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

Service description
Smart Registration & Signing Service

Swisscom Trust Services

Swisscom Trust Services Ltd

Konradstrasse 12
8005 Zurich

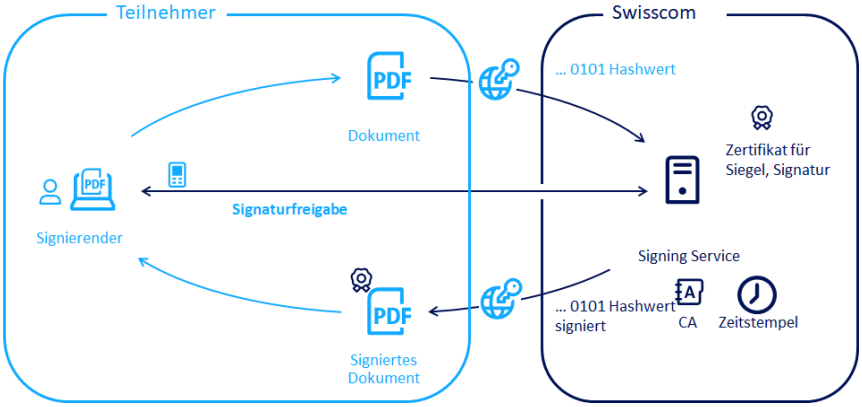
Switzerland

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

1 Content

2 Service overview

The Smart Registration & Signing Service is a server-based modular remote signature service marketed by Swisscom Trust Services Ltd and provided by the Swisscom Certification Service of Swisscom (Switzerland) Ltd, the Swisscom Trust Service of Swisscom IT Services Finance S.E. (Vienna) (hereinafter referred to as "Swisscom ITSF") and other affiliated partners or trust service providers. The Signing Service for Switzerland and the EU is provided in data centres in Switzerland. Swisscom Trust Services AG markets the Signing Service in its own name or in turn grants third parties the right to market the Signing Service in their own name.
The remote Signing Service is made available to Subscribers who operate a Subscriber Application. Signers can use it to sign digital files electronically. This ensures the integrity and authenticity of a file. Swisscom (Switzerland) Ltd. as the Swiss certification service or Swisscom IT Services Finance S.E. as a qualified EU Trust Service Provider under eIDAS generates and manages the signature certificate in trust for the signer or seal requester and makes it available for the remote Signing Service via an encrypted channel. As a result, the signatory does not require any additional equipment, such as a token or signature card for this service, apart from a Subscriber Application operated by the Subscriber for sending the document to be signed and receiving the signed document.
The Subscriber application prepares a document in such a way that only the hash value (checksum of fixed length without inference to the content) is transmitted to the Signing Service for signing. The actually readable files and the information they contain do not leave the Subscriber's system environment and are therefore not visible to the Swisscom Certification and Trust Services. The signed hash is re-incorporated into the document by the Subscriber Application creating a signed document. Before the signature is triggered, the Subscriber must authenticate to the Subscriber Application and approve the signature.

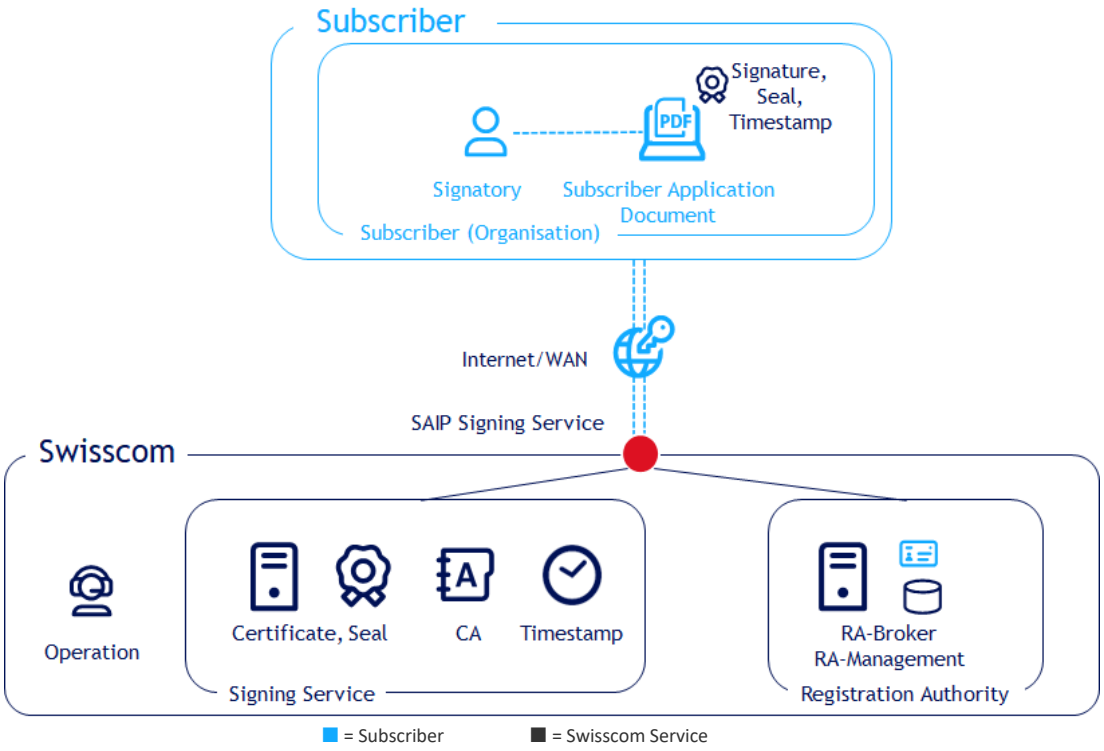


Additionally, the service offers a one-time, time-limited registration and the continuous use of a signature approval method (e.g., fingerprint application) for the personal signature ("repetitive signing"). However, one-shot signing is also possible. For the use of identification and signature approval methods, stores (marketplaces) are available in which partners offer their methods for Subscriber Applications, but for which Swisscom Certification and Trust Services also provide its own methods. A permanent signature approval can be set up for the provision of seals and time stamps. The Multiple Authentication Broker orchestrates the registration and signature approval with the registration and approval methods available in the stores. As a result of the broker communication, the signature application receives a token with which the signature application can then execute the hash signature. The broker and the available methods are described in the "Service description for registration and signature approval methods".
The signing service offers depending on the ordered positions advanced and qualified electronic signatures for natural persons, advanced and regulated or qualified seals for organisations and timestamps. Qualified electronic signatures have the highest legal effect and are in many cases equivalent to a handwritten signature. This means that, in principle, business requirements can also be fulfilled for which a handwritten signature is required by law (cf. Section 8.2).
Swisscom (Switzerland) Ltd is a recognised provider of signature and certification services in Switzerland in accordance with ZertES, and Swisscom ITSF is a recognised qualified trust service provider in accordance with the eIDAS Regulation and the Austrian Signature and Trust Services Act (SVG) for the issuance of advanced and qualified certificates for electronic signatures and electronic seals. The accredited supervisory bodies regularly check whether the applicable legal and regulatory requirements are also met.
This service description describes the service for electronic signatures for natural persons resident in the EU, Switzerland and EEA countries, seals for organizations and timestamps.

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 (Subscriber), monitored and the service levels provided are reported.
The following purely schematic diagram serves to illustrate the services and service components of Smart Registration & Signing Service:



The Service Access Interface Point of the service for the signatures is the connection to the Internet of Swisscom Registration & Signing Service. The availability of the service is given if requests are received by the service and answered correctly according to the interface description to the SAIP. The correct response can also consist of a documented error message or an error message that is meaningful for the Subscriber.
The interface description can be found at https://trustservices.swisscom.com/downloads under the link "Reference Guide":
https://documents.swisscom.com/product/filestore/lib/e2007490-6fd4-4012-801d-b104801a9abc/reference_guide_smartregistration_signing-en.pdf?idxme=pex-search
As well as the integration guide in the partner area:
trustservices.swisscom.com/hubfs/Website Files/Documents/Developer Documentation/MAB-IntegrationGuide-en.pdf
SMS information, if not provided within the Swisscom network, is provided at the interface to the roaming partner. Swisscom Trust Services does not guarantee the functioning of the Internet or the roaming partner's network.

