



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

Service Description Signing Onboarding

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	2
2	Service overview	3
3	Definitions.....	4
3.1	Service Access Interface Point (SAIP).....	4
3.2	Service-specific definitions	4
4	Variants and options.....	5
4.1	Definition of the service specifications and options.....	5
5	Service provision and responsibilities.....	8
6	Service levels.....	9
6.1	Service levels	9
6.2	Service level reporting	9
7	Billing	10
8	Special provisions.....	10
8.1	Service limitations	10
8.2	Data processing	10









2 Service overview

Signing Onboarding is a bundle of targeted, optional support services of Swisscom Trust Services Ltd. that enable electronic signatures to be integrated into Subscriber processes in a Subscriber-specific manner and within a reasonable period of time. Starting with a workshop, these services address topics ranging from “the Subscriber’s own identification procedures” and “authentication procedures” to registration with the auditor and compliance assessment authorities, all as per the Subscriber’s requirements. They may also be called up individually as a service. The provision of support services for onboarding to the Swisscom Signing Service enables Subscribers to receive project-specific support in order to connect their process environment to the Swisscom Signing Service quickly and in a targeted manner while taking the legal and regulatory requirements into account.

This service does not yet require a Swisscom Signing Service to be ordered.

Before the electronic signature service can be provided, the following points first have to be clarified:

- Signature: What are the typical procedures for signing? What is the connection between identification and signing?
- Identification: Which procedure identifies potential signatories? Can existing subscriber-specific forms of identification be used? Which identification procedures can be used for what signature quality? How is identification archived?
- Signature Approval: Which authentication options are available for signature approval? Can subscriber-specific procedures be used if necessary? Which authentication procedures can be used for what signature quality?
- Audit: Which procedures require prior audits? Which have already been approved? Or which procedures are tested within the scope of renewed auditing? What are the legal differences between Switzerland and the EU?

Subscriber Environment <ul style="list-style-type: none"> • Digital transformation by use of electronic signature • If applicable subscriber-specific authentication means for declaration of will • If applicable subscriber-specific identification method • Anti-money laundering 	 
Signing Onboarding Option <ul style="list-style-type: none"> • Consultancy: use of standard components or subscriber-specific ones • Coordination audit / conformity assessment (if necessary) • Use of signatures for identification in scope of AML 	 
Signing Service and Smart Registration Service <ul style="list-style-type: none"> • Signature based on Smart Registration Service Identification • Authorized registration method 	 

Swisscom Trust Services Ltd. provides its own experienced staff and selected partners to support the Subscriber within the framework of this package. Swisscom Trust Services Ltd. advises the Subscriber with regard to the integration of electronic signatures into the Subscriber’s target processes, including any required approval and auditing, or on drawing up alternative concepts.

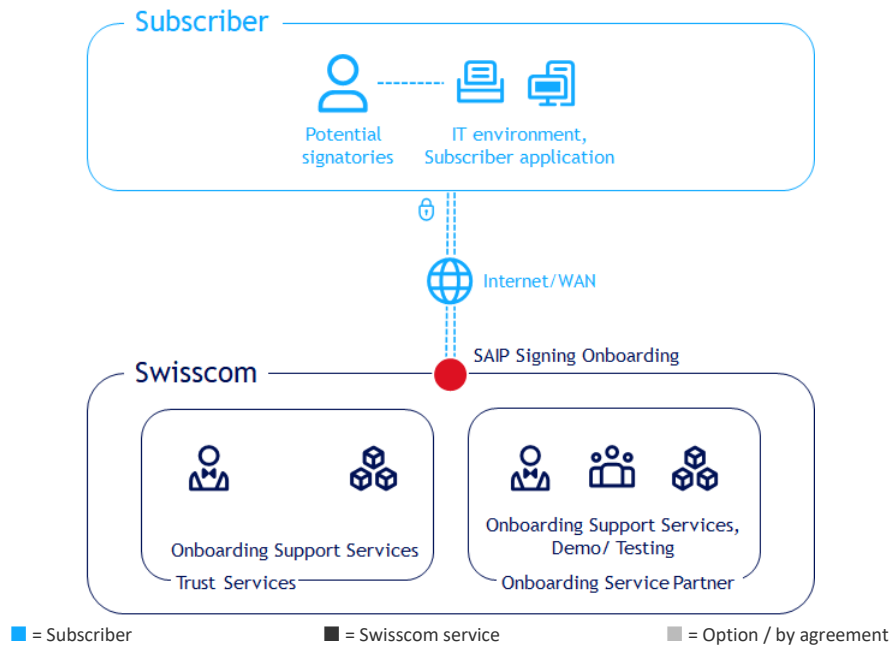


3 Definitions

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 delivered to the Subscriber (service user). It is also the point at which a service is monitored, and the provided service level is documented.

