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

Service description
Smart Registration & Signing Service
incl. Docusign Connector

Swisscom Trust Services

Swisscom Trust Services Ltd

Konradstrasse 12
8005 Zurich

Switzerland

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

1 Content

Swisscom Trust Services

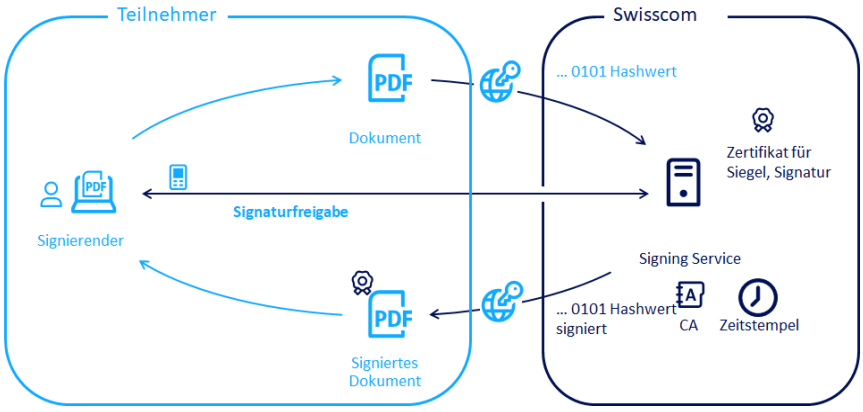
2 Service overview

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 like Docusign signature platform. 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 like Docusign 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.

With the Docusign Connector, Swisscom offers a special module that connects the standard interface of Docusign for Trust Service Providers to the remote signature of Swisscom Trust Services and thus ensures the hash transmission and embedding of the hash.



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"). For the use of identification and signature approval methods, a registration portal is available in which partners offer their identity proofing methods for registration. The available methods are described in the "Service description for registration and signature approval methods". In addition, face2face identification can also be carried out using the RA app or in a Swisscom shop in Switzerland.

The signing service offers depending on the ordered positions advanced and qualified electronic signatures for natural persons 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).

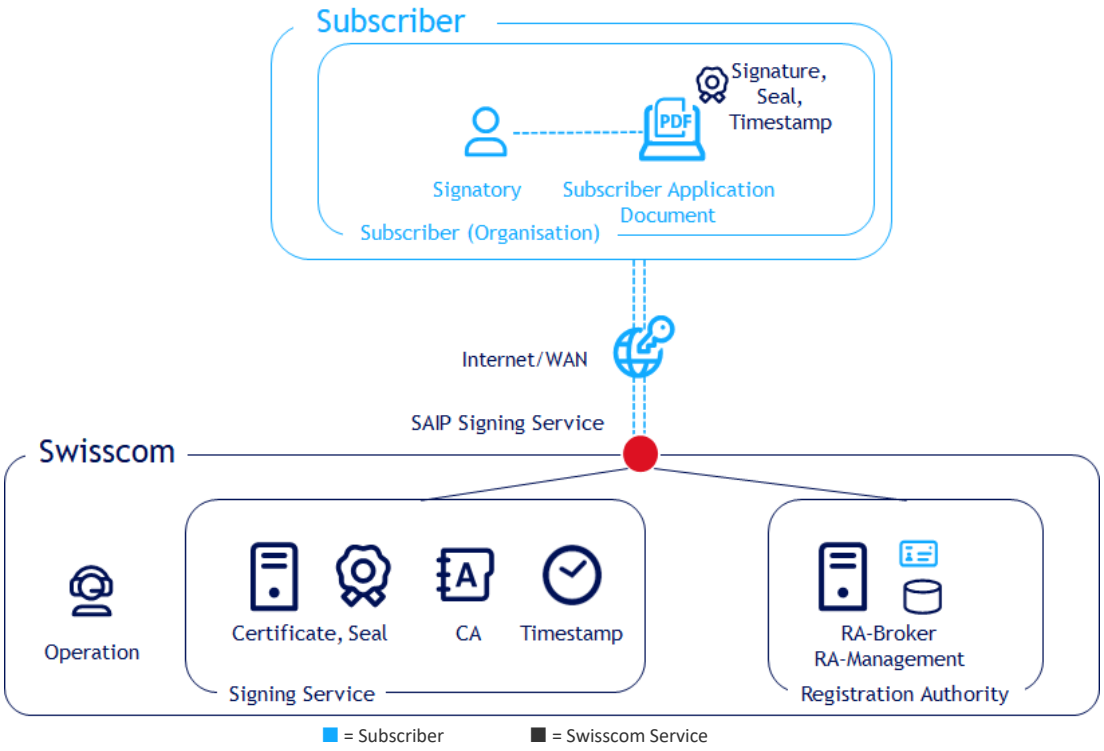
Swisscom (Switzerland) Ltd is a recognised provider of signature and certification services in Switzerland in accordance with ZertES, and Swisscom ITSF is a recognised qualified trust service provider in accordance with the eIDAS Regulation and the Austrian Signature and Trust Services Act (SVG) for the issuance of advanced and qualified certificates for electronic signatures. 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 in combination with the Docusign Connector.