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 method in which the signatory applies 2 factors. These 2 factors must be part from two of 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.

Term	Description
Access Token	The Access Token gives a user access to a resource. The token identifies the user to the resource. In the signature context, identification and signature approval are ensured beforehand. The issued token enables the user to request and receive a signature. They are defined in the OAuth 2.0 standard and can also have various properties, e.g. 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.
Supervisory body	According to ZertES, the supervisory bodies are responsible for recognising certification services. In Switzerland, KPMG is currently the supervisory body. The counterpart in the eIDAS Regulation to this is the supervisory body of Austria, RTR in case of accreditation in Austria.
Supervisory body	According to the eIDAS Regulation, a supervisory body is responsible for ensuring the qualification of the corresponding trust services and thus guaranteeing a comparable level of security. For this purpose, it uses the audit report of the conformity assessment bodies. The Swiss Signature Act ZertES contains the counterpart of the supervisory body.
Authorization Code	In the OAuth2.0 standard protocol, the authorisation code is a temporary code that a client system can use to obtain an access token. This prevents e.g. a visible exchange of the access token via a browser interface, so that an attacker is prevented from intercepting the access code.
CEN/TS 419 241	CEN is a European committee for standardisation, which published a standard for remote signatures by the standard ISO EN 419 241. This standard standardises the access to a signature and thus also the signature approval. It is part of the Swiss signature law and is also required by various supervisory bodies in Europe for the authorisation of remote signature providers.
Claimed ID	The Claimed ID is the access account to the Signing Service of Swisscom Trust Services. It consists of a unique identifier for the Subscriber (e.g. the URL of their homepage) and an additional designation of which certificates are used for the signature.
CMS	Cryptographic Message Syntax - A syntax defined in RFC5652 for digital signature and cryptographic messages.
CP/CPS (certificate guidelines)	Certificate Guidelines (CP/CPS) for issuing "Diamant" (Diamond, qualified) and "Saphir" (Sapphire, advanced) class certificates. Certificate policies and certificate practices are documents of a certification body that describe the policies and practices for issuing certificates. These can be found in the repository at https://trustservices.swisscom.com/repository
Distinguished Name	A certificate also contains a directory with information about the certificate holder, e.g. the signatory. The parameter object that characterises the certificate holder is called the "distinguished name". It contains parameters such as the "common name", the "surname" or "last name", "country" (country of issue of the signature or the ID card or residence country of the registration authority), "serial number" but also "organisation" (organisation to which the certificate holder belongs) or "organisational unit" (sub-organisation).
DSG	Federal Act on Data Protection in Switzerland. The version dated September 1st, 2023 is largely aligned with EU data protection legislation (GDPR).
GDPR	EU General Data Protection Regulation.
Document	For better comprehensibility, the term document is used synonymously with the term data. Both documents and data can be signed.
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 acts" which regulate aspects nationally that were not regulated in the regulation. In Austria, this is the “SVG” (Signature and Trust Services Act), which regulates e.g. the term of the archiving period for data.

Term	Description
Conditions of use for seal creation	If qualified (EU) or regulated (CH) seals are issued, the approval of the seals is ensured via an interface protected with a TLS access certificate. For this purpose, the person in charge of the seal requester must store and manage the private key of the access certificate accordingly under its private control. The solution behind this must be described by the partner in the conditions of use for the seal creation. Swisscom Trust Services will then check this solution and conclude a contract with the Subscriber for the " Seal Approval Solution".
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.
Electronic seal	The electronic seal is technically based on 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.
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.
Evidence	Collection of data that can proof a registration and identity of a signatory. This proof may also consist of a reference to a data set (evidence) managed by a delegated registration authority.
Seal Approval Solution	Contract signed by Swisscom Trust Services and the provider of a seal Subscriber application for the use of a Seal Approval Solution including the management of the private key of the access certificate.
Hash	Fingerprint or unambiguous image of a document, i.e. a large character string (e.g. the document) is converted into a small characteristic character string, which can only be created from the large character string. This means that all signature operations can be performed on the hash and do not have to be performed on the document itself. The content of the hash cannot be used to infer the content of the document, i.e. the hash can only be determined the other way round on the basis of the document.
HSM	Hardware security module refers to a device for the efficient and secure execution of cryptographic operations. In particular, the private keys for the certificates are generated and managed here and thus offer the best possible protection against an external attack.
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 also 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 and audited identity checks for authentication, the registration takes place with an initial authentication and acceptance of the terms of use. Example: a bank. However, an IdP can also only provide the authentication means as a signature approval method and have this coupled with the results of an identity verifier.
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.

Term	Description
LTV / long-term validation	If a signature is created with a time stamp and various information on the revocation or validity of the signature certificate and the higher-level issuing certificates and root certificates is added to the signature, the signature contains all the verification information that allows this signature to be verified in the future if the signature certificate itself or the issuing certificate or the root certificate has lost its validity. The validity information also includes the certificates for the validity service, the so-called OCSP service (Online Certificate Service Protocol), where the validity of certificates can be requested online. Such signatures can be validated over a long period of time.
Mobile ID	Managed service for secure user authentication. Mobile ID can be obtained from various providers, including Swisscom (Schweiz) AG.
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 initiating 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.
Terms of Use (Subscriber Agreement)	Provisions every user must accept before cooperating with a trust or certification service as required by law. 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 terms 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 available at https://trustservices.swisscom.com/repository.
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.
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 support 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. This verifies the "ownership" factor of a mobile device with the specified mobile number.
OU entry	Organisational unit entry, an identifier in the distinguished name of a certificate that specifies the organisational unit under the leading organisation.
PAdES	PAdES (PDF Advanced Electronic Signatures) is a set of restrictions and extensions for PDF files to make them more usable for electronic signatures. They have been standardised by the European Telecommunications Standard Institute (ETSI) under ETSI EN 319 412. In the EU, the standard is mandatory for electronically signed documents by the EU Commission's Implementing Decision 2015/1506.
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 can also be used. This makes it possible to approve signatures independently of a mobile number or even a smartphone.
Personal signature	Signatures by natural persons as opposed to seals.
PKCS#1	Cryptographic standard of the RSA Laboratories for encryption.
PWD	Password (-entry), password to be used for authentication at the service or signature approval, which offers the factor "knowledge".

Term	Description
RA	Registration Authority
RA Agent	Authorised operator of the RA App
RA agency	Organisation providing the RA agents
RA app	App (application) downloaded from the Android or iOS store. This enables a trained RA agent to identify signatories for advanced and qualified signatures and transmits the data to the RA Service of Swisscom Trust Services. The RA agents work 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 and other registration means.
Registration Authority (RA)	Internal or (partly) external delegated body that takes over the registration.
Registration	Registration always consists of identification, acceptance of the terms of use and assignment and verification of a signature approval method.
RFC3161	RFC (Request for Comment) is an Internet standard. RFC 3161 standardises the time stamp protocol and defines the exact formats of the request to a time stamp service and the responses. Swisscom Trust Services follows exactly the formats of this protocol but embeds the request in its own Signing Service interface, also for billing purposes. This means that a so-called RFC 3161 URL is not available.
RoW	Rest of World - this means the countries outside Switzerland that are not part of the EU or the EEA.
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.
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.
Seal Requester	Organisation (legal entity, administrative units, etc.) that is a UID entity within the meaning of Article 3 paragraph 1 letter c of the Swiss Federal Act of June 18th, 2010, on the Business Identification Number (UIDG) or legal entity within the meaning of the eIDAS Regulation on whose behalf a digital certificate has been issued by Swisscom Certification and Trust Services. Based on this certificate an advanced or qualified electronic seal is issued. Future seal requester must first apply for the issuance of a digital certificate to the relevant Swisscom Certification or Trust Service. Until the application is approved by the relevant Swisscom Certification or Trust Service, seal requesters are applicants (who cannot create seals if the application is rejected).
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 based on one factor. With the signature approval, the signatory expresses his will to sign.
Signatory	Natural person who electronically signs a document with prior identification and signature approval.
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.

