



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

Service Description Personal Signatures Switzerland (ZertES)

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

Switzerland

<https://trustservices.swisscom.com>

E-Mail: sts.salessupport@swisscom.com



1	Content	
1	Content	1
2	Service overview	3
3	Definitions	3
3.1	The Service Access Interface Point (SAIP)	3
3.2	Service-specific definitions	4
4	Variants and options	7
4.1	Definition of the services	7
4.1.1	Signature creation procedure for all options	9
4.2	Processes and tools for personal identification (registration authority)	10
4.2.1	Organisation check process	10
4.3	Data storage and responsibilities	10
4.4	Declaration of consent	10
4.5	Option DocuSign Connector	11
5	Performance description and responsibilities	11
5.1	Signature service	11
5.2	Invoicing model «Renumeration per active signatory»	13
5.3	Option DocuSign Connector	14
5.4	Option Own Identification and/or Authentication Methods	14
5.5	Option Use by signatories domiciled outside of Switzerland, EU and EEA	15
6	Service levels and reporting	16
6.1	Service levels	16
6.2	Service level reporting	17
7	Billing and quantity report	17
7.1	Billing	17
7.1.1	Renumeration per signature – postpaid model	17
7.1.2	Renumeration per active signatory – postpaid model	17
7.1.3	Renumeration according to volume-based usage prices – prepaid model	17
7.2	Quantity report	17
8	Special provisions	17
8.1	Subscriber application	17
8.2	Signature types and their applications	18
8.3	Data processing by third parties in Switzerland or abroad, emergency access	18

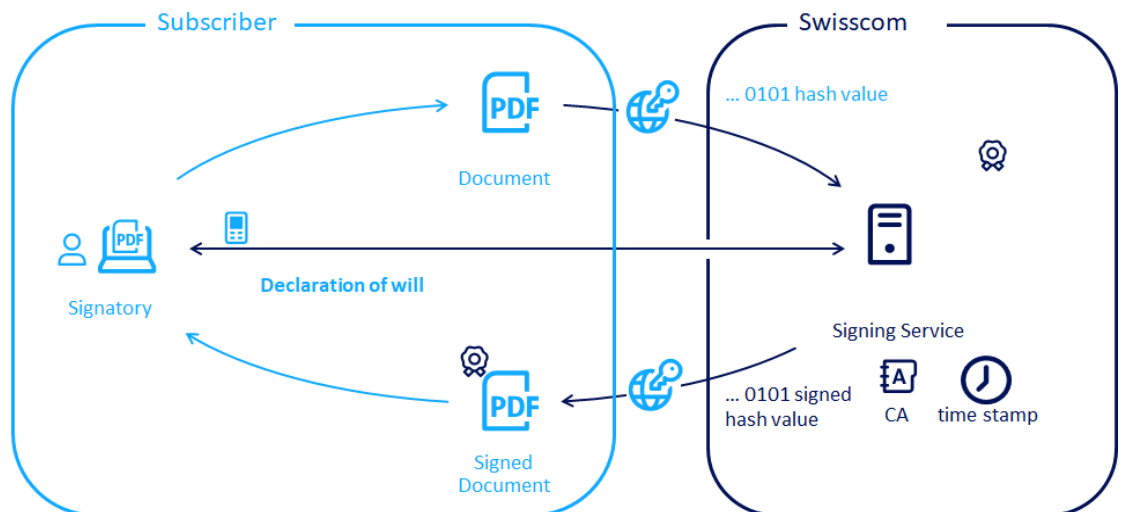


2 Service overview

The Signing Service in accordance with this service description is a server-based remote signature service provided at the data centres of Swisscom (Switzerland) Ltd in Switzerland and distributed by Swisscom Trust Services Ltd (hereafter "Swisscom"). Swisscom Trust Services Ltd. distributes the Signing Service in its own name or grants third parties the right to distribute the Signing Service in its own name.

The remote signature service is made available to Subscribers operating a Subscriber application. It enables signatories to electronically sign digital files and thus ensure the integrity and authenticity of a file. Swisscom (Switzerland) Ltd creates and manages the signature certificate for the signatories as a fiduciary and makes it available to the remote signature service via an encrypted channel. Apart from a Subscriber application operated by the Subscriber for the sending of the document to be signed and receipt of the signed document, the signatory does not require any other operating equipment, such as tokens or signature cards.

The Subscriber application prepares a document so that for signing only the hash value (check sum of fixed length without any indication of the content) must be sent to Signing Service. The effectively readable files and the information they contain do not leave the Subscriber's system environment and cannot therefore be viewed by Swisscom. The signed hash is reintegrated into the document by the Subscriber application and thus creates a signed document. Before activating the signature, the Subscriber must be authenticated by the Subscriber application and declare their consent to sign. The Signing Service uses a previous registered authentication means like Mobile ID or a signature approval means of an IDP.



The identification of the signatory can be done beforehand by ZertES approved procedures ("RA-App", "Video Identification") or by various audited procedures (own registration authority).

With regard to the signatures, a general distinction is made between advanced and qualified electronic signatures. Qualified electronic signatures have the highest degree of legal validity and have the same status as a handwritten signature in many cases. This means that generally business requirements where a handwritten signature is necessary by law can also be met (see section 8.2).

