Order by Swisscom Partner

All-In Signing Service Seals in Switzerland and EU

Order No.

PRO No.

(numbers will be filled in by Swisscom in the order confirmation)

Partner:

End customer:

Please use Adobe Acrobat to fill in the form!

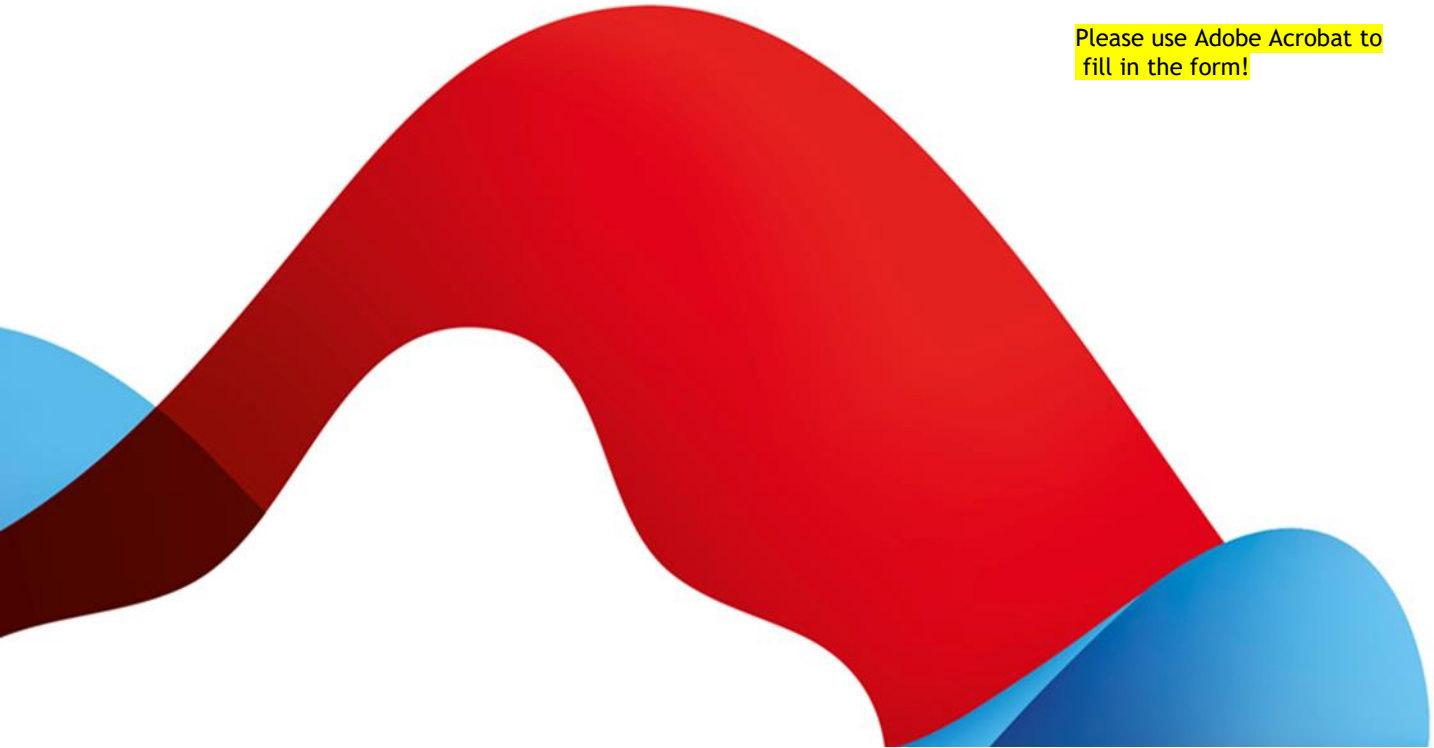

Table of contents

1 Purpose of the document

This order enables Swisscom to provide the All-in Signing Services of Swisscom (Switzerland) Ltd or Swisscom IT Services Finance S.E. Vienna to the end customer of the partner (hereinafter referred to as "end customer"). The service provider is:

Swisscom (Switzerland) AG
enterprise customers
Identification Services
Pfingstweidstrasse 51
CH-8005 Zurich (hereinafter referred to as "Swisscom")

The order is placed by the partner of Swisscom:

Company name / organisation name	
Address	
Postcode/Town	
Country	

hereinafter referred to as "Partner". The order is based on the provisions of the valid signed "Partner Agreement for Reselling All-in Signing Services" between Swisscom and the Partner.
The end customer addresses the AIS service via a "subscriber application". The subscriber application is used by the signatories who intend an advanced, regulated or qualified seal. The end customer is the following organization (details in the attached configuration and acceptance declaration):

Company name / organisation name	
Postcode/Town	
country	

2 Characteristics of the service for the end customer

2.1 Quality of signature, legal area (CH, EU)

Each service requires a separated ClaimedID!	Chosen option
Advanced seal according eIDAS regulation for the jurisdiction of EU/EEA	
Advanced seal according CP/CPS for the jurisdiction of CH	
Qualified seal according eIDAS regulation for the jurisdiction of EU/EEA	
Regulated seal according ZertES for the jurisdiction of CH	

☑ incl. timestamp (qualified only according ZertES)

The service will be provided based on the following service description:

- Swisscom Service base documents:
  - "Information Security" of Sept. 1st, 2018
  - "Service Glossary" of Sept. 1st, 2018
  - "Service Management Processes" of Sept. 1st, 2018
  - "SLA – Definitions" of Sept. 1st, 2018

The seal application will be operated by a subscriber. The subscriber can be the customer or a third party:

- ◉ Signed configuration and acceptance declaration of the subscriber is attached
- ○ Signed configuration and acceptance declaration of the subscriber will be forwarded
- ◉ Signed application for a certificate is attached and signed by a qualified signature
- ○ Signed application for a certificate is attached and shall be signed by a QES in the SwissTrustRoom

3 Checklist for filling in the certificate application form

(NA): "not applicable" or relevant based on the configuration of the service

Requirements for the application form	fulfilled
• Joint signature (according to registry) needed: 2 representatives entered • One signature (according to registry) needed: 1 representative entered Name, mobile number, e-mail of the representatives are entered. Please pay attention to the fact that the mobile number will be necessary for the confirmation of a revocation.	☐
Certain representatives are entered in the Register as authorised signatories	◉
Certain representatives are not entered in the register as authorised signatories but can present a power of attorney. This power of attorney to sign is signed by representatives according to the Commercial Register and is attached to the application.	○
Certain representatives have already been identified with the RA-App and can therefore sign the application electronically with a qualified signature.	☐
Certain representatives must make an appointment with Swisscom or authorised representatives and sign the application by hand during their presence. A power of attorney to sign - signed by representatives in accordance with the Commercial Register - must be presented. At the same time, a valid ID/passport of the signatories must be presented.	(NA)
End customer is registered in the commercial register.	☐

A valid extract from the commercial register is attached (original, not older than 3 months).	
A certified extract from the commercial register is attached (original, not older than 3 months).	(NA)
End customer is registered in the BIN Register (UID) of Switzerland	(NA)
The end customer is entered in the BIN Register of Switzerland and has not agreed to the publication of its data on the characteristics in accordance with Art. 11 para. 3 BINA. A current extract from the BIN Register is attached (original, not older than 3 months).	(NA)
The end customer is entered in the BIN Register of Switzerland and has not agreed to the publication of its data on the characteristics in accordance with Art. 11 para. 3 BINA. A current certified extract from the BIN Register is attached (original, not older than 3 months).	(NA)
End customer is not registered in the commercial register (e.g. simple partnership, association, etc.). A written power of attorney in favour of the designated representatives has been issued by the applicant's officers (e.g. CEO). An extract from the register or proof of the company in the official register is enclosed.	
The customer's access certificate will be sent to Swisscom.	(NA)
The access certificate is sent by the subscriber (operator of the signature application) to Swisscom and the subscriber is not the same as the end customer. The end customer has issued a power of attorney to the Subscriber for this.	(NA)
The access certificate is created in a common ceremony, i.e. the private key is created on a cryptographic module (FIPS 140 2 Level 2) and the corresponding certificate is created. The following cryptographic module is used (manufacturer, type, firmware version, version, certificate number FIPS or description of similar safeness)	

