



# Order by Swisscom Partner

All-In Signing Service Personal Signatures 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	<b>Purpose of the document</b> .....	3
2	<b>Characteristics of the service for the end customer</b> .....	3
2.1	Quality of signature, legal area (CH, EU) and accounting methods .....	3
2.2	Registration of new signers .....	4
3	<b>Information on the RA agency contract / RA delegation contract</b> .....	4
4	<b>Contact person of the customer for this order</b> .....	4
5	<b>Contact person for Swisscom Roll-Out and Support</b> .....	5
6	<b>Activation of the service</b> .....	5
7	<b>Payment due</b> .....	5
7.1	Service fee, connection prices and audit costs .....	5
7.2	Invoicing of the provision price, connection prices and audit costs .....	6
7.3	Current usage prices .....	7
7.4	Invoicing of the current usage prices .....	8
7.5	Use of multiple Service Access Internet Points .....	8
7.6	Price list glossary .....	8
8	<b>Submission</b> .....	8
9	<b>Special project-specific information</b> .....	9

# 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 "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 or qualified signature. The end customer is the following organization (details in the attached configuration and acceptance declaration):

Company name /  
 organisation name

Postcode/Town

country

- Signed configuration and acceptance declaration of the end customer is attached.
- Signed configuration and acceptance declaration of the end customer will be submitted later

# 2 Characteristics of the service for the end customer

## 2.1 Quality of signature, legal area (CH, EU) and accounting methods

Each characteristic requires a ClaimedID!	Billing per signature		Billing per signer	
	CH	EU	CH	EU
Advanced electronic signature incl. time stamp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Qualified electronic signature incl. time stamp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The offered service is based on the following service description:

- ["All-in Signing Service description for personal signatures in Switzerland" of May 1st, 2020](#)

- ["All-in Signing Service description for personal signatures in the EU" of May 1<sup>st</sup>, 2020](#)
- [Swisscom Service base documents:](#)
  - ["Information Security" of April 1<sup>st</sup>, 2019](#)
  - ["Service Glossary" of April 1<sup>st</sup>, 2019](#)
  - ["Service Management Processes" of April 1<sup>st</sup>, 2019](#)
  - ["SLA - Definitions" of April 1<sup>st</sup>, 2019](#)

**2.2 Registration of new signers**

- A. The standard procedure according to service description is used for qualified and advanced signatures: the identification and registration of new signers is handled with the RA App or Smart Registration Service provided by Swisscom. The authentication is either based on MobileID (for swiss signatures), MobileID App or PWD/OTP (for swiss or EU signatures).
- B. A separate identification method is used and an implementation concept accepted by Swisscom is applied.
- C. A separate signature confirmation procedure is used and an implementation concept accepted by Swisscom is applied.

**3 Information on the RA agency contract / RA delegation contract**

Required <a href="#">RA-Agency contract</a> cf. 2.3	Required RA Delegation Contract cf. 2.3
(NA) already concluded	(NA) already concluded
(NA) attached to this order	(NA) attached to this order
(NA) will be submitted later	(NA) will be submitted later
(NA) no contract will be concluded (use of Smart Registration Service)	

**4 Contact person of the customer and 1<sup>st</sup> level support contact**

- according to partner contract

First name \_\_\_\_\_

Name \_\_\_\_\_

Language \_\_\_\_\_

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
- 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

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

**Deployment, service fee and audit using the standard identity verification process (RA App)**

Number	benefits	remark	prices annually	one-off price	Total
Nbr:	Annual service fee per service interface (Claimed Identity = SAIP)	Annual invoicing, for the first time in the month after conclusion of the contract	2'400.00		
	Audit expenses per service interface (SAIP)	Audit based on identification by RA App or Smart Registration Service	inclusive		
		Special audit expenses due to non-compliance with cooperation duties.	Charged by effort		

The RA App can be used for identification purposes free of charge.

**Option: additional price for project-specific methods for identity verification**

A project-specific identification procedure is only offered in connection with an additional signed consulting contract "Signature Onboarding once per procedure. In addition to the one-off costs mentioned therein, the following annual charges are due for each end customer. If no "Signature onboarding" contract comes into effect, the one-time price is due in any case.