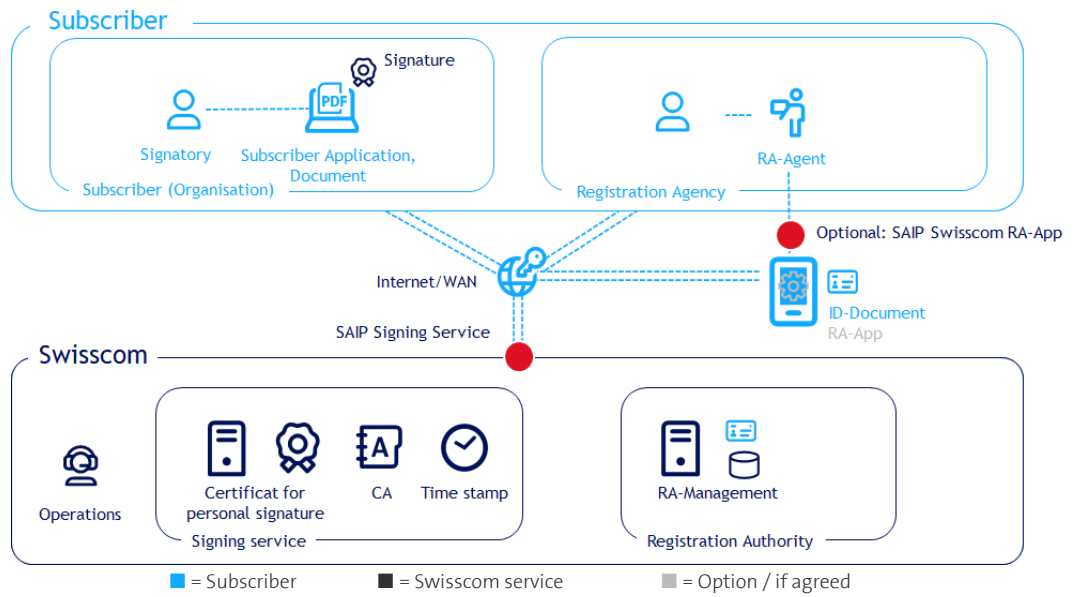
Swisscom (Switzerland) Ltd is a recognised provider of signature and certification services in Switzerland in accordance with ZertES. An accredited certification authority regularly checks whether the requirements made of providers of certification services by Swiss law and/or recognised technical norms are also met. Signing Service generally provides advanced electronic signatures for natural and legal persons and qualified electronic signatures for natural persons depending on the contract structure and selection of the Subscriber. This service description describes the service for electronic signatures for natural persons in Switzerland.

3 Definitions

3.1 The Service Access Interface Point (SAIP)

The Service Access Interface Point (SAIP) is the contractually agreed, geographical and/or logical point at which a service is delivered to the service user, the Subscriber. It is also the point at which a service is monitored, and the service level provided is documented.

The following schematic diagram illustrates the services and service components of the Signing Service:



The service provision point for the signatures is Swisscom's connection to the Internet. The availability of this service is assured if enquiries are accepted by the Service and answered correctly to the SAIP in line with the interface description. The correct reply can also consist of an error message that is documented or meaningful for the Subscriber.

The interface description can be found at: <https://trustservices.swisscom.com/downloads> under the link of the "Reference Guide":

http://documents.swisscom.com/product/1000255-Digital_Signing_Service/Documents/Reference_Guide/Reference_Guide-All-in-Signing-Service-en.pdf

SMS or MobileID information is provided at the interface to the roaming partner unless it is provided within the Swisscom network. A service promise for the proper performance of the Internet or the network operation of the roaming partner is excluded.

3.2 Service-specific definitions

Term	Description
CMS	Cryptographic Message Syntax – a syntax defined in RFC5652 for the digital signature and cryptographic messages
CP/CPS	Certificate guidelines (CP/CPS) for issuing certificates of the "Diamond" (qualified) and "Sapphire" (advanced) classes. Certification guidelines, certification practice, documents of a certification authority which describe the guidelines and practice for issuing certificates.
Distinguished name	Standardised form to describe a certificate subject. The subject of a certificate clearly designates the identification of the signatory.
Document	For the sake of clarity, the term document is used synonymously with the term data. Both documents and data can be signed.
Electronic signature	The electronic signature is a technical procedure for checking the integrity of a document, an electronic message or other electronic data and the identity of the signatory.
Hash	Clear depiction of a large amount of data on a small amount of data, almost like a document's fingerprint. The document contents cannot be traced from the hash.
IdP	Identity Provider: In this context, a registration authority approved for Swisscom's Signing Service which, after audit and approval, registers for Swisscom Signing Service either with its own authentication means for the expression of will or with a standard authentication means of Swisscom Trust Services.
Mobile ID	Managed service for secure user authentication. Mobile ID can be purchased from various providers including Swisscom (Switzerland) Ltd.



Term	Description
Mobile ID App	Managed Service App (Application) downloadable from the Google Play Store or Apple store for secure user authentication based on offered authentication means of the mobile device like fingerprint, face recognition, etc. Initialization is done by use of the mobile number. The Mobile ID App can be used with any international mobile number and by use of an Internet connection.
OASIS DSS	Interface standard for digital signatures for web services and other services of the OASIS Group (non-profit organisation for open standards in IT)
On-demand signature	Term frequently used in technical documents for the “personal signature” in accordance with this service description.
OTP	One Time Password – One time code created for use on one occasion which is sent via SMS.
PKCS#1	Cryptographic standard of the RSA Laboratories.
PWD	Password (entry) for the authentication of the password to be used for the service
RA agent	Authorised operator of the RA app
RA agency	Organization providing the RA agents
RA app	App (application) which can be downloaded from the Android or iOS store. This enables a trained RA agent to carry out identification for advanced and qualified signatures and sends the data to the RA service.
RA service	Service for receiving and archiving the identification data, operation in relation to the RA app.
Registration authority (RA)	Authority responsible for the identification of the signatories. May be provided by the Subscriber, Swisscom or third parties provided a contractual relationship with Swisscom (Switzerland) Ltd. exists.
REST	Representational State Transfer, programming paradigm for distributed systems, particularly web services.
Secure signature creation unit (HSM)	Qualified and certified hardware for creating signature keys and signature certificates.
Signing	Natural person who signs a document electronically after prior identification, authentication and declaration of consent.
Smart Registration Service	Additional service of Swisscom with online identification methods which import the evidence data also into the RA-Service in the same way as the RA-App
SOAP	Simple Object Access Protocol – alternative interfaces, programming paradigm concerning REST for web services
SSL/TLS	Secure socket layer, transport layer security, encryption protocol for secure data transmission on the internet based on SSL (access) certificates
Subscriber	Swisscom provides the services in accordance with this service description for the benefit of the Subscriber. The Subscriber is either a direct client of Swisscom with a Signing Service contract (including the existing declaration of acceptance towards Swisscom (Switzerland) Ltd.) or has a commercial contract with a reseller of Swisscom services with a declaration of acceptance vis-à-vis Swisscom (Switzerland) Ltd.
Subscriber application	The Subscriber provides the signatories with access to an application with which it can create electronic signatures in accordance with the terms and conditions of use and the Subscriber ensures the transmission of signature data to the remote signature service of Swisscom as well as the authentication (“Subscriber application”). The Subscriber application receives the signed data and prepares the document for the signatories. The signature service provides an interface linked to a Subscriber application to activate the signature. The Subscriber application is not part of this service description. It is provided outside of the Signing Service, for example by partners.