Term	Description
Smart Registration Service (SRS)	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 methods 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 historical reasons, there is also a direct SRS interface for mobile number-based signature approval procedures. 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, provided that 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.
SSL/TLS	Secure Socket Layer, Transport Layer Security, encryption protocol for secure data transmission on the Internet based on SSL (access) certificates.
TAV	Technical Administrative Regulations on the Signature Act ZertES of Switzerland.
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 authorisation by the Seal Requester sending or handing over the access certificate electronically to Swisscom Trust Services or accepting the access certificate authorised 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.
Token	See Access Token.
UID unit	Organisation pursuant to Art. 3 para. 1 let. c UIDG to which a company identification number (UID) has been assigned for unique identification. Only UID units can be issuers for Swiss electronic seals according to CP/CPS.
UIDG	Swiss Federal Act of June 18th, 2010, on the Company Identification Number
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.
UUID	A Universally Unique Identifier (UUID) is a 128-bit number used for identification in computer systems. It is used by Swisscom Trust Services as an identifier for access certificates.
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.

Term	Description
Webauthn	WebAuthn is a standard published by the World Wide Web Consortium (W3C) as part of the FIDO2 standard for an application programming interface (API) with which web applications and websites can offer their users direct authentication using the public key procedure (Passkey) 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.
X.509	X.509 is an ITU-T standard for the creation of digital certificates and specifies the certificate structure.
Timestamp	Confirmation that certain digital data is available at a certain time. The structure of the time stamp is based on RFC 3161.
ZertES	Swiss Federal Act on Certification Services in the Field of Electronic Signature and Other Applications of Digital Certificates
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.
Access certificate	Certificate which authenticates the Subscriber application's access to the Signing Service and Multiple Authentication Broker and is used for encrypted communication with the Signing Service and the Multiple Authentication Broker. It is an SSL/TLS access certificate with a unique identifier (UUID) created by Swisscom Trust Services based on a certificate request (CSR) submitted by the Subscriber. The Subscriber holds the private key for this CSR. The specification is included in the acceptance declaration. In the case of a seal application due to the lack of individual signature approval, if the Subscriber and seal requester are not identical, in addition to the handover of the access certificate to Swisscom Trust Services, written approval of the seal requester is also required, which permits the use of the access certificate to create electronic seals on behalf of the seal requester via the Subscriber's application to Swisscom (Switzerland) Ltd or Swisscom ITSF. In the case of a regulated certificate, the seal requester always retains access to the private key of this access certificate and hands it over in person to a representative of the relevant Swisscom Certification or Trust Service.

4 Characteristics and options

Standard version	Electronic personal signatures
Platform for obtaining identifications, signature approval methods and electronic signatures, seals, or time stamps	●
Personal signature: Qualified electronic ZertES	○
Personal signature: Advanced electronic signature for Switzerland	○
Qualified electronic time stamp ZertES/eIDAS	○
Regulated seal ZertES	○
Advanced seal for Switzerland	○
Authority seal for Switzerland	○
Personal signature: Qualified electronic signature eIDAS (EU)	○
Personal signature: Advanced electronic signature eIDAS (EU)	○
Qualified seal eIDAS (EU)	○
Advanced seal eIDAS (EU)	○
Registrations in selected Swisscom Shops	●
Registrations by RA App	○

Standard version	Electronic personal signatures
Access to the Store Registration methods and signature approval methods	●
Data retention in Switzerland	●
Operation and issuance of all certificates, signatures, seals, and time stamps according to certificate guidelines (CP/CPS)	●
Use for signatories domiciled in Switzerland, the EU and the EEA	●
Use for signatories domiciled outside Switzerland, the EU and the EEA	○
Limitations of liability in the certificates	○

 = Standard (included in the price) = Against surcharge

4.1 Definition of performance

Provisioned service part	Definition
Platform for obtaining identifications, signature approval methods and electronic signatures, seals, or time stamps	With access to the Registration Service & Signing Service Platform, Subscribers have the option of obtaining signatures, seals and/or time stamps for a hash of a document. The option of service must be ordered in the order form. For a signature, the signatory must be registered to approve the signature later on. The platform offers access to various identification options and signature approval methods. These can also be selected and ordered individually in the order form and are described in the service description for the registration and signature approval methods. In addition and in connection with the service "Onboarding Support", the inclusion of own identification procedures and approval methods is also possible. In this case, an audit will usually be necessary as well as additional project and consulting services. The Multiple Authentication Broker coordinates the registration and signature approval process in advance of the signature. The signature application therefore first communicates with the Multiple Authentication Broker and receives the authorisation code via the OpenID Connect (OIDC) protocol and uses this to acquire the access token for the signing service for the hash signature.
Personal signature: Qualified electronic signature ZertES	Qualified electronic signature according to Art. 2 let. e ZertES.
Personal signature: Advanced electronic signature for Switzerland	Advanced electronic signature according to ETSI standard 319 411 "NCP+" and according to CP/CPS of the certification service of Swisscom (Switzerland) Inc., Switzerland.
Qualified electronic time stamp ZertES/eIDAS	Qualified electronic time stamp according to Art. 2 let. j ZertES and according to Art. 3 No. 34 eIDAS-VO. In principle, a qualified electronic time stamp is always included with all signatures and seals, unless otherwise stated.
Regulated seal ZertES	Regulated electronic seal pursuant to Art. 2 let. d ZertES: an advanced electronic signature created using a secure seal creation device pursuant to Art. 6 ZertES and based on a regulated certificate that is valid at the time the electronic seal is created. The seal certificates can be issued exclusively in the name of a UID unit.
Advanced seal for Switzerland	Advanced electronic seal according to ETSI standard 319 411 "NCP+".
Authority seal	Authority seals are regulated seal certificates issued for authorities in accordance with the "Technical Administrative Regulations" (TAV) to the ZertES of March 15th, 2022. These are issued by Swisscom (Switzerland) Ltd with the regulations specified in chapter 2.3.4 a) of the TAV regarding the authority designations in the OU fields, but without the optional field businessCategory according to 2.3.4 b) of the TAV.
Personal signature: Qualified electronic signature eIDAS (EU)	Qualified electronic signature according to Art. 3 No. 12 eIDAS-Reg.
Personal signature: Advanced electronic signature eIDAS (EU)	Advanced electronic signature according to ETSI standard 319 411 "NCP+" and according to Art. 3 No. 11 eIDAS-Reg.
Advanced seal eIDAS (EU)	Advanced electronic seal according to Art. 3 No. 26 eIDAS Regulation and according to ETSI Standard 319 411 "NCP+".

Provisioned service part	Definition
Qualified seal eIDAS (EU)	Qualified electronic seal pursuant to Art. 3 No. 27 eIDAS Regulation. This can only be issued in the name of a legal person within the meaning of the eIDAS Regulation.
Registrations in selected Swisscom Shops	In selected Swisscom shops (see overview on https://srsident.trustservices.swisscom.com/) in Switzerland, a future signatory can be identified free of charge in the face2face procedure and register the following signature approval methods: • Mobile ID App • Mobile ID on Swiss SIM card • Password in combination with one-time code via SMS For this purpose, the Mobile ID app must be installed before registration, or the Mobile ID must be activated on the Swiss SIM card at mobileid.ch. After registration, the future signatory receives an SMS on his smartphone at the mobile number provided during registration with links to the terms of use of the Swisscom Certification and Trust Services and must confirm these with a signature approval method. Afterwards, he can use the selected signature approval method for all signatures until the expiry of the validity of his ID document or for a maximum of 5 years. The signature approval methods are described in the service description for the registration and signature approval methods. Further signature approval methods and identification methods will be added on an ongoing basis.
Registrations by RA App	The RA-App is an app that enables individuals from an RA agency to carry out face2face identifications. For example, the RA agency may also be the Subscriber itself and must enter into a contract with Swisscom Trust Services. Further details can be found in the separate "RA-App" service description.
Access to the Store Remote registration methods and signature approvals	Swisscom Trust Services offers via the Multiple Authentication Broker (MAB) various remote identification and signature approval methods in the so-called store concept. This means that the possibility to use ordered identification procedures and signature approval methods can be configured within the scope of a signature application. In this case, a regular provision fee can be waived according to the order form. In addition, usage fees can also be charged by the Subscriber who embeds this store in his signature flow. In the store, Swisscom Trust Services offers are provided, such as the Mobile ID, Mobile ID App, the password/one-time code approval procedure or a signature approval app, as well as offers from third parties, e.g., Passkeys/FIDO2 or apps from selected IdPs. In this case, the services of third parties are resold by Swisscom Trust Services. The services are described in separate service descriptions and are subject to their own SLA and participation requirements by the user of these services. Within the scope of the store concept, Swisscom Trust Services offers that audited and approved IdPs and identity verifiers as well as signature approval methods of the Subscribers are also resold. As a reseller, Swisscom Trust Services charges a support and service fee on the purchase prices offered. The store concept is described in the service description for the registration and signature approval methods.
Data retention in Switzerland	The data storage of personal data from the certificates and the evidence data transmitted to Swisscom Trust Services takes place only in Switzerland in accordance with the relevant provisions of Swiss data protection legislation and in compliance with the EU's DSGVO and Switzerland's DSG. The data processing by the registration and/or signature approval methods partly provided by partners may - depending on the type - also take place abroad. Mobile ID and password processing only takes place on Swiss servers. The SMS with the one-time code is sent from Switzerland or the EU.
Operation and issuance of all certificates, signatures, seals, and time stamps according to certificate guidelines (CP/CPS)	The operation of a certification service provider of Switzerland or the trust service provider of the EU and the issuance of the relevant certificates, signatures, seals, and time stamps is governed by the certificate guidelines (CP/CPS) for the issuance of certificates of the "Diamant" (qualified) and "Saphir" (advanced) class in the respective legal area of Switzerland or the EU/EEA. These can be accessed in the current version here: **https://trustservices.swisscom.com/repository/**