This is located at Swisscom for the scope of service defined in this service description, even if some workshops and meetings may take place on the Subscriber's premises.



3.2 Service-specific definitions

Term	Description
eIDAS regulation	An EU regulation on electronic identification and trust services for electronic transactions within the internal market.
Evidence	Proof in the form of a signed PDF document. This PDF typically contains the photos and scans created during the identification process as well as the collected data or other data required by regulatory authorities as proof of identification. The electronic signature of the organisation that carries out the identification is attached to the evidence.
Identification partner	Swisscom partners that handle identification and the submission of evidence as part of the Smart Registration Service or directly for the subscriber application.
RA delegation contract	A contract between Swisscom and the identifier to which Swisscom has recourse for implementing the identification procedures.
Registration	A regulated process for identifying and storing identification data and the means of authentication associated with such identification data that are required to trigger an electronic signature via the Signing Service.
Registration authority (RA)	The registration authority is responsible for identifying the signatories. Under an RA delegation agreement, Swisscom trust service may outsource parts of the registration process to third parties.
Signing app	The counterpart to the signature service: The user interface for the signatory, used for displaying the document, triggering signing, hashing, receiving the signed hash and creating the signed document from the signed hash, with the option to download the signed document.
Subscriber	Swisscom provides the services covered by this service description to the subscriber. The subscriber is either a direct Subscriber of Swisscom with a Signing or Registration service contract or has a commercial contract with a reseller of Swisscom services.



Term	Description
Subscriber application	The subscriber provides one or more persons with access to an application with which they can register for the Signing Service in accordance with Swisscom's terms and conditions of use or sign documents. The subscriber application is not part of this service description. It is normally provided outside of the Swisscom Service, for example, by partners of Swisscom or the subscriber itself.
Terms and conditions of use	The terms and conditions of use for Swisscom's signature service define the conditions for utilisation of the signature certificates and signature service on a subscriber application within the framework of the relationship between Swisscom (Switzerland) Ltd or Swisscom IT Services Finance S.E. and the signatory. They may be consulted at https://trustservices.swisscom.com/downloads .
ZertES	The Swiss federal law on electronic signatures

4 Variants and options

Standard variant	Signing Onboarding
Onboarding support workshop	<input type="radio"/>
Use of a Subscriber specific identification and/or signature approval solution/archiving: Development of an implementation concept	<input type="radio"/>
Audit and Audit Support	<input type="radio"/>

○ = For an additional fee

4.1 Definition of the service specifications and options

Specification/Option	Definition
Onboarding support workshop (standard or Subscriber's own registration procedure)	<p>Advice and implementing the steps needed to integrate an electronic signature using approved standard procedures or initial analysis of the envisaged subscriber-specific identification and/or authentication solutions. This includes the following aspects:</p> <p>The project will start with a joint workshop which will clarify the following points:</p> <ul style="list-style-type: none"> • The Subscriber's requirements • The legal/regulatory framework for the Subscriber and Swisscom • The safety and security requirements • The registration procedure (identification and allocation of the means of authentication for signature approval) • The signing procedure, session control • Presentation/comparison of Swisscom's standard procedures • API adaptation (integration in the signature flow) • One-shot signature vs. repetitive signing • Import data structure of an evidence • Own archival of evidences vs. archival at Swisscom • Audit cycles and audit procedures • Effects of other laws on the signature: consumer protection, GDPR/DSG, NIS2, AML, AI Act (biometry) • Introduction of the implementation concept template • Project planning



Specification/Option	Definition
	<p>The following people from the Subscriber's organisation should participate in this workshop (duration: 4-6 hours depending on complexity):</p> <ul style="list-style-type: none"> • Security officer • Legal contact person • Project manager • System architect <p>If the Subscriber cannot provide its own implementation resources or its own signing app, STS will suggest suitable partners that already have a tested and proven interface to the Swisscom Signing Service.</p> <p>If standard procedures are not used, contact persons are defined to draw up the implementation concept together with Swisscom. The results are summarised by Swisscom in a final document and handed over to the Subscriber.</p>
<p>Use of a Subscriber specific identification and/or signature approval solution/archiving: Development of an implementation concept</p>	<p>If a subscriber-specific identification or signature approval process is used, the subscriber elaborates an implementation concept by support of Swisscom (template and reviews). The contents of the implementation concept are as follows:</p> <ul style="list-style-type: none"> • Governance (service responsibility, organisational anchoring, role concept): A role concept, including security officers, system officers and training officers, must be available for presentation on request. Particular attention must be paid to the separation of roles. • Processes (identification, roles during identification, signature creation, acceptance of the Signing Service's terms and conditions of use within the process, control of signature approval, data administration, administration of the distinguished name, conformity checks and the information provision obligation): The identification type and procedure must be described in detail. During signing, the physical presence (or equivalent procedure) of the applicant is important when verifying his identity and a using photo ID as proof of his identity. The validity of the identification at the time of signing must be ensured. Security aspects with regard to secure communication, failed attempts at signing, etc. must be described. The identification process must also include the subsequent means of authentication. The indivisible testing procedure, comprising identity checking and the means of authentication, must be described. The terms and conditions of use for Swisscom's signing service of must be verifiably accepted by the identified person at the time of identification. Swisscom procedures (Smart Registration Service) can also be used to support this process. Data from the registry (archiving of documentation, archive transfer/storage after contact termination, archive transfer after the discontinuation of business activities, data protection): All proofs of identification (IDs or passport copies) and acceptance of the terms and conditions of use must be archived (for at least 11 or 35 years respectively). Procedures must be described to detail how such proofs are transferred to Swisscom if business operations or the contract are discontinued. Alternatively, the evidence can be imported permanently. All employees must be trained in the employed procedure. Training and proof of training must be described. All employees must comply with the necessary data protection measures and treat data as confidential. Options for Swisscom's auditor and Swisscom itself to review the process must be demonstrated. • Evidence records can be archived at the subscriber's premises as part of the implementation concept and audit, or it can be handed over to Swisscom Trust Services for archiving. Archiving concept must be described.