Term	Description
Terms and conditions of use (Subscriber Agreement)	The terms and conditions of use govern the terms for using the signature certificates and signature service in the relationship between Swisscom (Switzerland) Ltd and the signatory on a Subscriber application. They can be viewed at https://trustservices.swisscom.com/repository/
ZertES	Swiss federal law on certification services in the field of electronic signatures and other digital certificate applications.



4 Variants and options

Standard variant	Electronic personal signatures
Qualified electronic signature	●
Advanced electronic signature	●
Qualified electronic time stamp	●
Identification based on Swisscom registration Authority / RA-App identification	●
Identification based on Subscriber's own registration methods	○
Usage of Mobile ID or Mobile ID App for declaration of will	●
Usage of combination of password and one time code (SMS)for declaration of will	○
Other procedures for declaration of consent that differ from the standard (Mobile ID, Mobile ID App, PWD/OTP)	○
Data storage in Switzerland	●
Operation in accordance with certification guidelines (CP/CPS)	●
Use by signatories domiciled in Switzerland, EU and EEA	●
Use by signatories domiciled outside of Switzerland, EU and EEA	○
Connection to DocuSign Signature Application	○

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

4.1 Definition of the services

Service	Definition
Qualified electronic signature	Qualified electronic signature in accordance with Art. 2 (e) ZertES.
Advanced electronic signature	Advanced electronic signature in accordance with CP/CPS.
Qualified electronic time stamp	Qualified electronic time stamp in accordance with Art. 2 (j) ZertES.
Identification based on Swisscom registration Authority / RA-App identification	The Subscriber and signatory can use standard identification methods offered by Swisscom and described in the service description of the RA-App and the Smart Registration Service. These services must be ordered separately.
Identification based on Subscriber's own registration methods	<p>Optionally, identification methods of the Subscriber or third parties can also be used if they have been audited and approved for ZertES. For this purpose, additional options for the approval of these procedures (onboarding support, audit by the conformity assessment body) shall be ordered, as well as an option for ensuring conformity during service life. The options are all additionally described in the service contract or the order. Likewise, a so-called "Contract for Delegation of the Registration Authority Activity" (RA delegation contract) must be concluded with the Subscriber concerned or a third party as "RA authority" and Swisscom (Switzerland) Ltd.</p> <p>During the productive use of these methods, Swisscom Trust Services ensures that these methods are considered as part of the annual repetitive and surveillance audit and that enquiries from the conformity assessment body or supervisory body are answered in this regard. This also includes obtaining offers of separate audits by the conformity assessment body. These offers are submitted to the customer or partner for acceptance and execution. If approval is given, the conformity assessment body shall carry out these audits and Swisscom Trust Services shall then charge the customer or partner the invoice amount claimed by the conformity assessment body in addition to Swisscom Trust Service's costs. If the customer or partner does not wish to carry out the audit and thus refuses further</p>