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) – here: Docusign, 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 via Docusign interface https://developers.docusign.com/docs/tsp-api/tsp101/
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.
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.
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.

Term	Description
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.
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.
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.
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.
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.
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.

Term	Description
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.
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.
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.
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".
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.

Term	Description
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	Certificate issued to the signatory, administered in trust by Swisscom Certification and Trust Services and used for signature or seal creation.
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.
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.
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.
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.

Term	Description
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.
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.

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	✓
Personal signature: Qualified electronic signature eIDAS (EU)	✓
Personal signature: Advanced electronic signature eIDAS (EU)	✓
Registrations in selected Swisscom Shops	✓
Registrations by RA App	✓
Access to the registration portal for remote registration methods	✓
Identification and signature approval methods from the stores	-
Signature approval by Password and One Time Code or Mobile ID (App)	✓
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 – not (yet) provided

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 and 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

Provisioned service part	Definition
	order form and are described in the service description for the registration and signature approval methods.
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, unless otherwise stated.
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.
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 registration portal for remote registration methods	Swisscom Trust Services offers via the registration portal **https://srsident.trustservices.swisscom.com** different remote identification methods. These are offered by partners. In the scope of registration a signature approval method must be chosen and initialized to approve signatures in all future signature workflows.
Identification and signature approval methods from the stores	The connector for Docusign is not yet connected to the Multiple Authentication Broker and the associated extended methods for remote identification and other methods for signature approval. Implementation is being planned, but this means that currently only identification methods that are labelled "Portal" in the service description of the registration methods are available. "Store" methods are excluded from this.
Signature approval by Password and One Time Code or Mobile ID (App)	After the one-off registration, all signatures can be released in the participant application using the following signature release methods: • Password / one-time code via SMS (PWD/OTP) A pop-up window is displayed for each signature process, in which a password and, in the next step, a one-time code are entered. The password was initially set once during registration and must not be forgotten. If the password is forgotten, a new registration is required. The one-time code is transmitted via SMS with each signature process. • Mobile ID (Switzerland)