Provisioned service part	Definition
Use for signatories domiciled in Switzerland, the EU and the EEA	The terms of use only meet the legal requirements for signatories domiciled in Switzerland, the EU and the EEA. This means that the service is only intended for signatories domiciled in these countries without ordering additional options.
Use for signatories domiciled outside Switzerland, the EU and the EEA	Due to possible country-specific legal requirements, the currently available terms of use cannot be used for signatories residing outside of Switzerland, the EU and the EEA. There is a risk that the issued signature will be invalid. If the service is intended to offer to signatories outside Switzerland, the EU and the EEA, this must be checked legally and technically (e.g., with regard to the use of the signature approval methods and the encryption requirements). If necessary, the terms of use must be adapted based on the consumer law regulations and the technical signature approval options must be checked and made available. This is possible by mutual agreement and against a separate offer from Swisscom Trust Services.
Limitation of liability in the certificates	It is possible to issue certificates with a liability limit within the meaning of Art. 13 (2) eIDAS or Art. 7 (3) c and d ZertES. In this case, the certificate shows the upper liability limit as the parameter "QcEuLimitValue" in EUR. The limitation of liability only applies on special request or for signatures issued to signatories domiciled outside the EU/EEA and Switzerland.

4.2 Certificate content

4.2.1 Personal signatures

Personal signatures contain the following information in the certificate (Distinguished Name):
Common name= <First name, last name of the signatory>
givenname= <First name(s) according to ID document>
surname= <Last name(s) according to ID document >
country= <Country of residence or home country of the signatory >
serialnumber= < evidence ID in the RA Service or other serial number in the case of a customer specific identification>

Alternatively, pseudonymized certificates can be used:
Common name= <First and last name of the signatory> OR PSEUDONYM:<other information related to the signatory>
pseudonym= <mobile number in the international format or evidenceID>
country= < Country of residence or home country of the signatory >
serialnumber= < evidence ID in the RA Service or other serial number in the case of a customer specific identification>
Please note that validators will issue a warning in case of use of pseudonyms.

The service description for the registration and signature approval procedures describes the Fasttrack procedure, which allows the approval of advanced electronic signatures via a mobile number registered in Switzerland without prior registration and utilises the legal identification requirement for SIM issuance in Switzerland. Fasttrack certificates (Switzerland/AES) contain following fields:
Common name = <Mobile number of the signatory with prefix "417">
pseudonym= <Mobile number of the signatory with prefix "417">
country = "CH"
serialnumber= <Current date in the format YYYYMMDD>-<Mobile number of the signatory with prefix "417">

4.2.2 Seal

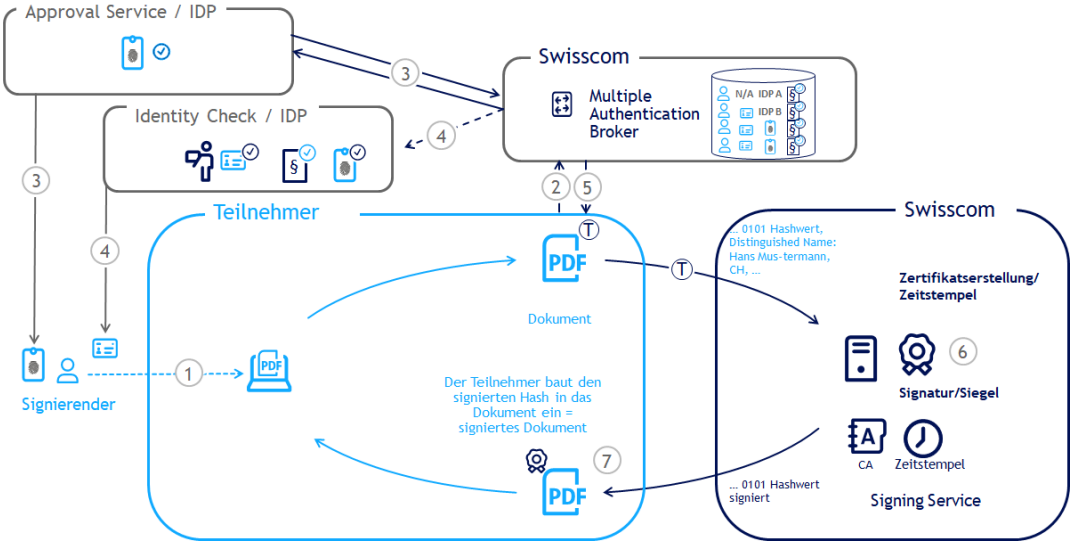
Seals contain the following information:
Common name: <Denomination according to the seal certificate request of the seal requester>
Organization: <Exact designation according to the registry, UUID registry, TAV, etc.>
Organizational Unit:<Unit within the organization (optional)– or designation for the authority seal in Switzerland. Organizational names of other organizations are not allowed.>
Country: <Country of the Organisation, or original country of the registry>
Locality: <Town / city of the organization (optional)
State: <Canton, state etc. of the organization (optional)
organizationIdentifier: <Switzerland: UUID – EU: Registry abbreviation and registry number>

4.3 Signature creation procedure for all options

The Subscriber Signature application has two main endpoints:

- Multi-Authentication Broker: This broker accepts signature requests and checks the signature approval against the signature approval method stored during registration. If necessary, it offers a registration using one of the procedures offered by the registration method store if the signatory is not already registered. In accordance with the Open ID Connect standard protocol, the Multi-Authentication Broker issues an authentication code to get an access token to the Signing Service.
- Signing Service: Based on the access token, the Subscriber application can make a signature request and send the document hash along with the signature. The hash is returned signed and must now be reassembled in the signing application to form a complete signed document (e.g., PDF).

Registration can either be done in advance, e.g., by visiting a shop, using the RA app, via the Swisscom Trust Services registration portal or via a registration portal offered by the Subscriber via direct access to the Smart Registration Service, or the person is registered via the remote identification methods available in the shops. The registration and unlocking methods are described in a separate service description.



- A signatory wishes to sign a document (1). The document is displayed in the Subscriber's signature application.
- The Subscriber first sends an authorisation request to the Multi-Authentication Broker (2). This request already contains the hash of the documents to be signed, as well as the legal area and the signature type (FES/QES), as well as any other process parameters. The Swisscom system looks up in the Swisscom RA database which signature approval methods the signatory has deposited during registration. This can also be offered by a delegated service (e.g. an IdP), which ensures the signature approval with its own authentication means. For this purpose, the Subscriber application can provide a hint ("login_hint" for e.g., an e-mail/mobile number or "IdP_hint" for an IdP). If there is no hint, the signatory is prompted to select the signature approval method stored during registration.
- The Multi Authentication Broker now connects to the signature approval service (3), which can be an internal service such as Mobile ID or a delegated service of a partner a standard service like Passkeys/FIDO2 (via webauthn) or external IdP, e.g., a bank. During this OAuth authentication request call, the signer must initiate the signature approval, e.g., by approving it with a fingerprint in a signature approval app. For qualified/regulated signature certificates, a two-factor signature approval is required; for advanced signatures, a one-factor signature approval is sufficient. A check is made to see if the user has already been registered in combination with the chosen signature approval method. If the signature approval fails, there is a maximum of 5 attempts. After that, the user has to register again.
- If the signatory is not already registered, an identification procedure or IdP is offered for registration which is appropriate for the legal area, the signature level (FES/QES) and the selected signature approval method. If not configured otherwise, a "store" is opened in the signature flow where different registration options are offered (see

separate service description). The selected identification service is requested by the Swisscom system to perform the identification (4). The registration always consists of the following steps.