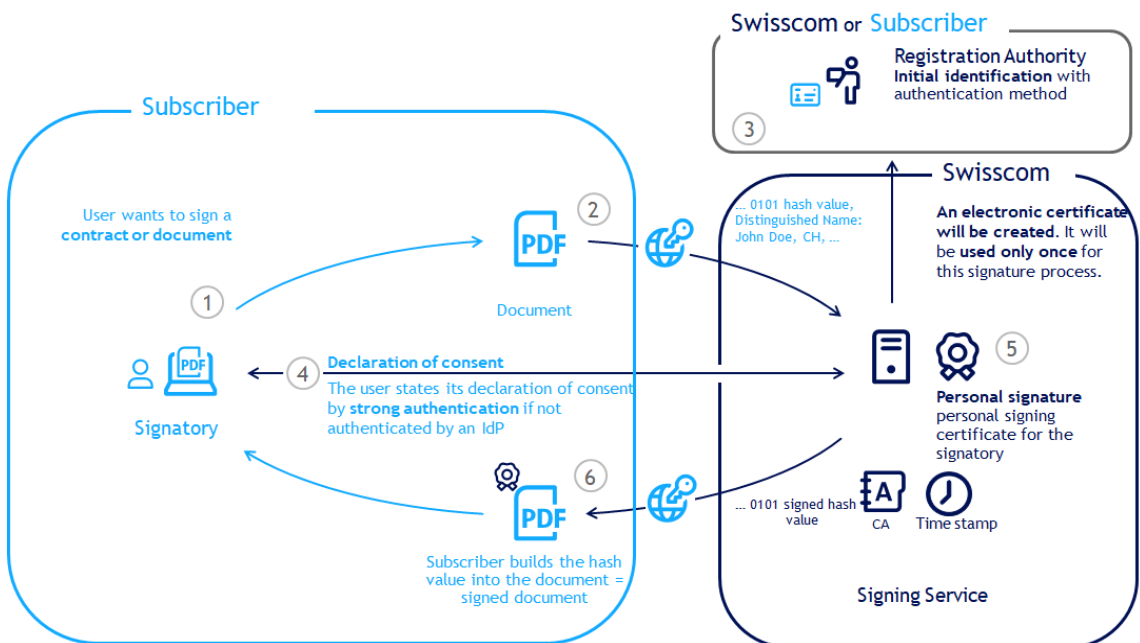


Service	Definition
	recognition, this will lead to the deactivation of the relevant identification method in the signature service for the Subscriber and to the automatic termination of the signature contract by Swisscom Trust Services.
Usage of Mobile ID or Mobile ID App for declaration of will	The service offers the use of Mobile ID which is provided by Swisscom for all mobile phone Subscribers in Switzerland or the Mobile ID App which can be downloaded in the EU/EEA, Switzerland and some other countries. For further information: https://mobileid.ch
Usage of combination of password and one time code (SMS) for declaration of will	As far as Mobile ID or Mobile ID App cannot be used for signatures which are not invoiced in the scope of a monthly flat model per user also a combination of password and one-time code can be used. They have to be entered for each signature. The password will be set after registration during the confirmation of the Terms of Use for the first time. The one-time code will be sent over via SMS to the mobile number which was registered during registration process. In case of an advanced electronic signature only one factor (one time code) is sufficient.
Other procedures for declaration of will that differ from the standard	<p>Optionally, authentication methods of the Subscriber or third parties for the signer's declaration of will can be used if they have been audited and approved for ZertES. Swisscom Trust Services will provide more own procedures on an ongoing basis in accordance with the order form or service contract. These may also be authentication procedures of other customers/IdPs that have already been released. The use of authentication procedures of other IdPs may be subject to separate fees that these IdPs charge their users.</p> <p>Independently of this, customer-specific authentication procedures can also be checked and approved, e.g. customer's own apps. For this purpose, additional options for the approval of these procedures (onboarding support, audit by the conformity assessment body) must be ordered, as well as an option for ensuring conformity during service life. The options are all additionally described in the service contract or the order. Likewise, a so-called "Contract for Delegation of the Registration Authority Activity" (RA delegation contract) must be concluded with the Subscriber concerned or a third party as "RA authority".</p> <p>During the productive use of these methods, Swisscom Trust Services ensures that these methods are considered as part of the annual repetitive and surveillance audit and that enquiries from the conformity assessment body or supervisory body are answered in this regard. This also includes obtaining offers of separate audits by the conformity assessment body. These offers are submitted to the customer or partner for acceptance and execution. If approval is given, the conformity assessment body shall carry out these audits and Swisscom Trust Services shall then charge the customer or partner the invoice amount claimed by the conformity assessment body in addition to Swisscom Trust Service's costs. If the customer or partner does not wish to carry out the audit and thus refuses further recognition, this will lead to the deactivation of the relevant identification method in the signature service for the Subscriber and to the automatic termination of the signature contract by Swisscom Trust Services.</p>
Data storage in Switzerland	The data storage with the personal data from the certificates takes place only in Switzerland in accordance with the relevant regulations of the Swiss data protection legislation.
Operation in accordance with certification guidelines (CP/CPS)	The operation of a certification service provider is based on the certificate guidelines (CP/CPS) for issuing certificates of the "Diamond" (qualified) and "Sapphire" (advanced) classes. The latest version can be viewed here: https://trustservices.swisscom.com/repository/
Use by signatories domiciled in Switzerland, EU and EEA	The terms of use comply with the legal requirements only for signatories domiciled in Switzerland, the EU and the EEA.
Use by signatories domiciled outside of Switzerland, EU and EEA	Due to country-specific legal requirements where applicable, the current terms of use for signatories domiciled outside Switzerland, the EU and the EEA cannot be used. There is a risk that the issued signature will be invalid. If the service shall also be made available outside Switzerland, the EU and the EEA, this will have to be



Service	Definition
	verified legally and technically (e.g., with regard to the use of authentication means and encryption requirements). If necessary, the terms of use must be amended to local consumer law, and the technical authentication possibilities checked and made available. This is possible by agreement and against a separate offer by Swisscom Trust Services AG.
Connection to DocuSign signature application	In case of this option the Subscriber uses DocuSign as signature application which foresees an interface for use of a remote signature services. As an option Swisscom offers a DocuSign connector which bridges the DocuSign API to the Swisscom Signing Service API and enables the use of advanced and qualified signatures within DocuSign.

4.1.1 Signature creation procedure for all options



- The Subscriber application is linked to the Swisscom Signing Service platform using a SSL/TLS access certificate.
- The signatory, who has already been identified for the service directly or via Identity Provider (IdP), logs into their Subscriber application (1) and selects the document to be signed. The Subscriber application creates a hash in accordance with Swisscom provisions (2) and sends it to the Signing Service platform. Information relevant to the signature certificate subject (distinguished name) is also sent by the Subscriber application.
- If the registration authority of Swisscom (Switzerland) Ltd. or partners is used with the RA app, video identification service or Smart Registration Service, the signature data sent by the Signatory is compared with the identification data of the Swisscom (Switzerland) Ltd. registration authority. (3)
- If the Subscriber is recorded by the registration authority and authorised for the signature, the Signing Service requests the declaration of consent from the signatory. (4)
- The signatory's declaration of consent is sent via the authentication means used during registration. Qualified certificates and signatures are only created on the basis of 2-factor authentication, advanced signatures can be confirmed by a 1-factor authentication.
- Generation and use of key material (private and public keys) as well as certificates that are required for the advanced or qualified electronic signature (incl. the qualified time stamp in accordance with ZertES). (5) The key material is generated and used on the Signing Service platform at Swisscom. An advanced or qualified certificate is issued for this key pair in accordance with the certification guidelines of Swisscom (Switzerland) Ltd. and the subject of the certificate sent by the Subscriber application (distinguished name). The certificate



and the key pair are used for a single signature request by the Subscriber and the key pair is deleted after use. Personal certificates are generally valid for a few minutes.