Provisioned service part	Definition
	All SIM providers / mobile phone providers in Switzerland support the mobile phone service "Mobile ID", which works independently of the smartphone operating systems directly via an app on all SIM cards provided by Swiss providers. This service can be activated once via **https://mobileid.ch**. It may be necessary to check whether Mobile ID is included in the tariff. It is then activated by pushing the Mobile ID functionality in the smartphone and entering a PIN that was defined during initialisation. A restoration code is also created during initialisation, which can be used to move the SIM card to a new mobile phone. • Mobile ID app The Mobile ID functionality is offered outside Switzerland, particularly in the EU/EEA, via a corresponding app that can be downloaded from the Google Play or Apple Appstore and must be initialised once. Authorisation can even be carried out using fingerprint or facial recognition if the smartphone supports this. • One-time code (OTP) Qualified electronic signatures always require two independent factors from the areas of knowledge, biometrics and possession for approval (e.g. possession of the mobile number plus fingerprint approval in the app or possession of the mobile number and knowledge of the PIN). In the case of advanced electronic signatures, one factor is sufficient; a one-time code is used here, which is sent by SMS to the registered mobile number. As all mobile phone users in Switzerland are required to register using an ID card, advanced electronic signatures with Swiss mobile numbers do not require prior registration and can be confirmed immediately.
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/**
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.

Provisioned service part	Definition
	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

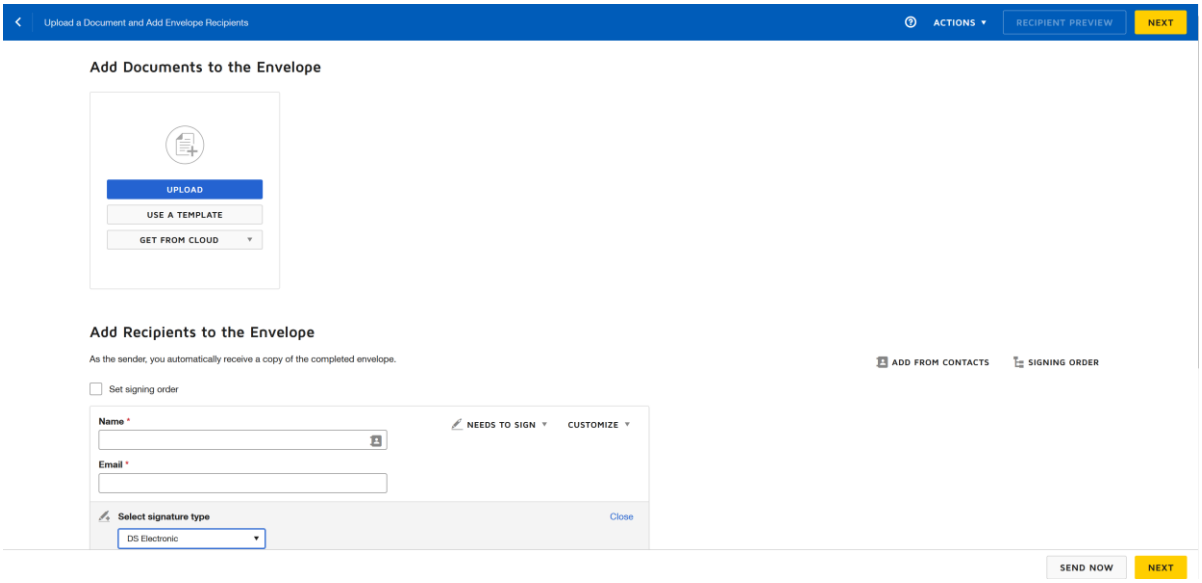
Personal signatures contain the following information in the certificate (Distinguished Name):
Common name= <First name, last name of the signatory>
givenname= <First name(s) according to ID document>
surname= <Last name(s) according to ID document >
country= <Country of residence or home country of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