Benefits	Remarks	Prices annually	One-off price
Additional audit expenses per registry	Audit with own registration authority	5000.00	
	Further audit expenditure in the event of non-compliance with cooperation duties	Charged by effort	

**Option: additional price for project-specific procedures for signature authentication**

A project-specific procedure for signature authentication is only offered in connection with an additional signed consulting contract "Signature Onboarding once per procedure. In addition to the one-off costs mentioned therein, the following annual charges are due for each end customer. If no "Signature onboarding" contract comes into effect, the one-time price is due in any case.

Benefits	Remarks	Prices annually	One-off price
Additional audit costs per procedure	Audit with specific signature authentication method	5000.00	
	Further audit expenditure in the event of non-compliance with cooperation duties	Charged by effort	

**7.2 Invoicing of the provision price, connection prices and audit costs**

The service fee and optional audit costs are invoiced annually, for the first time in the first month after activation of the service.

Optional one-off prices will be invoiced after confirmation of this order. The annual service fees will be invoiced at the beginning of each contract year. The price resulting from the exercise of the right of inspection and control at Swisscom or by third parties commissioned by Swisscom is included in the price list above, unless the result of the inspection justifies a price being charged by the customer, as his end customer has not fulfilled his cooperation obligations.

Any additional audit costs incurred by third parties in the event of non-compliance with cooperation services will be invoiced annually by Swisscom or third parties on the basis of the audit expenditure actually incurred.

All refunds in the event of premature termination of the contract are excluded.

### 7.3 Current usage prices

One Claimed Identity (Service Access Internet Point) is required for each billing procedure (per signature/per signer performed).

#### Price per signature performed (volume-dependent)

The volume consumed for the respective contract month is decisive. The price per signature falls when crossing from one volume band to the next for the following signatures.

Service	Volume band: Signatures per year via a Service Access Internet Point			Price per signature
Advanced electronic signature (FES) with qualified time stamp, legal area CH	1	-	50'000	
	50'001	-	200'000	
	200'001	-	1'000'000	
	more			
Qualified Electronic Signature (QES) with qualified time stamp, legal area CH	1	-	50'000	
	50'001	-	200'000	
	200'001	-	1'000'000	
	more			
Advanced electronic signature (FES) with time stamp, legal area EU	1	-	50'000	
	50'001	-	200'000	
	200'001	-	1'000'000	
	more			
Qualified electronic signature (QES) with time stamp, legal area EU	1	-	50'000	
	50'001	-	200'000	
	200'001	-	1'000'000	
	more			

#### Alternative model: Price per signer (flat rate)

The triggering of a signature by a signer in the contract month is decisive. A signer is identified by its name in the signature certificate (technically "Distinguished Name", e.g. "CN=Hans Mustermann, C=CH, serialNumber=<unique number>"). All subsequent signatures in the relevant month (hereinafter "contract month") are included in the price for this signatory (monthly flat price).

Service	Calculation	Price per month
Advanced Electronic Signature (FES) with qualified time stamp, Switzerland legal area	Per signing party and contract month per service interface (SAIP)	
Qualified Electronic Signature (QES) with qualified time stamp, legal area Switzerland	Per signing party and contract month per service interface (SAIP)	
Advanced electronic signature (FES) with time stamp, legal area EU	Per signing party and contract month per service interface (SAIP)	
Qualified electronic signature (QES) with time stamp, legal area EU	Per signing party and contract month per service interface (SAIP)	

**7.4 Invoicing of the current usage prices**

The current usage prices are invoiced at the end of the month. Depending on the usage price model selected at the start of this order, the service invoice contains the number of signatures performed per month or the active signatories. A separate invoice is issued for each SAIP, i.e. each billing procedure performed for the user charges or each signature type.

All refunds in the event of premature termination of the contract are excluded.

**7.5 Use of multiple Service Access Internet Points**

Volume bands or signatures are applied per Service Access Internet Point. Volumes cannot be accumulated across multiple Service Access Internet Points. If several separate Service Access Internet Points have to be supplied with remote signatures, all current usage prices are reduced by a further 30%. For resellers with a partner contract, several SAIPs are generally assumed for the various end customers. Amounts are rounded up to the nearest cent. The reduction of 30% is already taken into account in the 7.3 pricing.

