Service description

Signing Onboarding
Provision of onboarding support

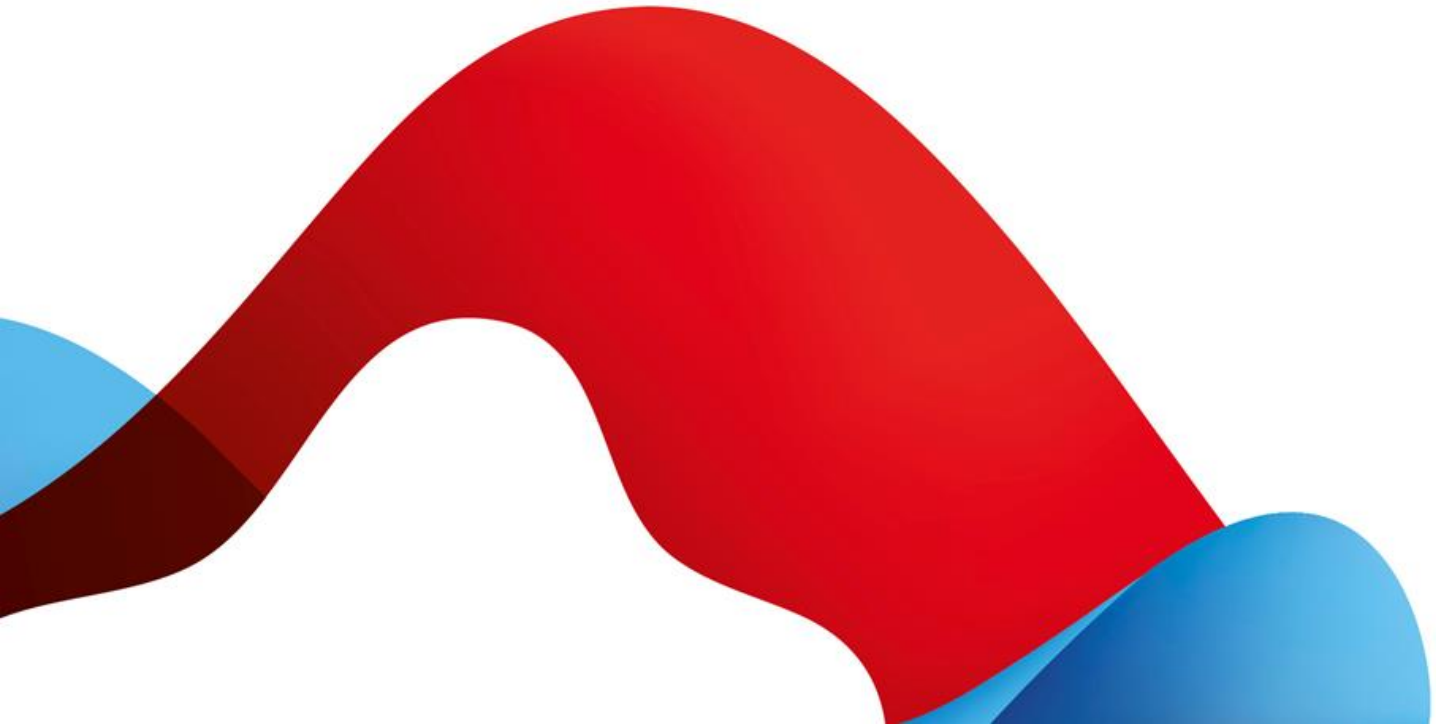


Table of contents

1 Service overview

Signing Onboarding is a bundle of targeted, optional support services that enable electronic signatures to be integrated into customer processes in a customer-specific manner and within a reasonable period of time. Starting with a workshop, these services address topics ranging from “the customer’s own identification procedures” and “authentication procedures” to registration with the auditor and compliance assessment authorities, all as per the Customer’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 customers 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 customer-specific forms of identification be used? Which identification procedures can be used for what signature quality? How is identification archived?
- Authentication: Which authentication options are available for signature approval? Can customer-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?
- Test: How can a test signature be set up quickly to learn about the processes in greater detail?
- Signatures for identification within the context of preventing money-laundering: Which technical procedures are necessary to ensure efficient identification when combatting money laundering?