- Signing of the hash value (cryptographic check sum of a data set/text of any length) to safeguard its integrity according to the CMS or PKCS#1 standard.
- Return of the signature as well as any additional validation information in the certificate (e.g. certificate chain for the trustworthy root certificate and qualified time stamp). The Subscriber application ensures the signature of the document based on the signed hash. (6)

4.2 Processes and tools for personal identification (registration authority)

Before authentication is possible, the signer must identify himself according to the requirements of the respective type of electronic signature. The identification process can take place separately from the signature process by a so-called registration authority, Swisscom offers several variants for this purpose:

- The Subscriber can be enabled to identify colleagues, customers and partners locally for Swisscom in a face2face process. He can use the RA app for this purpose. This is to be ordered separately and described in a separate service description.
- The Subscriber may use identification methods offered by Swisscom or its partners as a remote identification methods within the framework of Smart Registration Service. These are described in a separate service description and must be ordered separately.
- IdPs can also offer their users either directly or via the Smart Registration Service registrations means of authentication that can be used in other signature applications for expressing the will to sign. In this case, the offer is made either by the IdP or within the framework of the Smart Registration Service.
- Swisscom also offers the registration options of the Smart Registration Service directly for purchase via voucher codes or direct payment via the website <https://rsident.trustservices.swisscom.com>.
- The Subscriber can use the registration possibilities in the Swisscom Shop.
- The Subscriber can use his own identification methods and set up a registry with project-specific identification ("IdP"). This procedure must be coordinated with Swisscom in advance and developed as part of a signing onboarding project. For this purpose, the Subscriber must present an implementation concept, which is reviewed and evaluated by Swisscom. Generally, individualised registry processes must also be released for Subscribers by the certification body or conformity assessment body for certification services. The registration data can remain with the Subscriber depending on the implementation or can also be transferred to the Smart Registration Service at Swisscom. A separate order is necessary for this purpose.

All identification procedures and registrations are not part of this service description.

4.2.1 Organisation check process

If the organisation associated with the person is also determined in the aforementioned procedure on personal identification, an organisation check is also carried out in accordance with the provisions of CP/CPS before commencement of the service by Swisscom. This must also be indicated in the declaration of acceptance and an authorised representative of the organisation must have signed the declaration of acceptance. By signing he/she also grants consent for the use of the organisation name in relation to the signatories.

4.3 Data storage and responsibilities

With the use of the RA app, remote identification and Smart Registration Service provided by Swisscom or its partners, the data on the identified person and the identification documents and evidence of acceptance of the terms and conditions of use are only stored on Swisscom servers in Switzerland and are retained for the periods in accordance with CP/CPS or under law. This is not valid for data of an IdP since here the rules of the IdP apply. On the other hand, the data can also be taken outside, depending on the situation (e.g. when using the RA app abroad). For project-specific procedures, the storage and place of storage are set out in the separate agreement on the delegation of personal identification with implementation concept.

4.4 Declaration of consent

Every personal signature requires the submission of a declaration of consent by the signatory. Typically a device like a mobile phone with the mobile phone number registered during the identification of the signatory or smartphone is used for the declaration of consent.

Various procedures are currently available for the submission of the declaration of consent itself:



- Mobile ID: Currently only usable with MobileID-enabled SIM cards with Swiss mobile phone numbers. This allows signatories to authenticate themselves using direct 2-factor authentication and send a declaration of consent to the signature. If Mobile ID is not available for the mobile phone number, the PWD/OTP or Mobile ID App procedure is automatically used. The Mobile ID must be initialized beforehand on mobileid.ch.
- Mobile ID App: This Authenticator app can be used as long as the standard Mobile ID procedure is not in use. It is also suitable for international mobile use outside Switzerland. The signer triggers a 2-factor authentication by means of a biometric feature enabled by the device or a one-time code/password. For this purpose, the app must be installed before the first use, e.g. before the confirmation of the terms of use, and initialized with the mobile number. A smartphone connected to the Internet is required.
- PWD/OTP: Here signatories authenticate themselves via a password entry page, which they receive via the signature application, in the Signing Service and activate the generation of a one-time code on the service which is sent via SMS to the mobile phone of the signatory. The signatory enters this in the Subscriber application.
- OTP: The authentication of the signatory in the Signing Service is omitted in this procedure and instead the signatory sends a one-time code directly to the Signing Service which is sent to them beforehand via SMS. This procedure can only be used for advanced signatures.
- Project-specific declaration of consent: If the aforementioned procedure is not used, any project-specific declaration of consent procedure will be agreed beforehand with Swisscom. The Subscriber must present an implementation concept prior to the conclusion of the contract which is checked and evaluated by Swisscom. Individualised declaration of consent processes must generally also be approved by the certification authority or conformity assessment authority for certification services for Subscribers.
- IdP procedures: these project specific authentication means have been authorized by Swisscom. The methods vary from IdP to IdP and the user must contact the respective IdP (e.g. bank) that offers this authentication means to its customers and users for the description of the procedures.

4.5 Option DocuSign Connector

If the DocuSign Connector is used, the Subscriber can also sign with DocuSign advanced or qualified. This option only works with procedures that rely on standard Swisscom will-declaration methods and use identifications carried out by Swisscom or in which the registration data is managed by the Smart Registration Service.

The DocuSign application must be extended to include a so-called “Swisscom Pen”, a selection field in the DocuSign user interface, which allows the user to enter the mobile number of the signer and select the signature quality (advanced/qualified).

The document signed by DocuSign contains after successful signature not only the seal of DocuSign but also the corresponding personal signature on behalf of a Swisscom certificate. For the signature a declaration of will (PWD/OTP or Mobile ID, Mobile ID App) must be submitted. This requires a one-time pre-registration.