**7.6 Price list glossary**

AIS Service	All-In Signing Service provided by Swisscom up to the SAIP.
Distinguished Name	Standardized form for the description of a certificate subject.
NA, (NA)	Not applicable option
RA	Registration Authority, responsible for the identification of the signatories. Can be provided by the end customer, Swisscom or third parties on condition of a contractual relationship with Swisscom.
SAIP = Service Access Internet Point	The Service Access Interface Point (SAIP) is the contractually agreed, logical point at which the service is provided and monitored for the customer and the service levels provided are identified. It is the communication point for a ClaimedID with the subscriber application

**8 Submission**

Order date:

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

[msc.support@swisscom.com](mailto: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:



**swisscom**

# Configuration and acceptance declaration

All-In Signing Service for personal signatures  
in Switzerland and EU

Contract no.

Swisscom Partner:

By:

**Regarding:**

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

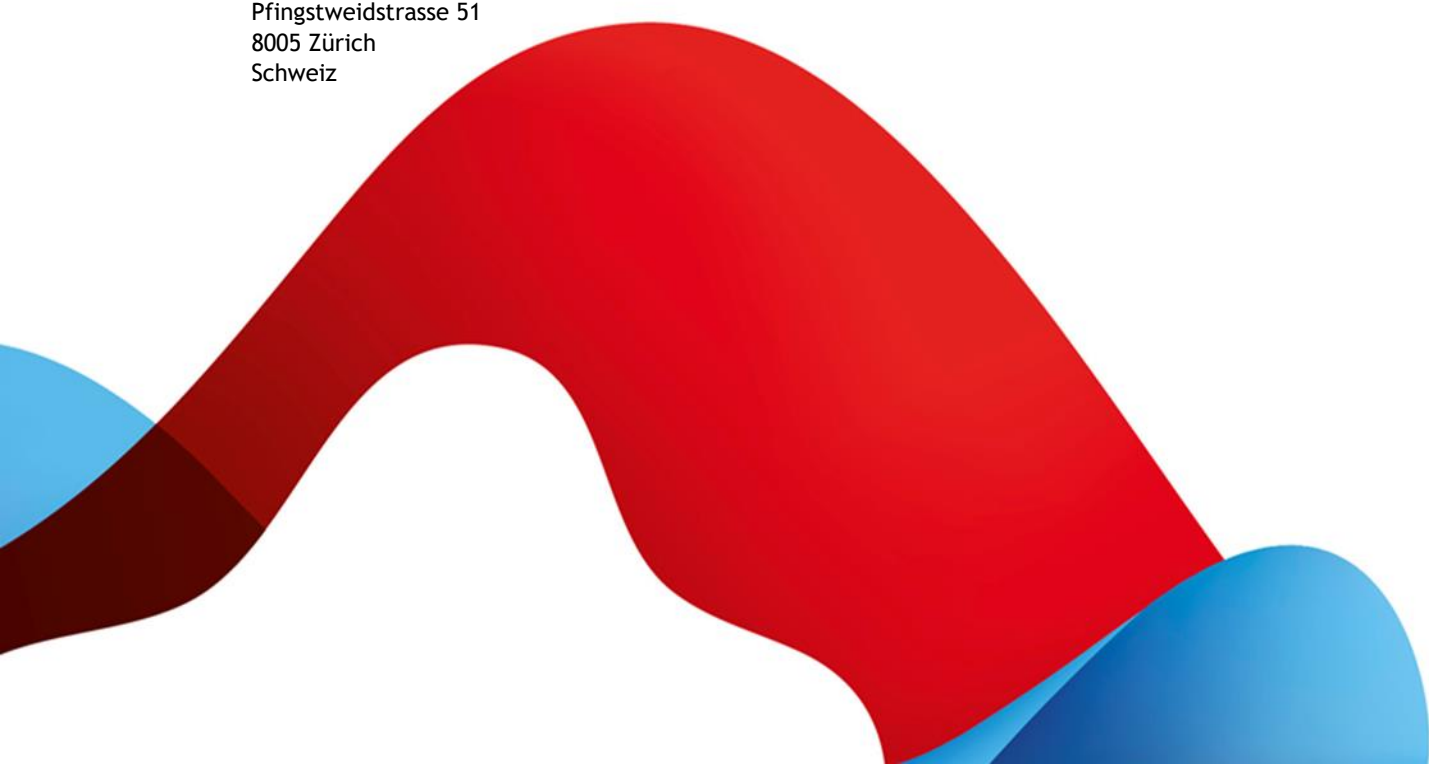
hereinafter referred to as "Subscriber"

hereinafter referred to as "Swisscom"

Postal address

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

Please use Adobe Acrobat  
to fill out this form!