Customer Environment
- Digital transformation by use of electronic signature
- If applicable customer own authentication means for declaration of will
- If applicable customer own identification method
- Anti-money laundering

Signing Onboarding Option
- Consultancy: use of standard components or customer specific ones
- Koordination audit / conformity assessment (if necessary)
- Use of signatures for identification in scope of AML

All-in Signing Service and Smart Registration Service
- Signature based on Smart Registration Service Identification
- Authorized registration method

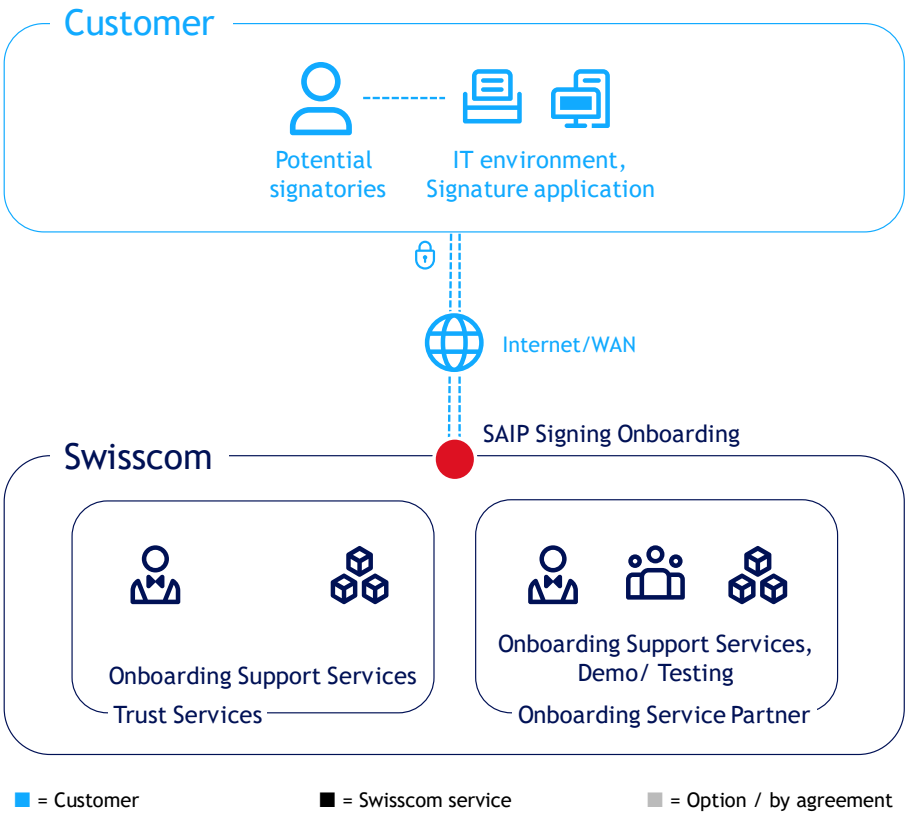
Swisscom provides its own experienced staff and selected partners to support the Customer within the framework of this package. Swisscom advises the Customer with regard to the integration of electronic signatures into the Customer’s target processes, including any required approval and auditing, or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

2 Definitions

2.1 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 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 Customer's premises.



2.2 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 customer 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.