5 Performance description and responsibilities

5.1 Signature service

Non-recurring services

Activities (S = STS / SB = Subscriber)	S	SB
Provision of the service		



Activities (S = STS / SB = Subscriber)	S	SB
1. Ensuring the registration of the signers (e.g. ordering a registration with Swisscom). Please note that registration methods cannot guarantee that all users are registered due to e.g., insufficient ID documents not allowed for automatic registration procedures, negative risk assessment outcomes, etc.		✓
2. Provision of the Signing Service infrastructure	✓	
3. Provision of the SAIP interface based on the OASIS DSS protocol via SOAP or REST or the ETSI 119 432 standard adopted for the use of short-term signature certificates. The interface can be found at http://documents.swisscom.com/product/1000255-Digital_Signing_Service/Documents/Reference_Guide/Reference_Guide-All-in-Signing-Service-en.pdf	✓	
4. Compliance with the regulations for the composition of the signature from the signed hash (e.g., compliance with the PAdES standard, observance of long-term validation rules) – see Reference Guide, topic 3.		
5. Sending of signed declaration of acceptance with regulation-relevant information.		✓
6. Organisation entry in the signature certificate option: Provision of all necessary documents for the organisation check at the request of Swisscom (e.g., attested commercial register extract). Signature in the declaration of acceptance by an authorised representative of the organisation for the consent that the organisation agrees with the entry of the organisation’s name in the certificate for the signatories.		✓
7. Organisation entry in the signature certificate option: Check of the authorisation to enter the organisation’s name in the certificate.	✓	
8. Sending of a publicly trustworthy (mandatory in the scope of the ETSI protocol) or self-signed SSL/TLS authentication certification for the authentication vis-à-vis the Signing Service server and for encrypted communication with the Signing Service. For specifications see declaration of acceptance.		✓
9. Activation of the communication for the authentication certificate sent.	✓	
10. If required, configuration of the firewall, on the server side at the Subscriber’s site.		✓
11. Designation of a person responsible including constant deputation for all matters concerning technology, security and the implementation of registration of signatories and contact partners for audit matters.		✓
12. Connection of the Subscriber and sending of Subscriber-specific access data.	✓	
13. Integration of the Signing Service into Subscriber-specific application(s) and/or Subscriber side connection of the interface to Signing Service, e.g., through the use of a partner application.		✓
14. Checking of the connection to the Signing Service server and the issuing of signatures. Immediate notification of any errors before the signatures are used.		✓
15. Fault rectification through update or re-installation.	✓	
16. Notification of the relinquishment of business activities and any bankruptcy notices against it, the opening of bankruptcy proceedings or a debt restructuring moratorium.		✓
Termination of the service		
1. Deletion of Subscriber authorisations in the Signing Service infrastructure.	✓	
2. Deletion of the key from the HSM.	✓	
Recurring services		
Activities (S = STS / SB = Subscriber)	S	SB
Standard services		
1. Operation of the Signing Service infrastructure.	✓	
2. Lifecycle management of the Signing Service infrastructure.	✓	



Activities (S = STS / SB = Subscriber)	S	SB
3. LifeCycle management of the Subscriber's infrastructure: Modification of the current status of technology and security (security patches, updates etc.).		✓
4. Appropriate technical and organisational measures to protect the data sent from the Subscriber application (e.g., including through the deactivation of connections not required or access regulations etc.). Disclosure of the security system of the Subscriber application and communication to Swisscom if requested by Swisscom or the supervisory body of Swisscom (Switzerland) Ltd.		✓
5. Modification of the definition of the security requirements.	✓	
6. Lifecycle management of its SSL/TLS authentication certificate, timely exchange upon expiry of validity by the designated security manager by e-mail to sts.salessupport@swisscom.com with designation of the account name. Avoidance of any disruption of the SSL/TLS connection (e.g., through "inspection" module).		✓
7. Creation of signature certificates based on the X.509 standard.	✓	
8. Definition of the signature certificate content and procedure for signature creation.	✓	
9. Ensuring the use of technical means of authentication and contractually agreed authentication methods (e.g., Mobile ID, PWD/OTP, etc.).		✓
10. Ensure in advance that only those signatories take part in the signature (e.g., by checking by use of a verification call offered by the API) who are registered and authorised with the corresponding means of authentication for the requested signature type. Otherwise an error message is shown or optional the forwarding to the standard offering of registration.		✓
11. Sending of the signatory's data (distinguished name) in accordance with the provisions of the declaration of acceptance.		✓
12. Implementation of signatures for which the signatory's declaration of consent exists.	✓	
13. Signature is provided in conjunction with a qualified time stamp in accordance with ZertES.	✓	
14. Meeting the cooperation obligations and requirements by the security officer.		✓
15. Provision of support services (service desk, incident management, etc.)	✓	
16. Counting of all signature requests according to the billing model and billing the sum to the subscriber	✓	
17. Implementation 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.		✓
18. Reporting of changes to Subscriber-specific information (contact persons, SSL/TLS certificate, etc.)		✓
19. Updating of Subscriber-specific information (contact persons, SSL/TLS certificate, etc.)	✓	
20. Reporting of security incidents on the system of the Subscriber application which concerns the Signing Service service.		✓
21. Reporting of security incidents on the system of the signature service which has an impact on Subscribers.	✓	
22. Decision-making and responsibility for the legal implications of the signature type selected (see section 8.1)		✓
23. Notice to signatories in the user interface of the Subscriber application or in the question regarding expressions of intent about the type of signature used.		✓
24. Notice to signatories in the user interface of the Subscriber application or in the question regarding expressions of intent about the type of signature used.		✓
25. Modification of the interface in line with Swisscom's new requirements within 3 months.		✓

5.2 Invoicing model «Remuneration per active signatory»

If the Subscriber wishes to be billed according to the remuneration model "remuneration per active signatory" (see 7.1.2), additional obligations must be followed, as this procedure only permits certain authentication procedures named in the service contract.



Activities (S = STS / SB = Subscriber)	S	SB
Recurring services during the use of the invoicing model «Remuneration per active signatory»		
1. Before participating in a signature, the Subscriber must ensure that the signer has the authentication method(s) prescribed in this invoicing model according to the service contract. This can be done, for example, with appropriate API calls (e.g. "VerifyCall") that indicate with which authentication methods the signer has been registered.		✓
2. If the signatory does not have the allowed authentication method, the Subscriber must give the signatory meaningful feedback on the rejection of the signature procedure and, for example, show him how a new registration with other authentication procedures can be carried out. Alternatively, he can also give him the possibility to enable a signature according to another billing model via another access (ClaimedID) to the signing service.		✓
3. The Subscriber must ensure to the best of his ability that Swisscom support can be avoided as a result of the choice of remuneration model and the incorrect use of non-approved authentication methods. In the event of increased support costs as a result of this, Swisscom reserves the right to charge the support costs after two reminders or to change the remuneration model to another remuneration model after consultation with the Subscriber.		✓