- Verify identification or establish identity
- Use of the signature approval method
- Acceptance of the terms of use for the signature service of the Swisscom Certification and Trust service.

In the case of an IdP, pre-existing identities are used, i.e. authentication takes place against the IdP. This authentication method is also used later for the approval of the signatures. Only the acceptance of the terms of use is required.

- If the signature approval is OK - after registration, if applicable - the Swisscom Multiple Authentication Broker returns an authorisation code to the Subscriber application, which the signature application can then use to request the access token (T) for the signature (5).
- With the token (T), the Subscriber application now requests a signature from the Signing Service. The protocol is based on the ETSI EN 119 432 standard for remote signatures. Only the hash of a document is transmitted to the Swisscom systems, not the entire document. The signature service immediately returns the signed hash. The Subscriber application can also obatin a timestamp. (6) Both can be combined with information on the certificate chain up to the trusted root certificate and information on the revocation status of the certificates in the document to create a long-term validated signed document (LTV). (7)
- For personal signatures, the Swisscom Certification or Trust Service usually uses a short-term certificate that is only valid for the respective signature request. The corresponding key pair is generated for a short living time and then deleted.

Seals are usually based on long-term certificates issued to an organisation. In the case of organisations, signature approval can also be permanent without individual approval, e.g. via a permanent certificate-based approval, where the private key is managed by the person responsible for the organisation. In this case, the Conditions of Use for Seal Creation must always be agreed with Swisscom Trust Services as to how the permanent approval can be carried out in compliance with the regulations and the law. In particular, the requirements of CEN/TS 419 241-1 must be observed.

Timestamps are structured according to RFC3161, but the RFC3161 protocol for issuing timestamps is not followed.

Batches of signatures can also be processed in one request (a maximum of 250 hashes can be included). The signature certificate contains the last name, first name, country and a serial number or a pseudonym instead of the last name and first name. Typically, the Signing Service compiles the certificate content from the information provided by the IdP or the RA database.
The signed hash value is returned in the CMS or PCKS#1 standard.

The process above can also vary due to process parameters that are specified. For example, it is possible to initiate a one-shot process that enables signature approval by identification only without signature approval means.

4.4 Process and tools for personal identification (registration office)

Before a signature can be approved, the signatory must identify and register himself in accordance with the requirements of the respective type of electronic signature. The identification process can be carried out separately from the signature process by a so-called registration authority, for which Swisscom Trust Services offers several variants:

- The Subscriber can be enabled to identify colleagues, customers, and partners locally for the Swisscom Certification and Trust Services in the face2face procedure. The RA application can be used for this purpose. This must be ordered separately and is described in a separate "Service Description RA-App".
- The Subscriber may use an online identification procedure offered by a Partner as part of the Smart Registration Service as a remote identification procedure on its own registration portal. These are described in the service description for the registration and signature approval methods and must be ordered separately.
- Swisscom Trust Services also offers online registration options for direct purchase via voucher codes or direct payment via its own registration portal https://srsident.trustservices.swisscom.com. These procedures are also described in the service description for the registration and signature approval methods.
- Within the signature flow, the Multiple Authentication Broker detects if a person is not registered and then offers various online registration options directly through a 'store'. The options can be configured on a Subscriber-specific basis and are subject to additional charges as per the order form or contract. Please also refer to the service description for the registration and signature authorisation procedures.
- IdPs can also offer their users or via the Smart Registration Service registrations with authentication means that are also used in other signature applications for expressing will to approve a signature. Based on the commitment of the IdP these procedures are then also offered in the store.
- Alternatively, the signatory can also be identified on site in the Swisscom shops (Face2Face).

- The subscriber can use their own identification methods and set up a registration authority with project-specific identification themselves, thereby assuming the role of an IdP. This procedure must be agreed in advance with Swisscom Trust Services and developed as part of a signing onboarding project. For this purpose, the subscriber must submit an implementation concept, which will be reviewed and evaluated by Swisscom Trust Services. As a rule, individualised registration authority processes for subscribers must also be approved by the recognition body or conformity assessment body for certification services or trust services. The registration data can either remain with the subscriber or be transferred to the Swisscom Smart Registration Service, depending on the type. A separate order is required for this. The process is described in the Onboarding Support service description.

Data of the own identification method or the IdP is provided to Swisscom as evidence and managed by Swisscom in the RA database. It is possible that only the reference to this data is archived and the actual data record then remains with the identifying party. The storage concept of the data must then be audited accordingly and commissioned as part of the onboarding support. A record includes:

- Use in relation to the quality of the signature (e.g. advanced / qualified / regulated)
- Use in relation to the applicable jurisdiction, e.g. Switzerland, EU/EEA, depending on the application.
- Use in relation to the allowed validity period of the evidence
- Required signature enabling device for use, unless an IdP is responsible
- Competent IdP (if registered) for signature approval
- Evidence of the identification itself (e.g., photo of the ID card/passport or other suitable evidence)

The RA database also compiles the necessary information for the certificate for the managed evidence: First name, last name and country as well as the serial number.

4.5 Organisational review process

If an organisation is to be named in the certificate, Swisscom Trust Services shall carry out an organisation check in accordance with the provisions of the CP/CPS before commencing the service. In the case of personal certificates, the organisation must be named in the declaration of acceptance and an authorised representative of the organisation must have signed the declaration of acceptance. By signing, the representative also gives permission for the organisation's name (optional) to be used in connection with the signatories.
In the case of seals, the Registration Authority checks the seal requester beforehand against entries in the Register and accepts an application from an authorised representative of the applicant for the seal. This representative must appear in person before an authorised person appointed by Swisscom Trust Service (e.g., identification with RA app). In the case of two authorised signatories, another representative of the seal requester must also sign. The application and other submitted documents are checked and archived. The signatures must be qualified electronic signatures and must have been enabled with a Mobile ID or password/one-time code process. The phone number used with the Mobile ID or password/one-time code allows the seal certificate to be revoked in the event of compromise (see below).
Once the application has been approved, the key material is generated and stored on the Signing Service platform for the seal requester. For this key pair, a corresponding long-term seal certificate (usually 3 years) is issued in accordance with the certificate policy of Swisscom (Switzerland) AG or Swisscom ITSF and the subject of the seal certificate named in the seal certificate application (Distinguished Name of the seal requester).

4.6 Revocation (invalidation) of a seal and/or access certificate

Seal certificates and the corresponding access certificates must be declared invalid by the seal manufacturer if misuse or compromise become apparent. The Swisscom system will then issue a new seal certificate, if necessary, on the basis of a new access certificate.

The revocation must be notified by the representative of the seal requester named in the certificate application, whose means of authentication (mobile phone number) has been deposited with Swisscom Trust Services. This can be done online at

https://trustservices.swisscom.com/repository. A revocation request is verified by means of the deposited mobile phone number or the authentication method used for the personal signature of the request. Other revocation procedures are possible in accordance with the provisions of the CP/CPS.

4.7 Timestamps

Time stamps do not require registration of the person or organisation. They are based on the same interfaces as signatures and seals and follow the RFC3161 standard.

4.8 Process for testing a Subscriber application

As Swisscom (Switzerland) Ltd or Swisscom ITSF is liable for the correct issuance of signatures and seals to the signatory or third parties, the responsibility for the issuance of signatures and seals extends to the correct processing in the Subscriber application. For this purpose, the Subscriber or seal requester must sign a declaration of acceptance, in which obligations such as the generation of TLS/SSL access certificates, the prevention of the exchange of a document hash, the protection of the application or, in the case of seals and time stamp services, the signing of the terms of use are guaranteed.