Term	Description
Registration authority (RA)	The registration authority is responsible for identifying the signatories. Under an RA delegation agreement, Swisscom 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.
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://www.swisscom.com/signing-service.
ZertES	The Swiss federal law on electronic signatures

3 Variants and options

Standard variant	Signing Onboarding
Onboarding support workshop	○
Use of a customer-specific identification and/or authentication procedure: Development of the implementation concept	○
Use of a customer-specific identification and/or authentication procedure: Audit support	○
Support during the preparation of an audit by the Customer	○
Use of the registration procedure / signature for identification purposes in combatting money laundering	○
Technical training: API connection	○
Test and demo system (mock-up)	○

○ = For an additional fee

3.1 Definition of the service specifications and options

Specification/Option	Definition
Onboarding support workshop (standard or Customer's own registration procedure)	Advice and implementing the steps needed to integrate an electronic signature using approved standard procedures or initial analysis of the envisaged customer-specific identification and/or authentication solutions. This includes the following aspects: The project will start with a joint workshop which will clarify the following points: ▪ The Customer's requirements ▪ The legal/regulatory framework for the Customer and Swisscom ▪ The safety requirements ▪ The registration procedure (identification and allocation of the means of authentication) ▪ The signing procedure ▪ Presentation of Swisscom's standard procedures

Specification/Option	Definition
	The following people from the Customer's organisation should participate in this workshop (duration: 4-6 hours depending on complexity): ▪ Security officer ▪ Legal contact person ▪ Project manager ▪ System architect If the Customer cannot provide its own implementation resources or its own signing app, Swisscom will suggest suitable partners that already have a tested and proven interface to the Swisscom Signing Service. 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 Customer.
Use of a customer-specific identification and/or authentication procedure: Implementation concept	If a customer-specific identification or authentication process is used, an implementation concept is drawn up together with the Customer. The contents of the implementation concept are as follows: ▪ 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. ▪ Technical details (the structure of the distinguished name, details of the declaration of intent, infrastructure protection)

Specification/Option	Definition
	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
Use of a customer-specific identification and/or authentication procedure: Audit support	Only if it has been determined that an initial audit is required and on condition that an implementation concept has been prepared in advance. 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. 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. 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 When conducting the audit, the following types of audits must be differentiated, which are offered at a separate price: ▪ Audits of the Customer's own authentication procedure and securing a two-factor declaration of intent (known as "sole control 2" or SCAL2) ▪ Audits of the Customer'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.
Support during the preparation of an audit by the Customer	If the Customer does not have documentation, process descriptions or security concepts for an audit of the Customer's own identification or authentication procedure, project-specific support can be provided.
Use of the registration procedure / signature for identification purposes in combatting money laundering	Advice and support as well as documentation of the necessary procedural and technical steps for determining an identity within the context of combatting money laundering. If the Customer has to perform identification in accordance with the German Money Laundering Act, two procedures are shown for identification in connection with an electronic signature: ▪ Use of the electronic signature for determining the user's identity ▪ Use of identification data for registration for the electronic signing, also for the purpose of determining identity within the context of combatting money laundering Special requirements must be observed depending on the procedure chosen, e.g. signature verification or data-protection contracts within the framework of GDPR requirements.
Technical training: API connection	If the Customer wants to develop or integrate its own signing app or works with a partner who is not yet a Swisscom partner, technical training in API integration is recommended. This comprises a three-hour joint Skype/Team session involving the Customer's developers and technical managers at Swisscom. Within the scope of this training, the interface is discussed in detail and a sample application is connected. Afterwards, questions about implementation can be answered within the scope of five hours of support, which are available on demand.
Test and demo system (mock-up)	A mock-up system used to test the signing system. This does not include full integration into the Customer's system.

Specification/Option	Definition
	For the test, Swisscom provides standard test access appropriate for the procedure to be evaluated. If a signing app of a Swisscom partner is used, the partner will be commissioned to create a demo app for use in conjunction with the testing access. If the Customer wishes to use a signing app itself, only the interface for test access, including the appropriate configuration, is provided. The test includes access both for the implementation of electronic signing and for use of services within the context of registration, where necessary. The access is configured accordingly.