4 Contact person of the customer and 1st level support contact

☐ according to partner contract

First name	
Name	
Language	English
Organization (if different)	
Address (if different)	
Telephone number	
Mobile	
Email	

This person is authorised to contact Swisscom's 1st Level Support for ticket submission under the PRO number mentioned.

All incidents and technical notices are published by Swisscom under the link https://trustservices.swisscom.com/service-status. The contact persons should subscribe to this page via RSS feed (e.g. via Outlook) or view it regularly.

5 Contact person for Swisscom Roll-Out and Support

The partner can submit his support request regarding the end customer to 1st Level Support (telephone +41 (0) 800 724 724 or ent.incident-data@swisscom.com): The PRO number, which is stated in the order confirmation, must be stated here! The names are stored in the acceptance and configuration declaration of the end customer. The customer's technical contact can submit tickets (role "caller"). The end customer then announces two further contact persons who receive Swisscom fault reports, important technical information (role "notificator") or maintenance reports (role "maintenance").

6 Activation of the service

The service will be activated after the following points have been fulfilled:

- Sending of this order by e-mail to Swisscom in combination with the configuration and acceptance declaration and the certificate application
- Completion by Swisscom with contract number and PRO number and confirmation
- Signing and submission of the configuration and acceptance declaration by the end customer
- Fulfilment of all cooperation services within the scope of the connection by the end customer
- Optional conformity confirmations for procedures deviating from the standard
- Ceremony fort he creation of the private key of the access certificate (in case of regulated or qualified certificates)

The setup takes place within 2 weeks after fulfilment of these points.

7 Payment due

All prices quoted are in Swiss francs (CHF) and exclusive of VAT.

7.1 Service fee, connection prices and audit costs

Services	Comments	Annual charges	One-off charge
Annual connection charge per service interface (SAIP) • Advanced seals (CH) • Advanced seals (EU)	Annual billing, for the first time in the month after conclusion of contract		
Annual connection charge per service interface (SAIP) • Regulated seals (CH) • Qualified seals (EU)	Annual billing, for the first time in the month after conclusion of contract contains the common ceremony for key generation		
Option: additional seal with same signature certificate and different organizational unit (OU entry)	Can be ordered separately. Annual billing, for the first time together with the annual billing of the annual connection charge. Price per certificate.	CHF 500	
Consulting efforts for implementation of the interface	Up to 3 man hours Each further man day	Included Billed at cost	
	Special audit charges due to non-fulfilment of cooperation obligations	Billed at cost	

*) Daily rate: Swisscom 1'920.00 CHF, For the involvement of an auditor approx. 2'600.00 CHF have to be calculated. All prices plus expenses and travel expenses

7.2 Billing of the provision, connection and audit charges

The connection and optional audit charges are billed annually and for the first time in the month after activation of the service.
Optional one-off charges are billed after conclusion of this contract. The annual connection charges are invoiced at the start of each contractual year.
The charges incurred through the exercising of the right of inspection and control by Swisscom or third parties engaged by Swisscom are included in the list of charges above unless the result of the control justifies the Subscriber bearing the charges because they have failed to meet their cooperation obligations.
Any additional audit charges from third parties in the event of failure to fulfil cooperation obligations will be billed based on effective audit costs by Swisscom or third parties annually.
Any reimbursement in the event of premature termination of the contract is excluded.