5.3 Option DocuSign Connector

Activities (S = STS / SB = Subscriber)	S	SB
Non-recurring services in case of optional use of the DocuSign Connector		
1. Ensuring the registration of the signer (e.g. visit of a Swisscom Shop or additional contracts for registration e.g. by RA-App).		✓
2. Ensuring the provision and parameterisation of DocuSign: <ul style="list-style-type: none"> Announcement of the correct DocuSign Account ID to Swisscom in the order form. After placing the order to Swisscom, the Subscriber orders the "DocuSign Express SKU" from DocuSign The Subscriber triggers a ticket from DocuSign (https://support.docusign.com/en/articles/How-Do-I-Open-a-Case-in-the-DocuSign-Support-Center) and orders the parameterisation of the "Swisscom Pen" (visual selection field of the Swisscom signature in the DocuSign interface). The Pen ID number for this will be: Swisscom advanced electronic signature in Switzerland: 954 Swisscom qualified electronic signature in Switzerland: 952 		✓
3. Information to Swisscom, announcing that the DocuSign installation with "DocuSign Express SKU" and "Swisscom PEN" is provided by DocuSign ready for the integration of the Swisscom DocuSign connector		✓
4. Setup of the DocuSign connector to the Signing Service of Swisscom for the announced account ID.	✓	

5.4 Option Own Identification and/or Authentication Methods

Activities (S = STS / SB = Subscriber)	S	SB
Non-recurring services in case of optional use of own identification and/or authentication methods		
1. Ensuring initial auditing: Order the necessary additional onboarding support (onboarding support) for the review and acceptance of an implementation concept as well as the necessary auditing of the delegated RA site by a conformity assessment body or auditor. (See service description "Onboarding Support").		✓
2. Submission of the RA Delegation Contract based on the implementation concept	✓	
3. Creation of an implementation concept by the delegated RA site. Conclude a RA delegation agreement of the Delegated RA site with Swisscom (Switzerland) AG.		✓
4. Submission of procedures to the auditors for the annual repetition or surveillance audits, who decide accordingly on additional audits efforts based on separate payment.	✓	



Activities (S = STS / SB = Subscriber)	S	SB
5. Regular participation of the delegated RA site in the annual repetition or surveillance audit, if required by the auditor, as well as separate commissioning of the repetition and surveillance audits according to offer, which Swisscom Trust Services AG obtains from the auditor in advance and which has to be confirmed by the customer or auditor.		✓

5.5 Option Use by signatories domiciled outside of Switzerland, EU and EEA

Activities (S = STS / SB = Subscriber)	S	SB
Optional services for signatories residing outside Switzerland, EU and EEA (hereinafter the country of the signatory is referred to as “RoW country of residence”, RoW = Rest of World)		
1. Fee-based examination of the possible provision of signatures for signatories of the intended RoW country of residence with regard to applicable consumer protection, data protection, cryptography and operational requirements as well as technical possibilities (e.g. SMS reception) with the involvement of experts. Depending on the examination result, an assignment is possible with the services described in the following points or an assignment is not possible, and the Subscriber is informed about this.	✓	
2. Waiver of the offer of signatures to signatories residing in the RoW country of residence, provided that the operational examination under point 1 has shown that it is not possible to offer signatures for signatories in this RoW country of residence.		✓
3. In the event of a positive examination: Compliance with legal obligations: <ul style="list-style-type: none"> Adaptation of the Terms of Use regarding consumer and data protection Compliance with the data protection obligations of the country of residence (e.g. maintenance of a special data processing directory, constitution of a data protection officer, etc.) Configuration with respect to permitted crypto algorithms Compliance with the requirements for the use of the authentication means in the country of residence (e.g. pre-registration of SMS sender numbers, Google Play or Apple Store conditions, etc.)	✓	
4. Accept that registrations of the signatory in his RoW country of residence without an adequacy decision of the Federal Council pursuant to the planned data protection law Art. 16 of Switzerland or the European Commission pursuant to Art. 45 para. 3 GDPR cannot take place due to the increased data protection requirements (e.g. no use of the RA app) but only remote registrations (e.g. video identification), if permitted.		✓
5. Acceptance that the certification service can limit its liability to CHF 5000 per signature in the certificate (QES/FES). The participant must inform the signatory of this.		✓
6. Acceptance of conditions for use in the country of residence: <ul style="list-style-type: none"> E.g. limitation of the authentication process to be used (e.g. use of the Mobile ID app only or use of a customer-specific process only) E.g. restrictions on the identification methods to be used		✓
7. Create an appropriate language version of the Terms of Use or other regulatory texts for the RoW country of residence, if necessary;	✓	
8. Technical and organisational adaptations and adjustments, e.g. <ul style="list-style-type: none"> 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, adjustments of SMS texts (e.g. unicode specifications) Enable the use of the Mobile ID App in the Google Play Store or Apple Store Information to the auditor or accreditation body Setting the limits for liability in the certificate and in the Terms of Use, binding the registered signers exclusively to the access of the Subscriber application of this contract	✓	
9. Acceptance that not all authentication methods are usable in the target country (e.g. acceptance of SMS is not supported)		✓



Activities (S = STS / SB = Subscriber)	S	SB
10. Ongoing 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 residing in that country. Inform the Subscriber about these changes. Creation of an offer for necessary changes for the continuation of the signature offer or information to the Subscriber about the necessary discontinuation of the signature offer in the RoW country of residence (if possible, 3 months before entry into force)	✓	
11. In case of necessary adjustments in accordance with Section 9, commissioning the necessary changes or discontinuation of the signature service for residents of this RoW country according to the deadline set.		✓

6 Service levels and reporting

6.1 Service levels

The following service levels generally relate to the agreed monitored operation times. Definitions of terms (Operation Time, Monitored Operation Time, Support Time, Availability, Security and Continuity) and the description of the measurement method and reporting are set out in the contractual element “Base Document”.

The following service levels are provided for the service variants (see section 3). If several possible service levels are available for each variant, the service level is selected in the service contract.

Service level & target values	Electronic personal signatures
Operation Time	
Monitored Operation Time	Mo–Su 00:00-24:00
Provider Maintenance Window	PMW-DC PMW Data Center Swisscom
	PMW-S With advance notice for security and system-critical updates
	Daily 19:00- 07:00, only for announced maintenance
Support Time	
Support Time ¹	Mo–Fr 08:00-17:00 ²
Fault acceptance	Mo–Su 00:00-24:00
Availability	
Service Availability	
• Signature service	99.8%
• Directory services according to CP/CPS section 3.1	99.9%
Security	
	See base document

¹ If the Signing Service was supplied by a Swisscom partner, the latter should generally be contacted in the event of faults. If the partner is not able to rectify the fault, the partner will pass it on to Swisscom.

