone. If the SDK with the associated app is used on another smartphone without the recovery code, the User must re-register.		✓
5. Activation of the biometric factor for signature approval.		✓
6. Call the signature approval SDK application on the signatory's device to trigger the signature, as well as logging and archiving this declaration of intent to sign.	✓	
7. Order of Walkthrough (estimated two man-days) of the auditor at STS		✓
8. Placing the walkthrough audit at KPMG	✓	
9. Update of the implementation concept with each change. Follow-up of the approval methods described in the concept.		✓
10 Approval of the changed concept, if necessary, placing the walkthrough audit at KPMG and configuration to use the update	✓	
11 Audit cost invoiced by Swisscom		✓

Activities (S = STS/U = User, i.e., customer of this service)	S	U
Swisscom Signature Approval App		
1. Download of the signature approval app from the smartphone app store and install it on the smartphone. The app is not available in the App Store in every country.		✓
2. Initialize the signature approval app on the smartphone and set up a second factor, e.g., facial recognition or fingerprint and PIN as fallback position. Securely archive the recovery code displayed during activation for activation on another smartphone. If the signature approval app is used on another smartphone without the recovery code, the User must re-register.		✓
3. Activation of the biometric factor for signature approval.		✓
4. Call the the signature approval app on the signatory's device to trigger the signature, as well as logging and archiving this declaration of intent to sign.	✓	

6 Service Level

6.1 Service Level

6.1.1 General service level of Swisscom Trust Services for all services

The following service levels generally refer to the agreed Monitored Operation Time for the provision of the services including the services of the partners. This refers to the services for the provision of the procedures in the Stores and on the registration website, as well as the support times for general ticket acceptance. Definitions of the terms (Operation Time, Monitored Operation Time, Support Time, Availability, Security and Continuity) as well as the description of the measurement procedure and reporting result from the contractual component "Basic Document".

The following service levels are provided. If there are several possible service levels per specification, the service level is selected in the service contract.

Service Level & Target Values			Registration & Signature Approval
Operation Time			
Monitored Operation Time	Mon-Sun	0am-12pm	●
Provider Maintenance Window	PMW-DC	PMW Data Center Swisscom (Schweiz) AG	●
	PMW-S: with advance notice for security and system-critical updates	Daily 7pm-7am, for announced maintenance only	●
Support Time			
Support Time [1]	Mon-Fri	8am-5pm[2]	●
Troubleshooting	Mon-Sun	0am-12pm	●
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 price) ○ = Against surcharge - = Not available

6.1.2 Specific SLAs per procedure used

The table below contains further SLA values per procedure:

- Procedure and partner: specific procedure for which SLA values are specified.
- Operation Time: Time during which registrations can take place. For services with human processing (also in the background) it takes some time until the results are validated.

[1] If the service was purchased via a Swisscom Trust Services partner, this partner must always be contacted in the event of faults. The partner will forward the fault to Swisscom Trust Services if it cannot be rectified.

[2] Holiday regulation see "Basic document (chapter SLA definitions)".

- Processing time until submission: Due to background checks, there may be further processing times after completion of the identification until the result of the identification has been submitted to Swisscom Trust Services and the first signature can be executed. The processing time is only valid within the operation time.
- Link expiry times: In the event of registration via the Swisscom Trust Services registration portal, Users will receive links with the redirects to the identification service providers, so that in the event of an error or cancellation, the identification can be repeated free of charge. The links are sent to the recipient by e-mail after payment or redemption of the voucher. They are subject to expiry dates and must be used promptly. 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. In case methods are offered via the Store these parameters are negligible.
- Please note the public holidays of the partners, which generally have the same effect as Sundays:
    - Switzerland: 1 and 2 January, Good Friday, Easter Monday, Whit Monday, Ascension Day, 1 August, 25 and 26 December

Procedure	Partner	Operation Time	Processing time until delivery	Link expiry times (days)	Number of retrievals	Other SLA
Standard identifications						
Video identification, app based	IDNow GmbH, Germany	Mon.-Sun. 7am-12pm	Max. 20 minutes	90	No limit	Measured uptake of calls on a monthly basis: 80% during the first 90 seconds, 90% during the first 120 seconds, 95% during the first 180 seconds.
eID Identification (Germany), App based	IDNow GmbH, Germany	Mon.-Sun. 7am-12pm	Within seconds	90	No limit	
Auto identification, browser based	Fidentity AG, Switzerland	Autoident: Mon.-Fri. 8 am -6 pm Sat. 8 am-12 am (extended SLA on request)	Max. 3 minutes	In case of use of the method in the store these parameters are negligible		
NFC Identification, browser based	Fidentity AG, Switzerland	7 days/24hrs	Max. 3 minutes	In case of use of the method in the store these parameters are negligible		
Auto identification, app based	Nect GmbH, Germany	7 days / 24 hours	Max. 2 minutes	30	5	
Auto identification, App based	ti&m AG, Switzerland	Mon.-Fri. 8am-8pm Sa. 8am-4pm 7 days / 24 hours on request and surcharge	Max. 5 minutes	In case of use of the method in the store these parameters are negligible		Technical availability per year 99.5%
NFC identification, App based	ti&m AG, Switzerland	7 days / 24 hours	Max. 5 minutes	In case of use of the method in the store these parameters are negligible		Technical availability per year 99.5%