7.3 Current usage charges

The usage will be charged "per seal".
The volume used for the contractual month concerned is the decisive factor. The charge per seal falls for the following seals when the threshold from one volume range to the next is exceeded.

Services	Volume range: Seals in the year via a service access internet point			Charge per seal
Advanced electronic or regulated seals (CH) with qualified timestamp according ZertES or advanced or qualified seal according eIDAS regulation (EU) with simple electronic timestamp	1	-	50'000	0.08
	50'001	-	500'000	0.06
	500'001	-	2'000'000	0.04
	Above			*)

*) according project agreement or contract specific price list

7.4 Billing of the current usage charges

The current usage charges will be billed at the end of a service month. The service invoice contains the number of seals made during the month.

Any reimbursement in the event of premature termination of the contract is excluded.

7.5 Use of several service access internet points

Volume ranges or signatories are applied per service access internet point. Volumes cannot be accumulated via several service access internet points.

7.6 Price list glossary

AIS service	All-In Signing Service which is provided up to the SAIP of Swisscom.
SAIP = Service Access Internet Point	The Service Access Interface Point (SAIP) is the contractually agreed logical point at which the service is delivered to the Customer and monitored and at which the service level is reported. It is the point of communication with the subscriber application

8 Submission

Order date:

This order will be submitted by e-mail to the following address:

msc.support@swisscom.com

You will then receive this order as order confirmation with added order number and PRO number for support cases by e-mail. The configuration and acceptance declaration signed by the end customer can be attached if digitally signed on the basis of the Swiss Digital Signature Legislation (ZertES).

Otherwise, the signed document shall be submitted by regular mail at:

Swisscom (Switzerland) AG
enterprise customers
Identification Services / Sales Support
Pfingstweidstrasse 51
8005 Zurich
Switzerland

9 Special project-specific information

Other data and configurations not mentioned above can be described here if necessary:

Configuration and acceptance declaration

All-In Signing Service for electronic seals in Switzerland and EU

Contract no.

(will be filled out by Swisscom)

By:

hereinafter referred to as “Subscriber”

Regarding:

Swisscom (Switzerland) Ltd, with its registered office in Ittigen

hereinafter referred to as “Swisscom”

Postal address

Swisscom (Schweiz) AG
Enterprise Customers
Identification Services
Pfingstweidstrasse 51
8005 Zürich
Schweiz

Please use Adobe Acrobat to fill out this form!

Table of Content

1 Object of the document

This document is attached to every order of an All-in Signing Service (hereinafter “AIS Service”) from Swisscom (Switzerland) Inc. for a user of this service, hereinafter “Subscriber”.

The advanced and qualified seals mentioned in the eIDAS Regulation of the EU are issued by the Trust Service of Swisscom IT Services Finance S.E in Vienna; Swisscom (Schweiz) AG accepts the configuration and acceptance declaration on behalf of Swisscom IT Services Finance S.E. in this context.

The Subscriber has a commercial contract with a Swisscom partner in conjunction with this declaration of configuration and acceptance. The Subscriber contacts the AIS service for a “subscriber application”. The subscriber application is used by creators of a seal (hereinafter "seal creator") who intend to use an advanced seal according Swiss CP/CPS or a regulated seal according Swiss federal act ZertES or an advanced or qualified seal according eIDAS regulation. Seal creators and subscribers could be same or different parties.

This statement serves as an overview of the desired service specification and of the responsible contact persons. It further contains the confirmation of obligations of Swisscom based on the general service description AIS for integrating the subscriber application in the All-in Signing Service.

The AIS Service can only be setup after all information is retrieved and the necessary obligations are confirmed.

This statement is used in the Swisscom audit pertaining to the accreditation authority or conformity assessment body to demonstrate the conformity of the AIS service.