## Table of Content

1	<b>Purpose of the document</b> .....	3
2	<b>Information on the contract</b> .....	3
2.1	Signature quality, jurisdiction (CH, EU), invoicing (per signature or signatory) - as mentioned in the contract .....	3
2.2	Client software used .....	3
2.3	Requesting a signature by authentication and declaration of intent .....	3
2.4	Signature approval method .....	4
2.5	Contents of the signature: Signature certificate .....	4
2.5.1	Signature certificates based on RA-App identification .....	4
2.5.2	Contents of the signature certificate in connection with the implementation concept .....	4
2.6	SSL access certificate and protection of the AIS service .....	4
2.7	Operation of the subscriber application .....	5
3	<b>Contact details of the Subscriber</b> .....	5
3.1	Address of the Subscriber .....	5
3.2	Support .....	6
3.3	First responsible in charge .....	6
3.4	Second person in charge .....	7
4	<b>Swisscom right of audit</b> .....	7
5	<b>Liability</b> .....	8
6	<b>Power of attorney and declaration of acceptance</b> .....	8
7	<b>Special project-specific information</b> .....	8
8	<b>Submission</b> .....	9
9	<b>Signatures</b> .....	9

## 1 Purpose 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 signatures mentioned in the eIDAS Regulation of the EU (eIDAS Regulation) 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 signatories who intend to use an advanced or qualified signature.

First, this statement serves as an overview of the desired service specification and of the responsible contact persons based on the general service description AIS for integrating the subscriber application in the All-in Signing Service.

Secondly, the subscriber confirms that the appointed persons in charge have read the underlying service description for the corresponding Swiss or EU AIS service for personal signatures and follow the duties described in this declaration. The All-in Signing Service can only be configured after the information has been received in full.

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), invoicing (per signature or signatory) - as mentioned in the contract

Each characteristic of the service requires a ClaimedID!	Invoicing per signature		Invoicing per signatory	
	CH	EU	CH	EU
Advanced electronic signature including time stamp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Qualified electronic signature including time stamp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### 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):

---

### 2.3 Requesting a signature by authentication and declaration of intent

Please confirm:

- A. On request, the signatory receives the document to be signed displayed in full and downloadable before the declaration of intent requesting a signature and after signature, and therefore can be sure that this specific document is signed. This is an obliged requirement!
- B. The signatory is informed before or during the expression of will that the signature is either an "advanced" or "qualified" signature. This is an obliged requirement!

The subscriber acknowledges that a signature can only be executed after acceptance of the terms of use. These are transmitted to the signatory after identification via RA app or via Smart Registration Service in the context of an SMS or in the context of the video identification process or according to the description in the implementation concept. This relates to the current and applicable versions of the terms of use, which can be downloaded from [https://www.swisscom.ch/en/business/enterprise/offer/security/digital\\_certificate\\_service.html](https://www.swisscom.ch/en/business/enterprise/offer/security/digital_certificate_service.html) under the column “Switzerland (CH)” for the service in Switzerland or “Europa (EU)” for the service in the EU.

**2.4 Signature approval method**

Swisscom will use MobileID with a fallback solution to PWD/OTP for all signatures in the Swiss legal area. Exclusively PWD/OTP or MobileID App will be used as standard for qualified signatures outside Switzerland. OTP will be used as standard for advanced signatures outside Switzerland.

(NA) Only OTP should also be used for advanced signatures in the Swiss legal area instead of MobileID.

Other signature approval method should be used according to the implementation concept.