Procedure	Partner	Operation Time	Processing time until delivery	Link expiry times (days)	Number of retrievals	Other SLA
Video identification, app based	Intrum AG, Switzerland	Mon. - Sat. 7am-10pm	Max. 15 minutes	90	No limit	
				In case of use of the method in the store these parameters are negligible		
Auto identification, app based	Intrum AG, Switzerland	Mon. - Sat. 7am-10pm	Max. 15 minutes	90	No limit	
				In case of use of the method in the store these parameters are negligible		
IdP identifications						
IdP identification with Postfinance App	Postfinance AG, Switzerland	7 days / 24 hours	Within seconds			

6.1.3 Validity of voucher codes

For the Swisscom Trust Services registration portal, voucher codes are guaranteed to be valid for a maximum 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.

7 Invoicing and quantity report

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. All other users get the report of the successful registrations and signature approvals to be paid per time period of the invoicing term. The prices are indicated on the website or in the order form for the vouchers.

8 Special regulations

8.1 Data processing by third parties from Switzerland or abroad, emergency accesses

The identification data transmitted by the identification service providers is archived exclusively on Swisscom servers in Switzerland. Depending on the identification method selected by the User, identification service providers from the EU and Switzerland specified in the service contract are used for the respective identification. These identification service providers are contractually bound to data protection in accordance with the Data Protection Regulation (GDPR/EU) and the Data Protection Act (DPA/CH) as part of the transfer of data processing.
Swisscom (Switzerland) Ltd or Swisscom ITSF shall enter into an agreement with the external identification service providers on commissioned data processing in accordance with the EU General Data Protection Regulation and the Swiss Data Protection Act, insofar as they do not act independently as data controllers vis-à-vis the person to be identified.

8.2 Identification of persons residing outside the EU/EEA/Switzerland

The range of signatures and registrations offered by Swisscom Trust Services is aimed at persons resident in the EU, the EEA and Switzerland, as different legal provisions (e.g., consumer protection and data protection law) often apply to persons resident 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 as an option. The legal possibilities will then be checked and, if necessary, the terms of use or other provisions will be adapted.

8.3 Exchange of methods, deactivation of methods

Swisscom offers the registration and signature approval methods under the following conditions:

- The methods are audited and approved for signature creation in accordance with regulatory and legal requirements.

- The providers comply with the requirements accordingly.

Should the regulations change, or events occur which no longer allow the continued existence of the identification or signature approval (e.g., failed audit, discontinuation of the provider's business activities, etc.), Swisscom is free to replace the offered method with an equivalent method or to remove the method completely from the offer. In the latter case, the customer has an extraordinary right of cancellation.

Within the framework of flat rate offers that enable registration, signature approval and signature in one price, the exchange of providers of similar methods is possible at any time.

8.4 Delimitation in the use of the identification service providers' identification data for further own purposes

In principle, the User with different identification methods has the option, if desired and agreed, of concluding a contract directly with the identification service provider to carry out the same identification method and to use the evidence thus obtained (e.g., in the context of combating money laundering) for the fulfilment of his own purpose, provided that the identification partner offers this. In this case, the identification data set created under this contract with the signature-relevant data will not only be made available to the Swisscom Certification and/or Trust Service, but also - if necessary enriched with further data - to the User.
This process requires the conclusion of additional, mutually agreed contracts (between the User and the Identification service provider on the one hand and between the Identification service provider and Swisscom Trust Services or the Swisscom Certification and Trust Service on the other) which are not the subject of this service description.
If the User makes use of this option and it concludes these contracts,

- the User shall be responsible, in accordance with the General Terms and Conditions, for providing its signatory with terms and conditions that define the construct together with a transparent data protection regime, and
- the User is obliged to inform Swisscom Trust Services of the existence of a contract with an identification service provider before activating a registration procedure.