4.9 Data storage and responsibilities

When using the registration procedures and signature approval methods of the Smart Registration Service provided by Swisscom Trust Services, the data on the identified person transmitted to Swisscom Trust Services, as well as the identification documents and proof of acceptance of the Terms of Use, are stored exclusively on Swisscom servers in Switzerland and are retained in accordance with the time limits set out in the CP/CPS or in accordance with the law. External registration authorities and registration agencies process your data in accordance with the respective service description of the registration and signature approval methods and RA-App. Except for RA agencies, external registration authorities are usually independent data controllers.
The Subscriber as provider of the signature application is also an independent data controller. Swisscom Trust Services has a direct contractual relationship with the signatory via the terms of use and processes the signatory's data in this direct relationship. The data of the Subscriber is not processed.

5 Performance presentation and responsibilities

5.1 Signature service

One-off benefits

Activities (S = STS/T = Subscriber)		S	T
Provision of the service			
1.	Inform signatories that a signature can only be made after proper registration with a signature approval method (e.g., by registration to Swisscom Trust Services). It should be noted that not all users can be registered, e.g., due to insufficient identity documents that are not suitable for machine registration or a negative risk assessment.		✓
2.	Provision of the Signing Service infrastructure	✓	
3.	Provision of the SAIP interface based on ETSI EN 119 432 standard adapted for the use of short-living signature certificates. The interface is available at https://documents.swisscom.com/product/filestore/lib/e2007490-6fd4-4012-801d-b104801a9abc/reference_guide_smartregistration_signing-en.pdf?idxme=pex-search	✓	
4.	Compliance with regulatory requirements when composing the signature from the signed hash (e.g., compliance with the PAdES standard, observance of long-term validation) - see also the Reference Guide.		✓
5.	Sending the signed declaration of acceptance with the information required for regulatory purposes.		✓
6.	Option "organisation entry in the signature certificate" for personal certificates: Provision on request of Swisscom Trust Services of all necessary documents for organisation verification (e.g., certified extract from the commercial register). Signature in the declaration of acceptance by a representative authorised for the organisation to agree that the organisation authorizes the use of the organisation name in the certificate for the signatories.		✓
7.	Option "Organisation entry in the signature certificate" for personal certificates: Check the authorisation to use the organisation name in the certificate.	✓	
8.	Seal" option: Provision of an application for a seal certificate signed by the seal requester with all necessary documents to verify the seal requester (e.g., certified excerpt from the commercial register in the case of a regulated or qualified seal) as well as agreement to the terms of use of the service. Signature in the application for the seal certificate by a representative authorised to sign for the seal requester. Arrangement of identification by personal appearance of a representative of the seal requester or by qualified electronic signature on base of an RA app registration. The Subscriber shall ensure that the OU entry (organisational unit) in the seal application does not collide with another organisation in terms of name law.		✓
9.	Seal" option: ensuring that an access certificate is sent to Swisscom Trust Services by the seal requester or his authorised representative with confirmation of power of attorney.		✓

Activities (S = STS/T = Subscriber)	S	T
10. Seal" option: If regulated or qualified electronic seals are created, a signature approval method approved by Swisscom Trust Services must be followed and described in a "Conditions of use for seal creation" document. Swisscom Trust Services will release a procedure with dedicated partners and conclude a contract for the "release solution seal".		✓
11. Option "Personal Signatures/Timestamp": Sending a CSR for generation of an access certificate for authentication towards the Multiple Authentication Service and for encrypted communication with the Signing Service. For specification see declaration of acceptance. The same certificate is used.		✓
12. Option "Personal Signatures": The allowed signature approval method and registration method must be enabled during the signature. These are configured in the "Store" (see separate service description). The signatory shall be informed of this. If the signatory has not been registered with one of these signature approval methods, a new registration is necessary for the use of the Subscriber application.		✓
13. Activation of the communication channels for the configured access certificate based on the CSR.	✓	
14. If necessary, configuration of the firewall, on the server side at the Subscriber.		✓
15. Appointment of a contact person for all questions regarding technology, security and implementation of the registration of signatories and contact person for audit questions.		✓
16. Connection of the Subscriber and sending of the Subscriber-specific access data.	✓	
17. Integration of the Signing Service into the Subscriber-specific application(s) or Subscriber-side connection of the interface to the Signing Service and, if necessary, multiple authentication broker, e.g., by using a partner application.		✓
18. Checking access to the Signing Service and, if applicable, Multiple Authentication Server and the issuing of signatures or seals or time stamps. Immediate reporting of any errors before the signatures are used.		✓
19. Troubleshooting by update or new installation.	✓	
20. Notification of the cessation of business activity as well as a threat of bankruptcy directed against the Subscriber, the opening of bankruptcy proceedings that has taken place or a debt-restructuring moratorium.		✓

Termination of the service

1. Deleting the Subscriber authorisations in the Signing Service infrastructure.	✓	
2. Deleting the keys from the HSM.	✓	

Recurring services

Activities (**S = STS/T = Subscriber**)	S	T
Standard services		
1. Operation of the Signing Service and Registration Service infrastructure.	✓	
2. LifeCycle Management of the Signing Service and Registration Service infrastructure.	✓	
3. LifeCycle Management of the Subscriber's infrastructure: adaptation to the current state of technology and security (security patches, updates, etc.).		✓
4. Appropriate technical and organisational measures to protect the data transmitted by the Subscriber application (e.g. also by disabling accesses that are not required, access regulations, etc.). Disclosure of the security arrangement of the Subscriber application and the communication to the Swisscom Certification and/or Trust Service, if required by Swisscom Trust Services or the supervisory body of Swisscom (Switzerland) Ltd or Swisscom ITSF.		✓
5. Adaptation of the definition of safety requirements.	✓	
6. Lifecycle management of the SSL/TLS access certificate: Option "personal signatures" and "time stamp": timely exchange on expiry by the designated security officer by e-mail of the CSR to **sts.salessupport@swisscom.com** under designation of the account name. "Seal" option Timely replacement before expiry of the validity by the seal requester himself by e-mail to the 1st level support of Swisscom Trust Services under designation of the claimed identity.		✓
7. Creation of signature certificates, seals, and time stamps according to the X.509 standard.	✓	

Activities (**S = STS/T = Subscriber**)	S	T
8. Definition of the signature/seal certificate contents and procedures for signature and seal creation.	✓	
9. Option "personal signatures": Ensuring the use of technical signature approval devices and contractually agreed signature approval method (e.g., Mobile ID, Mobile ID App, PWD/OTP, etc.). Display of the approved signature approval methods in the webview (store).	✓	
10. Option "personal signatures": Ensure in advance that only those signatories participate in the signature who are registered and authorised with the corresponding means of signature approval for the signature type, otherwise they will be forwarded to the identification service (optional depending on the configuration). Display of the mutually agreed identification methods in the webview (store).	✓	
11. Option "Personal signatures": Addressing the registered signature approval method, provided that a registered reference to the signatory (e.g., mobile number, uuid, e-mail, etc.) is included in the signature request.	✓	
12. Execution of signatures if approved by the signatory.	✓	
13. Signature in conjunction with a qualified time stamp according to ZertES and eIDAS.	✓	
14. Ensuring the confidentiality of the data exchange between the Swisscom Certification and/or Trust Service and the Subscriber (e.g., avoiding "inspection" modules to break the TLS connection).		✓
15. If regulated or qualified electronic seals are created: Selection of a cryptographic module or HSM that blocks access to the Subscriber application at the latest after 5 failed attempts to authenticate to the service. A new access certificate must be created after a blocking in a joint ceremony with Swisscom Trust Services.		✓
16. Option "Seal": Transmission of the data of the seal requester (Distinguished Name) according to the specifications in the certificate request of the seal requester and in the acceptance declaration.		✓
17. Ensure that the safety officer fulfils his obligations and requirements.		✓
18. Provision of support services (service desk, incident management, etc.)	✓	
19. Counting of all signatures, identification and signature approval requests according to the billing model and summary billing to the Subscriber. There is no reporting on the level of the individual signatory. Information on this is only available using anonymised data in the event of support.	✓	
20. Establishment of a billing system and counting of all signature requests and billing with the signatory or allocation of signature requests to different end customers of the Subscriber. All possible signature approval methods and optional identifications performed by a signatory within the scope of this signature must be included in the billing.		✓
21. Reporting changes to Subscriber-specific information (contact persons, SSL/TLS access certificate, etc.)		✓
22. Updating of Subscriber-specific information (contact persons, SSL/TLS access certificate, etc.)	✓	
23. Reporting security incidents on the Subscriber application system that affect the Signing Service or Registration Service.		✓
24. Reporting of security incidents on the system of the signature or Registration Service that have an impact on the Subscriber.	✓	
25. Decision and responsibility for legal effects of the selected signature type or signature level (cf. chapter 8.2)		✓
26. Indication to the signatory whether it is an advanced or qualified signature or advanced, qualified, or regulated seal.		✓
27. Operation of a revocation authority to invalidate a seal certificate in case of compromise or for other reasons	✓	
28. Revocation and enabling of revocations by the seal requester in the event of signs of compromise of the seal or access certificate via a revocation procedure published by Swisscom Trust Services.		✓
29. Further development, adaptation of the interface to current regulatory and security requirements. Information on interface adaptation 3 months before release unless there is an immediate need for action by law or for security reasons. Maximum of 2 adaptations per year		✓
30. Adaptation of the interfaces to the new requirements of Swisscom Trust Services within 3 months.		✓