² See the holidays definition in the base document (SLA definitions)



Service level & target values	Electronic personal signatures
Continuity	
Service Continuity (STSSC) ³ RTO 4 h RPO 1 h	●
● = Standard (included in the price) ○ = For an additional charge — = Not available	

6.2 Service level reporting

On request a Service Level Report is available showing the availability of a dedicated months.

7 Billing and quantity report

7.1 Billing

The details of invoicing are regulated in the service contract.

In principle, there are three billing methods:

7.1.1 Renumeration per signature – postpaid model

In this case, the quantities of signatures of the last service period are counted and charged with the price provided for this purchase quantity as mentioned in the service contract. With this billing model, any authentication procedure permitted in the service contract can be used for signature declaration of will.

7.1.2 Renumeration per active signatory – postpaid model

In this case, the number of active signatories in the last service period is counted and charged with the price provided for this purchase quantity as mentioned in the service contract. There can be a maximum number of allowed signatures per signatory per service period. Surplus signatures are then charged individually according to the model of 7.1.1 with the price provided for this subscription quantity. This billing model can only be used to a limited extent for certain authentication methods and is subject to special obligations for the subscriber in accordance with 5.2.

7.1.3 Renumeration according to volume-based usage prices – prepaid model

In this case, the subscriber determines the planned service period and the planned number of signatures in advance. He commits himself 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. Exceeding volumes shall be charged subsequently in accordance with the price in the service contract as described in 7.1.1. An increase in the volume is possible under certain circumstances during the term of the contract by concluding a new contract.

7.2 Quantity report

Quantity reports are regulated in the service contract. Anonymised reports with all signature queries for a service month can be requested on demand to clarify problems. Swisscom reserves the right to charge for the delivery of individual service reports in the event of regular requests.

8 Special provisions

8.1 Subscriber application

The Subscriber application is not part of this service description. It is provided by the Subscriber itself, by a Swisscom partner or by Swisscom.

³ RTO and RPO only concern the provision of the Signing Service on SAIP. Mobile services used for the identification, authentication or declaration of consent are not included here.



8.2 Signature types and their applications

It is the Subscriber's responsibility to obtain professional clarification of the legal implications of the selected type of electronic signature (with and without time stamp) made available to the signatories. Swisscom accepts no responsibility in this regard.

Qualified electronic signature (QES, Swisscom (Switzerland) Ltd. diamond class certificate): The QES created via the Signing Service meets the characteristics defined in the CP/CPS and the definition in accordance with art. 2 (e) of the Federal Act on Certification Services in relation to Electronic Signatures (ZertES; SR 943.03). Only the Qualified Electronic Signature accompanied by a qualified time stamp is equivalent to a handwritten signature under the application of Swiss law provided there are no statutory or contractual provisions to the contrary (Art. 14 para. 2bis of the Swiss Code of Obligations).

Qualified electronic time stamp: The qualified electronic time stamp created using the Signing Service meets the characteristics defined in the CP/CPS and the definition in accordance with art. 2 (j) ZertES.

Advanced electronic signature (AES, certificate of Swisscom (Switzerland) Ltd. sapphire class): The AES created via the Signing Service meets the characteristics defined in the CP/CPS. The AES is (in contrast to the QES) not governed by law in Switzerland and does not meet the legal requirement of the written form pursuant to article 12 of the Swiss Code of Obligations so does not have the same legal validity as a handwritten signature. The legal requirement of the handwritten signature (requirement for simple written form) can generally only be replaced equivalently by the QES together with a qualified electronic time stamp which should not be confused with the AES based on advanced certificates.

Depending on the situation, some documents therefore require the handwritten signature or the QES with a qualified electronic time stamp in order for the intended legal validity to enter into effect at all.

The validity of electronic signatures created via Signing Service in accordance with the certificate guidelines (CP/CPS) for the issuing of certificates issued by the issuing CAs "Diamond" (qualified) and "Sapphire" (advanced) may differ under the application of foreign law and may be more or less extensive compared to Swiss law.

The exchange of encrypted data and the issuing of certificates is also subject to legal restrictions in/with certain states.

8.3 Data processing by third parties in Switzerland or abroad, emergency access

Data sent to Swisscom by the Subscriber and on behalf of the signer within the scope of the provision of the services (Subscriber data) is generally processed by Swisscom in cooperation with Swisscom (Switzerland) Ltd. in Switzerland. Any data processing by third parties commissioned by Swisscom and/or from abroad is always carried out in accordance with the applicable provisions of the Swiss Data Protection Act. Such processing may occur if, for example, employees are domiciled in the EU (cross-border commuters), during business trips as well as by the maintenance divisions of foreign manufacturers from the EU. Within the framework of this service, the following constellations are affected by processing of this kind:

- Swisscom Trust Services Ltd. fulfils as service provider roles within the trust service of Swisscom (Switzerland) Ltd. in operation and support and has access to the registration and signing data under control and by order of Swisscom (Switzerland) Ltd.
- In the event of support cases from the EU, the 3rd level support of the application manufacturer has temporary VPN access to application data at Swisscom, which does not include any personal data other than the data published by the signatory in the certificate. The signature data published by the signatory in the certificate and the master data of the Subscriber organisation (e.g. organisation name, designation of the SSL certificate published by the Subscriber) may be visible to these third parties in individual cases. Access is monitored in real time by a Swisscom technician to ensure that there is no unsupervised access to data and that the connection can be severed immediately in the event of any misuse. This process corresponds to the best-practice approaches used in the banking and insurance sectors.
- Supervisory authorities and conformity assessment authorities which must confirm the conformity of the signature application may come into contact with personal and identification data as part of audits under the supervision of Swisscom in order to assess the compliant implementation of identity verifications and the issuing of signatures. These compliance assessments only take place in Switzerland.