Specification/Option	Definition
	<ul style="list-style-type: none">• Technical details (the structure of the distinguished name, details of the declaration of intent, infrastructure protection)• Cybersecurity measures and risk management processes <p>If analysis of the intended identification and authentication approach shows that the procedure cannot be recognised in its present form, the individual measures necessary to adapt the procedure are documented and analysed</p>
Audit and Audit Support	<p>Only if it has been determined that an initial audit is required and on condition that an implementation concept has been prepared in advance.</p> <p>Depending on the jurisdiction where the electronic signature is to be used – i.e. Switzerland or the EU – and the employed procedure, this procedure may need to be audited and approved by the compliance assessment authorities or supervisory authority.</p> <p>Audits are usually carried out in accordance with ETSI or CEN regulations and the legislation on which registration or remote signing are based. Swisscom will commission, support and coordinate the audit procedure. The costs of auditing by Swisscom-appointed auditors are included in this option. The costs are determined together with the customer and the auditor and presented transparently with the corresponding management fee for this offer point.</p> <p>If analysis of the intended identification and authentication approach or audits reveals that the procedure cannot be recognised in its present form, the individual measures necessary to adapt the procedure are documented and analysed.</p> <p>When conducting the audit, the following types of audits must be differentiated, which are offered at a separate price if requested:</p> <ul style="list-style-type: none">• Audits of the Subscriber’s own authentication procedure and securing a two-factor declaration of intent (known as “sole control 2” or SCAL2)• Audits of the Subscriber’s own identification method, if – depending on the intended jurisdiction – this has not already been audited by an auditor approved for the eIDAS regulation or ZertES.• Audits of the archiving of evidence data to identify and obtain acceptance of the terms and conditions of use, unless the archiving option of the Smart Registration Service is used. <p>Swisscom shall support the ordering of the audit or the submission of the audit paid for by the subscriber to the supervisory bodies and shall carry out any necessary further clarifications with these supervisory bodies and conformity assessment bodies.</p>



5 Service provision and responsibilities

Non-recurring services

Activities (S = STS/Sb = Subscriber)	S	Sb
Onboarding support workshop		
1. Provision <ul style="list-style-type: none"> Person responsible for the signing connection Legal contact person System architect Security officer associated with signing connection / registration 		✓
2. Provision <ul style="list-style-type: none"> Specialists for exchanging information on regulatory and legal requirements Specialists for the system architecture and security concept 	✓	
3. Providing MS Teams session or alternatively, on request space / meeting rooms at Swisscom	✓	
4. Optional instead of 3: Providing space / meeting rooms on the Subscriber's premises by arrangement. Travel by Swisscom at the stipulated travel expenses rate.		✓
5. Clarifying any questions arising in connection with electronic signatures and ID processes, in particular for assessing the various qualities of electronic signatures and their possible use to fulfil the Subscriber's specific needs or in areas where special regulations apply, such as the German Money Laundering Act, see also subsection 8b).		✓
6. Initial statements on feasibility based on regulatory/legal requirements	✓	
7. Workshop deliverable	✓	
Use of a Subscriber specific identification and/or signature approval solution/archiving: Development of an implementation concept		
1. Provision <ul style="list-style-type: none"> The system architect, security officer and the person responsible for the signing connection jointly develop the relevant topics within the implementation concept. Appointing deputies, where required, to ensure rapid response times 		✓
2. Developing an implementation concept framework that comprises all the points needed for an audit or repeat audit based on input from the Subscriber and a review of the Subscriber's suggestions	✓	
3. Finalising the implementation concept ready for submission to the auditor		✓
4. Approval of the implementation concept by Swisscom for use within the scope of ZertES or the eIDAS regulation or documenting the necessary changes and risks or rejecting this and suggesting changes	✓	
5. Providing MS Teams or alternatively on request space / meeting rooms at Swisscom.	✓	
6. Optional instead of 5: Providing space / meeting rooms on the Subscriber's premises by arrangement. Travel by Swisscom at the stipulated travel expenses rate.		✓
7. Template the implementation concept to be signed by the Subscriber or documenting the measures necessary to implement the process	✓	
Audit and audit support		
1. Defining a necessary environment for the initial audit, provision by Swisscom of the elements required for testing (e.g. test access)	✓	
2. Provision by the Subscriber of the subscriber application and all documents needed for the procedure (flow, security, etc.) to enable the auditor to perform the audit		✓
3. Appointing the auditor and coordinating the auditor's work based on the schedule developed together with the Subscriber and the implementation concept. Elaboration of audit scope and covering the cost of the auditor.	✓	