(NA) = "not applicable". Please refer to appendices if the field size is not sufficient!

2 Information on the contract

2.1 Signature quality, jurisdiction (CH, EU)

Service quality	CH	EU
Advanced electronic seal according CP/CPS (CH)	☐	
Regulated electronic seal (CH)	☐	
Advanced electronic seal according eIDAS		☐
Qualified electronic seal according eIDAS		☐

☒ incl. timestamp (qualified only according ZertES)

2.2 Client software used

The following client software authorized by Swisscom is used to communicate with the AIS service (product description, version number or version status (date), manufacturer):

3 Service access

3.1 SSL access certificate

For qualified seals (EU) or regulated seals (CH), the seal creator and Swisscom issue the access certificate in a joint ceremony. This is based on a public key whose private key is stored on a cryptographic module or HSM with FIPS 140-2 certification.

In case of advanced seals, the Subscriber generates a self-signed SSL client certificate with a key length as per the current certificate guidelines (currently at least 2048 bits for RSA, 256 bits for SHA2) to authenticate the AIS service, and conveys this beforehand to Swisscom. Please use always the latest state of SSL/TLS configuration and test your application Internet portals, such as https://www.ssllabs.com/ssltest/ .

Content of the “subject” or “distinguished name” of the certificate:

- CN=<URL of the subscriber system that communicates with AIS or other unique identification of the subscriber system>
- O=<name of the organisation>
- C=<country of the organisation>

Valid for three years. No particular requirements are set for the use of the key.

3.2 Protection of the SSL access certificate

The SSL access certificate which protects the communication between the subscriber application and Swisscom AIS is handed over to the subscriber and Swisscom by the seal creator or his authorised representative. If the subscriber is not a seal creator itself, the subscriber ensures that the seal creator authorises the susbcriber to use the certificate.

In case of advanced seals the following must be ticked for access certificates:

(NA) A. The private keys of this SSL certificate are not stored in a readable format on the system but are themselves encrypted on the system or stored on a special password protected area.

(NA) B. The private keys of the SSL certificate are stored on external data carriers, which are kept in a secured place.

(NA) C. The private keys of the SSL certificate are managed autonomously through the subscriber application and are not accessible by the administrator.

☐ D. The SSL access certificate will only be used for the ClaimedID of the seal creator. In case of multiple ClaimedIDs multiple access certificates are necessary.

4 Protection of the subscriber application

☐ A. The subscriber application is protected against any unauthorised access/manipulation, and the operating system software and the software components used are regularly kept up to date (update, patching).

☐ B. It is prevented organizationally or technically if administrators have access to the subscriber application, abuse it (e.g. force a signature on a document other than the one released by the user for signature, etc.) or otherwise have unauthorized access. The protection concept in this regard can be proven to Swisscom at any time upon request.

5 Contact details of the operations team

5.1 Address of the Subscriber

Name of company / organisation	
Company ID (BIN)	
Address	
Postcode, town/city	
Country	

5.2 Support

Based on the commercial contract with a Swisscom partner, the partner will provide 1st level support and accept the participant's requests. You can also specify persons who receive system messages, important technical information (role "notificator") or maintenance messages (role "maintenance") from Swisscom. When entering your e-mail address, please make sure that the messages will reach you and, if necessary, use a team mailbox.
1st Level Support will be provided by Swisscom Partner:

Organisation	

5.3 First responsible in charge

At least two persons in charge must be designated

First name	
Surname	
Language	English
Organisation (if different)	
Address (if different)	
Phone number	
Mobile	
E-mail	

This person should *)

☑ Receive error messages and important technical information (Role "notificator")

☑ Receive service announcements (Role "maintenance")

*) All incidents and technical notices are published by Swisscom under the link https://trustservices.swisscom.com/service-status. The contact persons should subscribe to this page via RSS feed (e.g. via Outlook) or view it regularly.