**2.5 Contents of the signature: Signature certificate**

The Subscriber must ensure regarding the cn that the name is presented in a way that is suitable and understandable to the holder of the certificate considers to be user-friendly or system-friendly. This is generally the first name and surname or a nickname. Nicknames have to be marked in the cn as "PSEUDONYM"!

**2.5.1 Signature certificates based on RA-App identification**

Provided that a standard identification procedure is used in accordance with Section 3.2.2 of the service description (RA app), the distinguished name in the signature certificate is as follows:

A. (NA)	cn= <First name, surname of the signatory> or PSEUDONYM:<other information relating to the customer> pseudonym= <Mobile number in international format or evidenceID (see below)> c= <Country of residence or citizenship of the signatory> serialnumber= <evidenceID of the RA service after verify call>
B. (NA)	cn= <First name, surname of the signatory> givenname= <First name(s) as per ID document> surname= <Surname(s) as per ID document> c= <Country of residence or citizenship of the signatory as per ID document> serialnumber= <evidenceID of the RA service after verify call>

A

**2.5.2 Contents of the signature certificate in connection with the implementation concept**

(NA)	The signature certificate is described in the implementation concept.
------	---

**2.6 SSL access certificate and protection of the AIS service**

For each connection to the AIS service (via https), 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>
- Email=<Email contact for this certificate>
- C=<country of the organisation>

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

The certificate must be renewed by the subscriber without prior request before the end of validity of 3 years. If this does not happen, no signature can be issued until renewal!

- A. The certificate has already been created and is submitted at the same time as this statement.
- B. The certificate will be forwarded to [msc.support@swisscom.com](mailto:msc.support@swisscom.com) with respect to this order.
- C. 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.
- D. The private keys of the SSL certificate are stored on external data carriers, which are kept in a secured place.
- E. The private keys of the SSL certificate are managed autonomously through the subscriber application and are not accessible by the administrator.

**2.7 Operation of the subscriber application**

- A. The subscriber application is protected against any unauthorized 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.  
  
===== OR =====
- C. The subscriber application is an application of a third party supplier and the subscriber has no admin rights. The access by administrators of the third party supplier is controlled in such a way that they cannot perform manipulations or the access of these administrators is completely prevented. The protection concept in this regard can be proven to Swisscom at any time upon request.

If an implementation concept is required, further operating conditions have been specified in this concept. Statement A and B or C must be accepted!

### 3 Contact details of the Subscriber

**3.1 Address of the Subscriber**

Name of company /  
organisation

Company ID (BIN)

Address

Postcode,  
town/city

Country

**3.2 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

---

**3.3 First responsible in charge**

At least two persons in charge must be designated

- Role according implementation concept
- System administrator
  - Security officer (including data protection)
  - (NA) Training officer

First name

---

Surname

---

Language

---

Organisation  
(if different)

---

Address  
(if different)

---

Phone number

---

Mobile

---

E-mail

---

Hierarchy level (head of the organisation, for example, CEO is hierarchy level 1)

---

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.

**3.4 Second person in charge**

- Role according implementation concept
- System administrator
  - Security officer (including data protection)
  - (NA) Training officer

\_\_\_\_\_

First name

\_\_\_\_\_

Surname

\_\_\_\_\_

Language

\_\_\_\_\_

Organisation  
(if different)

\_\_\_\_\_

Address  
(if different)

\_\_\_\_\_

Phone number

\_\_\_\_\_

mobile

\_\_\_\_\_

E-mail

\_\_\_\_\_

Hierarchy level (head of the organisation, for example, CEO is hierarchy level 1)

\_\_\_\_\_

This person should \*)

- Receive error messages and important technical information (Role "notificator")
- Receive service announcements (Role "maintenance")

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

\*) 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.

## 4 Swisscom right of audit

Swisscom is authorized 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 authorized 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.

## 5 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.

## 6 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.

Additionally, the Subscriber authorises the contact persons named under Section 3 for all information relating to the security of the connection and the content of the certificate. It also authorizes these persons named under Section 3 to provide information about any questions regarding the activity of the registration authorities for or either its own registration authority or that of a third party.

## 7 Special project-specific information

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



## 8 Submission

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

[msc.support@swisscom.com](mailto: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  
Pfungstweidstrasse 51  
8005 Zürich  
Switzerland

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.

## 9 Signatures

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)