Activities (S = STS/Sb = Subscriber)	S	Sb
4. Provision <ul style="list-style-type: none"> A system architect, security officer and a person responsible for the signature connection to support the auditor Appointing deputies, where required, to ensure rapid response times 		✓
5. Joint auditing discussion with the auditor		✓
6. Internally evaluating auditing results, documenting open issues and next steps	✓	
7. Optional adaptation of the registration or signing process by the Subscriber based on feedback from the auditor (if required based on 6)		✓
8. If the auditing result is positive: Submitting the auditing results and registering the new procedure with the supervisory authority, clarifying/presenting and discussing this with the supervisory authority	✓	
9. Releasing the procedure based on feedback from the supervisory authority, the compliance assessment authority and auditors	✓	
10. Providing MS Teams or alternatively on request space / meeting rooms at Swisscom.	✓	
11. Optional instead of 10: Providing space / meeting rooms on the Subscriber's premises by arrangement. Travel by Swisscom at the stipulated travel expenses rate.		✓
12. Auditing of the procedure, i.e. the audit report by the auditor or alternatively documentation of the open points needed for the auditor's approval of the procedure	✓	

6 Service levels

6.1 Service levels

The following service levels generally relate to the agreed Support Times. Definitions of terms (Support Time) and the description of the measurement method and reporting are based on the contractual base document (e.g. "SLA Definitions"). The following service levels will be provided for the different service variants in accordance with subsection 3. If more than one service level is available per variant, the service level is defined in the service contract.

Service levels & target values	Signing Onboarding
Support Time	
Support Time Mo-Fr 08:00-17:00 ¹	●

● = Standard (included in the price)

Responsibility for the conformity of the identification, authentication and archival procedures used lies with the Subscriber. This means that Swisscom cannot guarantee that the procedures will receive a positive conformity assessment.

6.2 Service level reporting

Standard service-level reporting is not provided in conjunctions with Signing Onboarding.

¹ See the holidays definition in the base document (SLA definitions)



7 Billing

Invoices are issued after one of the corresponding service packages has been accessed:

Performance option	Definition
LO1	Onboarding Support Workshop (Standard or own registration procedures)
LO2	Implementation concept for the first identification and signature approval method, or IDP and other implementation concepts An implementation concept must be ordered and developed for each identification method and each signature approval method. The first implementation concept contains both an identification solution and a signature approval method.
LO3	Audit price of the authorized auditor in accordance with his offer and prior service agreement with the subscriber ("Scope") plus STS surcharge for commissioning the auditor, monitoring the submission of the audit report to the authorities.
	Optional project costs for integration of the methods in the stores or signature flow incl. testing and activation.

In the event of travel, travel expenses are due in addition to the invoice items.

8 Special provisions

8.1 Service limitations

- a) The standard scope of the services does not include any technical implementation work connecting the Subscriber's target system to Swisscom's signature testing service or the creation/provision of signing apps or more complex testing that goes beyond the three-day implementation period. Swisscom partners are available for this purpose.
- b) **The services provided by Swisscom do not include legal advice.** Within the framework of service provision, Swisscom Trust Services Ltd. may also, for example, comment on legal assessments, including on topics concerning the Subscriber's legal or regulatory framework, etc. However, it is the Subscriber's exclusive responsibility to carefully study the legal circumstances affecting it, draw its own conclusions and to inform Swisscom if its assessment yields different opinions. Swisscom recommends that the Subscriber consult experts where necessary to clarify any questions that arise, in particular to assess the various qualities of electronic signatures and their possible applications to meet the Subscriber's specific needs or in areas where special regulations apply, such as the Money Laundering Act.

8.2 Data processing

The processing of Subscriber and/or personal data is not envisaged within the scope of these support services. If demo installations are used, these can use fictitious test data sets.