5.2 Option: Use for signatories resident outside Switzerland, the EU and the EEA

Activities (**S = STS/T = Subscriber**)	S	T
Services for optional use for signatories resident outside Switzerland, the EU and the EEA (in the following, the country of the signatory is referred to as "RoW country of residence", RoW = Rest of World)		
1. Fee-based assessment of the deployment options for the signatories in the intended RoW country of residence with respect to applicable consumer protection, data protection, cryptography and deployment requirements as well as technical options (e.g., SMS reception) with the involvement of experts. Depending on the results of the deployment test, deployment with the services described in the following points may or may not be possible and the Subscriber will be informed.	✓	
2. Waiving the offer of signatures for signatories domiciled in the RoW country of domicile, provided that the usage test under point 1 has shown that usage is not possible in that country of domicile.		✓
3. If the operational test is positive: Compliance with the legal requirements: • Adaptation of the terms of use respecting the appropriate consumer and data protection • Compliance with the data protection requirements of the country of residence (e.g., maintenance of a special data processing directory, appointment of a data protection officer, etc.). • Configuration with regard to permitted crypto algorithms. • Fulfilling the conditions for using the signature approval methods in the country of residence (e.g., pre-registration of SMS sender numbers, Google Play or Apple Store conditions, etc.).	✓	
4. Acceptance that registrations of the signatory in his RoW country of residence cannot take place without an adequacy decision of the Federal Council according to the planned Data Protection Act Art. 16 of the Swiss Data Protection Act or the European Commission pursuant to Art. 45 para. 3 DSGVO due to the increased data protection requirements (e.g., no use of the RA application), but only permitted remote registrations are possible (e.g., video identification).		✓
5. Acceptance that the certification or trust service may limit its liability to CHF 5,000 per signature in the certificate (QES/FES). The Subscriber must inform the signatory about this limitation beforehand.		✓
6. Acceptance of conditions for use in the country of residence: • E.g., restriction of the signature approval method to be used (e.g., sole use of Mobile ID App or sole use of a customer-specific procedure). • E.g., restrictions about the identification methods to be used		✓
7. Preparation of a linguistically adapted version of the Terms of Use or other regulatory texts for the RoW country of residence, if necessary.	✓	
8. Technical and organisational adjustments, e.g. • Extension and clarification of the registration with the registration partners of the Smart Registration Service or other registration partners or authentication partners. • Selection of suitable SMS providers, adaptation of SMS texts (e.g., Unicode specifications). • Placing the app-based signature approval method in the Google Play Store or Apple Store. • Information to the auditor or accreditation body. • Setting of the limits for liability in the certificate and in the terms of use, binding of the registered signatories exclusively to the access of the Subscriber application of this agreement.	✓	
9. Acceptance that not all signature approval method can be supported in the respective destination country (e.g., acceptance of SMS is suppressed).		✓
10. Continuous monitoring of legal regulations (changes in consumer law, data protection law, etc.) and technical requirements in the RoW country of residence, which may have an impact on signatories resident in this country. Informing the Subscriber about these changes. Preparation of an offer for required changes for the continuation of the signature offer or information to the Subscriber about the required discontinuation of the signature offer in the RoW country of residence (if possible, 3 months before entry into force).	✓	
11. In the event of required adjustments pursuant to Clause 8, commissioning of the required changes or discontinuation of the signature service for signatories of this RoW country of residence after setting a deadline.		✓

6 Service level and reporting

6.1 Service Level

The following service levels generally refer to the agreed Monitored Operation Time. 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 can be found in the contractual component "Basic Document".
The following service levels are available for the service features (see chapter 4). If there is more than one possible service level per feature, the service level will be selected in the service contract.

Service Level & Target Values			Smart Registration & Signing Service
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			
Signature service	99.8%		●
Directory services according to CP/CPS section 2.1	99.9%		●
Security			
	See base document		●
Continuity			
Service Continuity (STSSC)[3]	RTO 4 h | RPO 1 h		●

● = Standard (included in price) ○ = Against surcharge - = Not available

6.2 Service Level Reporting

On special request, a service level report on the availability of the respective month can be prepared and send to the Subscriber.

[1] If the Signing Service was obtained via a Swisscom partner, this partner must always be contacted in the event of faults. The partner will forward the fault to Swisscom if it cannot be rectified.
[2] Holiday regulation see "Basic document (chapter SLA definitions)".
[3] RTO and RPO refer only to the provision of the Signing Service at the SAIP. Mobile services used for identification, authentication or expression of will are not covered here.

7 Invoicing and quantity report

7.1 Billing

The billing details are regulated in the service contract or GTC.
Basically, there are the following billing methods:

7.1.1 Billing by retrieval - post-paid model

In this case, the quantities of signed or sealed document hashes retrieved during the last service period shall be counted and invoiced at the price specified in the Service Contract for this purchase quantity. In the case of batch signing, each contained hash is charged individually.

7.1.2 Volume-based pricing model - Prepaid model for personal signatures

In this case, the Subscriber determines both the planned service period and the planned number of signatures in advance. The Subscriber commits to this volume purchase during the service period and pays a contractually agreed price in advance, which is paid in regular instalments over the period in accordance with the service contract. Additional volumes will be invoiced later according to the price in the service contract as described in 7.1.1. It is possible to increase or decrease the volume or contract terms during the term of the contract by entering a new contract and eventually a payment of price differences. Signatures are converted into Service Units so that the Service Units purchased can be used for different products (e.g., advanced and qualified certificates or EU/Switzerland).

7.1.3 Package pricing

Packages can be offered that contain a certain volume of signatures including the necessary registrations and signature approvals. A monthly or annual flat fee is charged.

7.1.4 Payment for Signature Approvals and Registrations

These are described in a separate service specification.

7.2 Quantity report

Invoices will show the total number of hashes for the relevant service period for remuneration after retrieval. Anonymised reports of all signature queries for a service month can be requested on request to clarify problems. Swisscom Trust Services reserves the right to charge for the delivery of individual service reports in the case of regular requests. User-specific invoices are not issued. Invoices are issued per access (so-called "UUID" or "ClaimedID").

8 Special regulations

8.1 Subscriber application

The Subscriber application and a billing module for the individual signatory are not part of this service description. They are provided by the Subscriber itself, by a Swisscom Trust Services partner or by Swisscom Trust Services itself.