4 Service provision and responsibilities

Non-recurring services

Activities (S = Swisscom/C = Customer)	S	C
Onboarding support workshop		
1. Provision ▪ Person responsible for the signing connection ▪ Legal contact person ▪ System architect ▪ Security officer associated with signing connection / registration		✓
2. Provision ▪ Specialists for exchanging information on regulatory and legal requirements ▪ Specialists for the system architecture and security concept	✓	
3. Providing space / meeting rooms at Swisscom on request or alternatively Skype/Teams.	✓	
4. Optional instead of 3: Providing space / meeting rooms on the Customer'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 Customer's specific needs or in areas where special regulations apply, such as the German Money Laundering Act, see also subsection 7b).		✓
6. Initial statements on feasibility based on regulatory/legal requirements	✓	
7. Workshop deliverable	✓	

Use of a customer-specific identification and/or authentication procedure: Implementation concept

1. Provision ▪ 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 Customer and a review of the Customer'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 space / meeting rooms at Swisscom on request or alternatively Skype/Teams.	✓	

Activities (S = Swisscom/C = Customer)	S	C
6. Optional instead of 5: Providing space / meeting rooms on the Customer's premises by arrangement. Travel by Swisscom at the stipulated travel expenses rate.		✓
7. Drafting the implementation concept to be signed by the Customer or documenting the measures necessary to implement the process	✓	
Use of a customer-specific identification and/or authentication procedure: 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 Customer 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 Customer and the implementation concept. Covering the cost of the auditor.	✓	
4. Provision ▪ 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 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 Customer 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 space / meeting rooms at Swisscom on request or alternatively Skype/Teams.	✓	
11. Optional instead of 10: Providing space / meeting rooms on the Customer'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	✓	
Support during the preparation of an audit by the Customer		
An individual offer from Swisscom based on Customer's requirements	✓	
Use of the registration procedure / signature for identification purposes in combatting money laundering	☐	
1. Presentation of the standard electronic signing procedures with regard to combatting money laundering	✓	
2. Creating a concept for using the registration data, support for any contracts (e.g. order data processing) concluded with Swisscom's identification partner	✓	
3. Creating a concept for identity verification in line with money-laundering regulations based on signing and signature validation	✓	
4. Signing contracts with Swisscom's identification partner		✓
5. Handover of concept documentation to the Customer	✓	
6. Documenting the procedural and technical steps required by law to establish identification within the context of combatting money laundering	✓	

Activities (S = Swisscom/C = Customer)		S	C
Technical training: API connections		▫	
1.	Three-hour joint workshop via Skype/Teams or on site at Swisscom. Expenses will be charged additionally for travel. Joint setup of a test connection to the signing service. Specific answers to customer-specific questions	✓	
2.	Optional instead of 1: Organising and providing space /meeting rooms on the Customer's premises by arrangement. Travel by Swisscom at the stipulated travel expenses rate.		✓
3.	Five hours of consultancy during the subsequent three months to address technical questions about the connection	✓	
Test and demo system (mock-up)		▫	
1.	Configuration and activation of test access to the Signing Service, if necessary also to the Smart Registration Service in accordance with the requirements determined in the workshop or special requirements as per the implementation concept	✓	
2.	Connected demo app from a Swisscom partner for demonstration purposes and to generate a non-qualified test signature	✓	
3.	Connection of the Customer's own demo app to the API in accordance with the interface specification reference guide		✓

5 Service levels

5.1 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 other contract elements (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 [1]	Mo-Fr	07:00-18:00	●

● = Standard (included in the price)

5.2 Service level reporting

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

[1] Consulting services are provided at these times.

6 Billing

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

Performance option	Definition
LO1	Onboarding support workshop (standard or Customer's own registration procedure)
LO2	Use of a customer-specific identification and/or authentication procedure: Implementation concept
LO3	Use of a customer-specific identification and/or authentication procedure: Audit support
LO4	Support during the preparation of an audit by the Customer
LO5	Use of the registration procedure / signature for identification purposes in combatting money laundering
LO6	Technical training: API connection
LO7	Test and demo system (mock-up)

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

7 Special provisions

7.1 Service limitations

a) The scope of the services does not include any technical implementation work connecting the Customer'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 may also, for example, comment on legal assessments, including on topics concerning the Customer's legal or regulatory framework, etc. However, it is the Customer'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 Customer 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 Customer's specific needs or in areas where special regulations apply, such as the German Money Laundering Act.

7.2 Data processing

The processing of customer 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.