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">

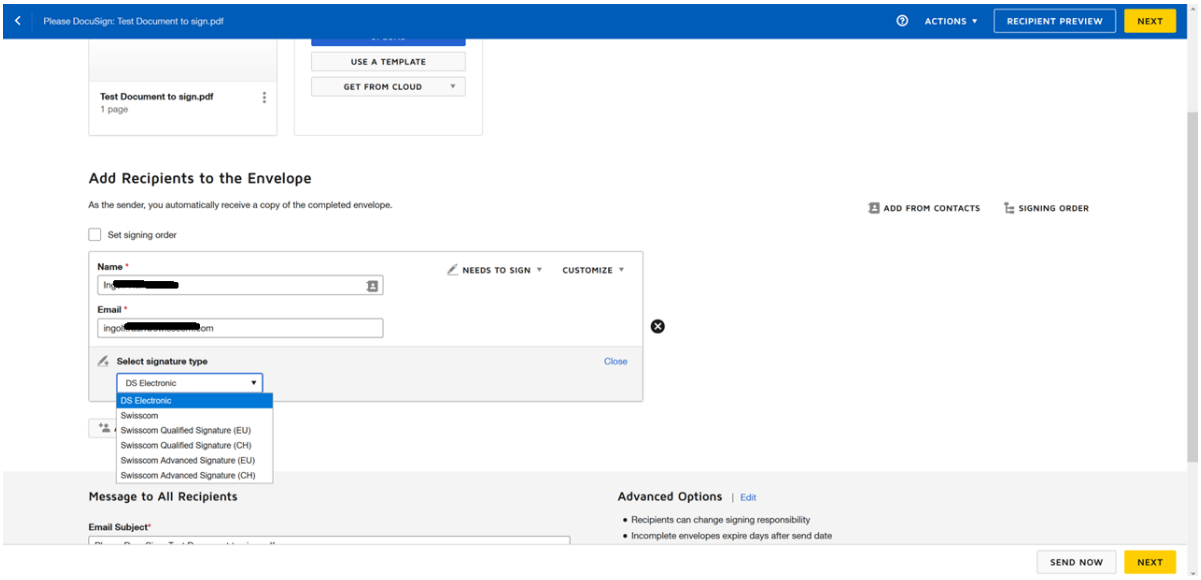
4.3 Signature creation procedure within Docusign

The following figures show the typical application flow within Docusign to create a signature. The flow is not provided by Swisscom Trust Services and hence it could lead to deviations and changes. By this the figures and the flow show the principle how a signature is created on behalf of the Docusign application without any claim to topicality and correctness.

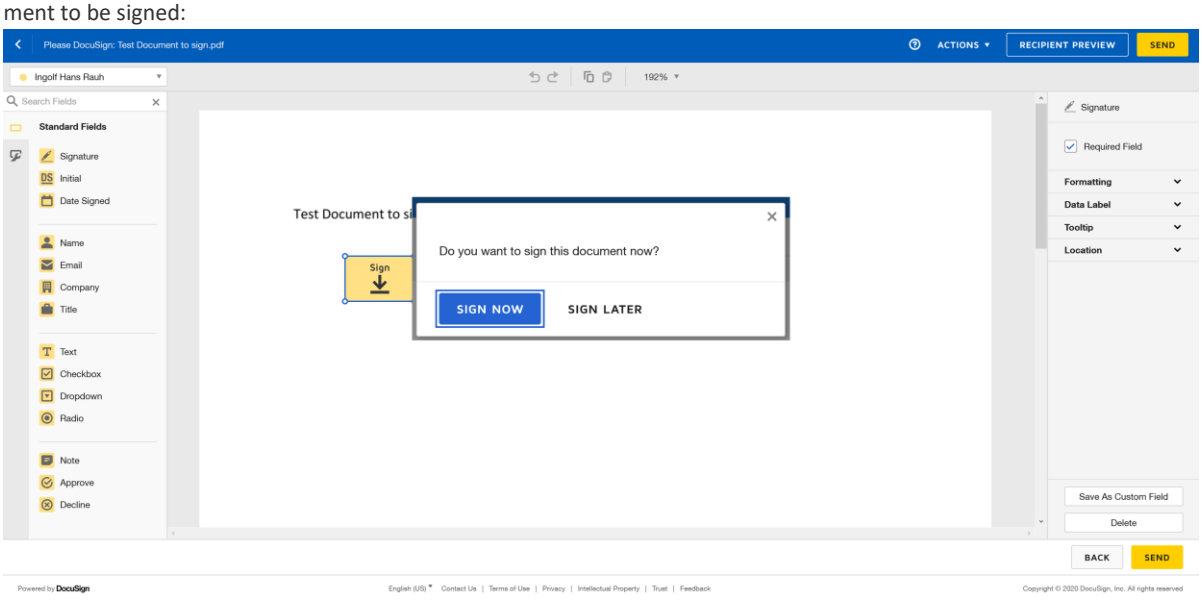
In the Docusign application you have first to upload a PDF document:



The signatories for this document are now defined in Docusign. For the signature, care must be taken to select the appropriate signature type from Swisscom Trust Services. This describes the legal area of application (EU/eIDAS or Switzerland/ZertES) and the quality of the signature (advanced or qualified electronic):



Finally, the creator of the signature circulation can set their own signature, if desired, otherwise other workflow users will receive an e-mail with a request for an electronic signature in a similar way after they have signed the link to the document to be signed:

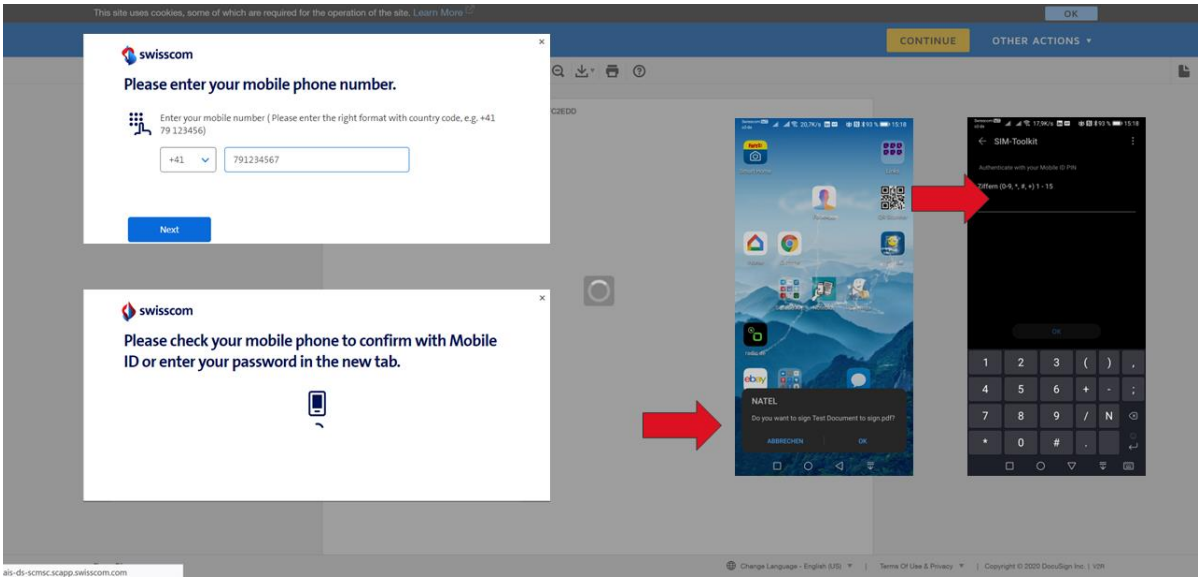


It is now pointed out that Swisscom Trust Services intervenes in the signature process and requests authorisation for access.