8.2 Signature types of the personal signature and their possible applications

It is the Subscriber's responsibility to have the legal implications of the selected type of electronic signature (with and without time stamp) made available to the signatories professionally clarified in advance. Swisscom Trust Services does not accept any responsibility for this:
Qualified Swiss electronic signature according to ZertES (QES, certificate of Swisscom (Switzerland) Ltd - class Diamant): The QES created via the Signing Service fulfils the properties defined in the CP/CPS and the definition according to Art. 2 let. e of the Swiss Federal Electronic Signature Act (ZertES; SR 943.03). Only the QES associated with a qualified time stamp is equivalent to a handwritten signature when applying Swiss law, provided that no deviating legal or contractual regulations take precedence (Art. 14 para. 2bis Swiss Code of Obligations).
Qualified electronic time stamp: The qualified electronic time stamp created via the Signing Service fulfils the properties defined in the CP / CPS and the definition pursuant to Art. 2 let. j ZertES and the definition pursuant to Art. 3 No. 34 eIDAS Regulation with the legal effects pursuant to Art. 42 eIDAS Regulation.
Advanced Swiss electronic signature (FES, certificate of Swisscom (Switzerland) Ltd -class Saphir): The FES created via the Signing Service fulfils the properties defined in the CP/CPS. The FES (in contrast to the QES) is not legally regulated in Switzerland and does not meet the legal requirement of being in writing within the meaning of Article 12 of the Swiss Code of Obligations, i.e., it does not have the same legal effects as a handwritten signature. The legal requirement of a handwritten signature (formal requirement of simple written form) can only be replaced electronically in an equivalent manner by the QES associated with a qualified electronic time stamp, which is not to be confused with the FES based on advanced certificates.

Qualified electronic signature of the EU according to eIDAS Regulation (QES, Swisscom ITSF class Diamant certificate): The QES created via the Signing Service fulfils the properties defined in the CP/CPS and the definition according to Art. 3 No. 12 eIDAS-Regulation with the legal effects according to Art. 25 eIDAS-Regulation.
EU advanced electronic signature according to eIDAS Regulation (FES, Swisscom ITSF -class Saphir certificate): The FES created via the Signing Service fulfils the properties defined in the CP/CPS and the definition according to Art. 3 eIDAS Regulation with the legal effect according to Art. 25 para. 1 eIDAS Regulation. The FES does not have the same legal effects as a handwritten signature or a QES.
Depending on the situation, certain documents therefore require the handwritten signature or the QES and, in Switzerland, combined with a qualified electronic time stamp so that intended legal effects can come into effect at all.
Electronic signatures created via Signing Service in accordance with the Certificate Guidelines (CP/CPS) for the issuance of certificates issued by the Issuing CAs "Diamant" (qualified) and "Saphir" (advanced) may, if foreign law is applicable, have different, possibly more far-reaching, or less far-reaching effects than is the case under Swiss law or under EU law.
The exchange of encrypted data and the issuing of certificates is also subject to legal restrictions in/with certain countries.
Depending on the situation, certain documents therefore require the handwritten signature or the QES and, in Switzerland, combined with a qualified electronic timestamp to have the intended legal effects.
Electronic signatures generated by the Signing Service in accordance with the Certificate Policy (CP/CPS) for the issuance of certificates by the Issuing CAs "Diamond" (qualified) and "Saphir" (advanced) may have different, possibly more or less far-reaching effects than under Swiss or EU law, if foreign law is applicable.
The exchange of encrypted data and the issuance of certificates are also subject to legal restrictions in/with certain countries.

8.3 Possible uses of the advanced or regulated electronic seal

The use of the advanced or regulated electronic seal is typically used to provide proof of the origin and integrity of the contents of a file. The electronic seal should not be confused with the legal concept of the electronic signature. In addition, the legal effects of the higher value regulated electronic seal are not the same as those of the advanced electronic seal. It is the responsibility of the Subscriber and his seal requestors to clarify the legal effects of the chosen type of electronic seal (with and without time stamp) in advance. Swisscom Trust Services accepts no responsibility in this respect.
Regulated electronic seal in accordance with Swiss ZertES (based on a certificate from Swisscom (Switzerland) Ltd. class Diamant): The regulated seal created via the Signing Service fulfils the properties defined in the CP/CPS and the definition according to Art. 2 let. d of the Swiss Federal Electronic Signature Act (ZertES; SR 943.03).
Advanced electronic seal for Switzerland (Swisscom (Switzerland) Ltd class Saphir certificate): The advanced electronic seal created via the Signing Service fulfils the properties defined in the CP/CPS and, unlike the regulated electronic seal, is not regulated by law.
Qualified electronic time stamp: The qualified electronic time stamp created via the Signing Service fulfils the properties defined in the CP/CPS and the definition pursuant to Art. 2 let. j ZertES and the definition pursuant to Art. 3 No. 34 eIDAS Regulation with the legal effects pursuant to Art. 42 eIDAS Regulation.
Qualified electronic seal in accordance with eIDAS Regulation (EU) (Swisscom ITSF Class Diamant certificate): The qualified electronic seal created via the Signing Service fulfils the properties defined in the CP/CPS and the definition according to Art. 3 No. 27 eIDAS-Regulation with the legal effects according to Art. 35 eIDAS-Regulation.
Advanced electronic seal in accordance with eIDAS Regulation (EU) (Swisscom ITSF Class Saphir certificate): The advanced electronic seal created via the Signing Service fulfils the properties defined in the CP/CPS and the definition according to Art. 3 No. 26 eIDAS-Regulation with the legal effect according to Art. 35 eIDAS-Regulation.
Neither the advanced electronic seal nor the regulated electronic seal has the same legal effects as a handwritten signature or a qualified electronic signature. Depending on the situation, certain documents therefore require a handwritten signature, a qualified electronic signature or a regulated electronic seal, if necessary, with an electronic time stamp, so that the intended legal effects can take effect at all.
If foreign law is applicable, electronic seals issued via the Signing Service may have different, possibly more far-reaching, or less far-reaching effects than is the case under Swiss law or EU law.
The exchange of encrypted data and the issuing of certificates is also subject to legal restrictions in/with certain countries.

8.4 Operation of the Subscriber application, if Subscriber and seal requester are not identical

The representative of the seal requester authorised in the certificate application must hand over the access certificate to Swisscom Trust Services or, in the case of advanced seals, agree in writing to the Subscriber handing over the access certificate to Swisscom Trust Services. This authorises the Subscriber to operate the Subscriber application for the seal manufacturer vis-à-vis Swisscom Certification or Trust Services. If the authorised representative changes, Swisscom Trust Services must be notified in writing or by e-mail by a representative of the seal manufacturer or by the previous contact person .

All documents transmitted via the interface to the Swisscom Certification or Trust Service are provided with an electronic seal. The Swisscom systems cannot check whether the access of the operator of the Subscriber application with access authorisation to the key material for the creation of the seal was authorised or error-free.

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

The signature requests (Subscriber data) transmitted by the Subscriber to the Swisscom Certification or Trust Service on behalf of the signatory as part of the provision of the service are generally processed by Swisscom (Switzerland) Ltd - also for Swisscom IT Services Finance S.E. - in Switzerland. Data processing by third parties and/or abroad shall be carried out exclusively in accordance with the relevant provisions of Swiss data protection legislation. In particular, such processing may be carried out by employees resident in the EU (cross-border commuters) or while travelling, as well as by maintenance departments of manufacturing companies from the EU. In the context of this service, the following constellations are affected by such processing:

- As a service provider, Swisscom Trust Services AG offers functions within the scope of operation and support to Swisscom (Switzerland) Ltd. and thus also processes registration and signature data under the control and on behalf of Swisscom (Switzerland) Ltd - also for Swisscom ITSF.
- Swisscom IT Services Finance S.E. processes through Swisscom (Switzerland) Ltd. the data required to provide its trust service, in particular for the issuance of electronic certificates.
- In support cases from the EU, the 3rd level support of the application manufacturer has temporary VPN access to application data at the Swisscom Certification and/or Trust Service that does not contain any personal data other than the data published by the signatory in the certificate. In individual cases, the signature data published by the signatory in the certificate and master data of the Subscriber organisation (e.g., organisation name, designation of the TLS/SSL access certificate published by the Subscriber) may also be visible to these third parties. Access is monitored in real time by a Swisscom (Switzerland) Ltd. or Swisscom Trust Services technician to ensure that no uncontrolled data access takes place and that the connection can be immediately terminated in the event of misuse. This procedure is in line with best practice in the banking and insurance sectors.
- Supervisory authorities and conformity assessment bodies from Switzerland and the EU, which must confirm the conformity of the signature application, may have access to personal and identification data within the scope of audits under the supervision of Swisscom (Switzerland) Ltd and/or Swisscom ITSF in order to be able to check the conformity of the identity checks and signature issuance. These compliance audits take place exclusively in Switzerland.