5.4 Second person in charge

First name	
Surname	
Language	English
Organisation (if different)	
Address (if different)	
Phone number	
Mobile	
E-mail	

This person should *)

☐ Receive error messages and important technical information (Role "notificator")

☐ Receive service announcements (Role "maintenance")

*) All incidents and technical notices are published by Swisscom under the link https://trustservices.swisscom.com/service-status. The contact persons should subscribe to this page via RSS feed (e.g. via Outlook) or view it regularly.

When entering your e-mail address, please make sure that you are receiving the messages, and if necessary use a team mailbox.

6 Swisscom right of audit

Swisscom is authorised to check by means of auditing that subscribers are adhering to the requirements that apply to them as per this service description and the certificate guidelines (CP/CPS) in relation to the subscriber application, RA app and an optional external registration authority. Swisscom may have an audit carried out by their own employees or by a third party and share the results with the relevant conformity assessment offices and supervisory authorities. In carrying out the audit, Swisscom shall respect the normal business hours. The Subscriber shall grant access to all necessary documents and systems throughout the audit and shall guarantee Swisscom and any third parties commissioned or authorised by it in this context access to the required amount of space. Swisscom or its representatives shall sign an agreement in advance specifying the regulations to be followed in the audit, such as in particular obligations of confidentiality, the plan of the audit, the right to comment etc. Unless a shorter period is required for legal reasons or because of instructions from the supervisory authority or conformity assessment body, the audit must be announced at least 60 calendar days in advance. An audit can also include a security audit of the subscriber system that is linked to the AIS service. In consultation with the security officer, it must be also be possible to conduct penetration tests or vulnerability scans on the affected system.

The contact person for audits of the Subscriber is one of the contacts named in the declaration of configuration and acceptance above. They make sure that a deputy is appointed. The annual charge for

reviewing the subscriber application and any possible external registration office can be found in the price list. The Subscriber shall bear their own costs.

The subscriber is obliged to rectify any defects identified in the audit.

7 Liability

The liability of both parties is based on this contract. In this case, the liability of Swisscom towards the Subscriber for damages in connection with providing the certification service in accordance with this configuration and acceptance declaration for simple negligence is excluded to the extent permitted by law.

8 Power of attorney and declaration of acceptance

As part of this declaration of configuration and acceptance, the Subscriber of Swisscom confirms, that

- it has declared that all the configuration parameters mentioned above are correct and Swisscom is entrusted with activating the service.
- In case the subscriber is not the seal creator it is contractually authorized by the seal creator to create the seals for the seal creator

Additionally, the Subscriber authorises the contact persons named under Section 5 for all information relating to the security of the connection and the access to Swisscom.

9 Special project-specific information

Other information and configurations which have not been mentioned above can be described here if necessary:

10 Submission

This declaration of configuration and acceptance will be submitted in advance by e-mail to the following address:

Msc.support@swisscom.com

You can then either sign this completed declaration in Swisscom's digital signature room with a qualified signature in accordance with ZertES or sign it by hand and send it by post to the following address:

Swisscom (Schweiz) AG
Enterprise Customers
Identification Services / Sales Support
Pfingstweidstrasse 51
8005 Zürich
Switzerland

PAY ATTENTION
Please have a look to the following tick boxes:
Please confirm: only address the ClaimedID of the seal creator (cf. 3.2)!
Subscriber application must be protected! (cf 4)!
Prevent compromise by admins! (cf 4)

☐ The signatories are identified for the qualified signature in accordance with the Swiss Signature Act and would like to sign the contract electronically in Swisscom's SwissTrustRoom.

11 Signatures

send/e-mail

Please send the form using the button on the right before signing, so that Swisscom can already check the data and prepare the setup: Swisscom requires the document to be signed by hand and filed in by regular mail or with a qualified signature in accordance with the Swiss Signature Act (ZertES).

Place, date

First name and surname
Title

First name and surname
Title

Signature(s)