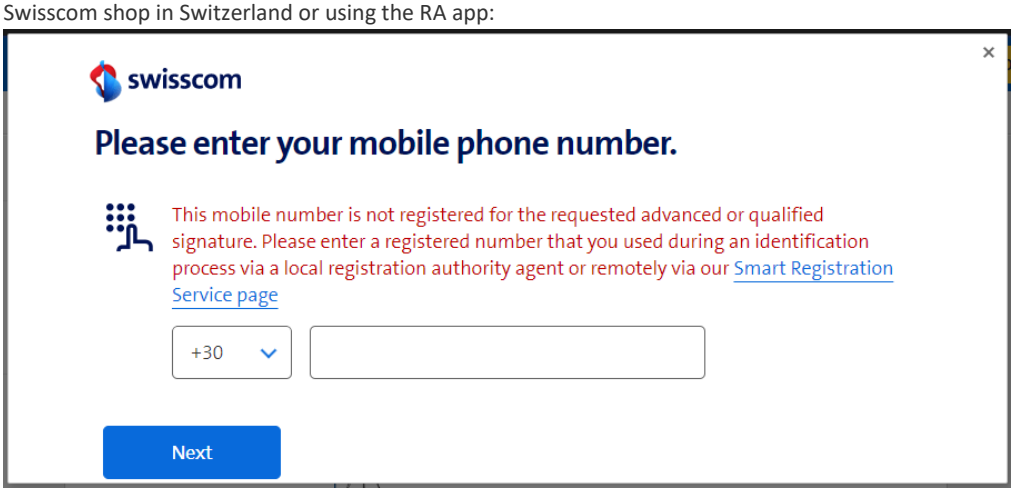
A registered user is now prompted to enter their mobile phone number and is redirected to the signature approval procedure that they specified during registration:

- Entering a password and entering a one-time code received via SMS
- Enter a Mobile ID PIN (Switzerland)
- Enter fingerprint or facial recognition in the Mobile ID app

The following figure is an example of the procedure with a Mobile ID PIN in Switzerland:



If a user is not registered, this is automatically recognised, and a link is provided to the registration portal for remote identification https://srsident.trustservices.swisscom.com. Alternatively, face2face identification can also be carried out in the Swisscom shop in Switzerland or using the RA app:



Once the signature has been approved by the registered procedure, the document is signed and can be downloaded within the Docusign application. A green tick is displayed in the Adobe PDF Reader. The document also receives the appropriate qualified electronic time stamp.

4.4 Process for vetting 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 must sign a declaration of acceptance, in which obligations such as the prevention of the exchange of a document hash, the protection of the application.

4.5 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 connector to Docusign based on the Docusign API for Trust Service Provider.	✓	
4. Provision of the subscriber application Docusign, configuration of the application based on the configuration hints on the order form.		✓
5. Sending the signed declaration of acceptance with the information required for regulatory purposes.		✓
6. Connection of the Subscriber and sending of the Subscriber-specific access data.	✓	
7. Immediate reporting of any errors before the signatures are used.		✓
8. Troubleshooting by update or new installation.	✓	
9. 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.	✓	

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. Creation of signature certificates and time stamps according to the X.509 standard.	✓	
7. Definition of the signature certificate contents and procedures for signature.	✓	
8. 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.).	✓	
9. 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 a forwarding hint will be displayed to the identification service.	✓	
10. Execution of signatures if approved by the signatory.	✓	
11. Signature in conjunction with a RFC3161, qualified time stamp according to ZertES and eIDAS. The subscriber application will be enabled to create PAdES signatures to be validated for a long term (LTV).	✓	
12. 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).		✓

Activities (**S = STS/T = Subscriber**)	S	T
13. Provision of support services (service desk, incident management, etc.)	✓	
14. 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.	✓	
15. 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.		✓
16. Reporting changes to Subscriber-specific information (contact persons, etc.)		✓
17. Updating of Subscriber-specific information (contact persons, etc.)	✓	
18. Reporting security incidents on the Subscriber application system that affect the Signing Service or Registration Service.		✓
19. Reporting of security incidents on the system of the signature or Registration Service that have an impact on the Subscriber.	✓	
20. Decision and responsibility for legal effects of the selected signature type or signature level (cf. chapter 8.2)		✓
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 interface configuration 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		✓

Activities (**S = STS/T = Subscriber**)	S	T
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			

[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)".

Service Level & Target Values		Smart Registration & Signing Service
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.

[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 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 (Docusign) 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 Docusign 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 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.