SwissSign

PLEASE USE THE ADOBE ACROBAT READER TO FILL OUT THIS DOCUMENT!

Declaration of Consent to the Delegation of Registration Authority Activity

(hereafter: Declaration of Consent RA Delegation)

(For details of organisation name and address, refer to the proof of organisation)

Official company name

Company short name

(if company name contains more than 64 characters, including spaces)

Domicile address
(street address)

Postcode,
Locality (Registered Office)

Country

Facilitated by the following SwissSign Partner ("Specialist Retailer")

SwissSign partner's
email address

New Agreement ☐

Amendment
of existing Agreement ◉

☐ Certificates for this organisation will be requested via already existing Managed PKI of the following organization:

Official company name
of the already existing
Managed PKI

SwissSign

1. Whereas

SwissSign is an accredited Certification Authority pursuant to the Swiss Federal Act concerning certification services in the area of electronic signatures (the Swiss Federal Electronic Signatures Act, ZertES), and an accredited provider of signatures in Liechtenstein under the eIDAS, and is recognised as such by numerous software- and operating systems manufacturers.

Certification Authorities have the task of identifying applicants for certificates. This role is referred to as the Registration Authority, or abbreviated to "RA" (Registration Authority).

According to national statutory provisions and international regulations, e.g.

- the ZertES in Switzerland
- the eIDAS Regulation in the EU
- international ETSI standards
- CA Browser Forum guidelines

recognised Certification Authorities may delegate to a third party their task of identifying an applicant.

Under a Managed PKI order, the external Registration Authority assumes the role of a limited or fully comprehensive Registration Authority (abbreviated to "RA") for requests for and approvals of certificates either directly or through a SwissSign partner or under the terms of any other contractual agreement.

Under the Managed PKI, unless agreed otherwise in this document, the Registration Authority shall be limited as follows by SwissSign for all publicly trusted certificates: the organisation and its address shall be reviewed according to the entry in the Commercial Registry or the proof of organisation of SwissSign and configured without amendment for the Registration Authority. All of the main domains indicated by the Registration Authority shall also be reviewed and unchangeably configured for the Registration Authority. Further subject entries in publicly not trusted certificates (e.g. names of people) will normally not be filtered further or reviewed by SwissSign and must be reviewed by the Registration Authority. The Registration Authority must review entries relating to people or sub-organisations or sub-domains for all publicly trusted certificates under the Managed PKI. In special cases and those not falling under a Managed PKI contract, the registration authority activity may also be expanded to the review of email addresses, domains and organisations. Should this occur, these entries shall not be configured without amendment.

SwissSign intends, in the context of the issuance of certificates, to allow verification of the identity of the applicants by Registration Authorities within the meaning of the aforementioned jurisprudence and regulations to be carried out by carefully selected and monitored organisations and expects in relation to this Declaration of Consent that the obligations indicated will be approved of.

2. Other applicable documents

The following documents, in the following descending order of priority, form an integral part of this Declaration of Consent:

- This Declaration of Consent duly completed and signed
- The guidelines on the delegation of registration authority activity: http://repository.swisssign.com/RA_Delegation.pdf
- Subscriber Terms and Conditions Certificate Services: http://repository.swisssign.com/SubscriberAgreement.pdf
- Configuration of the Registration Authority under a Managed PKI (Annex 1), where available
- Project-specific CP/CPS (Annex 3) where available

- General CP/CPS:

  SwissSign Silver CP/CPS (latest version) at:

  https://repository.swisssign.com/SwissSign-Silver-CP-CPS.pdf. Applies only where Silver certificates are being purchased.

  SwissSign Gold CP/CPS (latest version) at:

  https://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf. Applies only where Gold certificates are being purchased.

  SwissSign Platinum CP/CPS (latest version) at:

  http://repository.swisssign.com/SwissSign-Platinum-CP-CPS.pdf. Applies only where Platinum level qualified certificates are being purchased.

The relevant amended version of the SwissSign CP/CPS and the Subscription Agreement Certification Services shall be published on the website https://www.swisssign.com/support/repository.html in good time before it comes into effect and shall be notified through the system status page: https://www.swisssign.com/support/systemstatus.html. These documents are subject to supervision by the auditors of SwissSign and cannot be substantively amended. They must be adjusted on an ongoing basis in line with regulations and standards applicable to certification authorities. Alerts concerning substantive changes to the system status page may be subscribed to on that page. They shall be deemed to be approved unless the REGISTRATION AUTHORITY SUBSCRIBER objects in writing thereto within one month of their adoption. An objection shall be deemed to constitute notice of ordinary termination of the relevant agreements. A new version of the guidelines on the delegation of registration authority activity must be approved and accepted under all circumstances in writing by a renewal of this Declaration of Consent.

Section 9 of the Registration Authority Subscriber Agreement Section shall apply to changes in the project-specific CP/CPS. General Terms and Conditions of Business of the Registration Authority organisation shall not apply.

SwissSign

3. Declaration of Consent to the registration process for non-qualified publicly trusted certificates

For all non-qualified and publicly trusted certificates, the Registration Authority shall verify the identity and, if applicable, the specific attributes of a certificate subject. The basic certificate issuance process under this Agreement is configured as follows:

The certificate is issued for the following subjects (more than one answer is possible):

- ☐ **A)** Full-time and part-time employees (for personal certificates)
- ☐ **B)** Subcontractors and consultants (for personal certificates)
- ☐ **C)** Machines, equipment and (web) servers (for SSL/codesigning certificates)
- ☐ **D)** Others:

In all cases, the Registration Authority warrants that it is able to check or arrange for the checking of the registration and of all documents pertaining thereto in accordance with the aforementioned rules. All persons who receive certificates are personally known to the organization in the case of e-mail Gold ID certificates.

SwissSign

4. Appointment of access managers for the registration authority activity

The Registration Authority may arrange for the tasks that are required in the context of certificate application, approval and administration to be performed by the following undersigned persons to whom it hereby grants power of representation for the registration authority activity (said power being limited to performance of the said tasks). They are not authorised to act as a representative in any additional way, and they are specifically not authorised to amend this Agreement. For the registration authority activity, said persons shall be given access for the purpose of approving a certificate application. The persons indicated are each entitled to sign alone and to release certificates in accordance with the registration process in section 3.

Access manager 1 as authorised representative for the registration authority activity:

First name, last name

Company name

Email address

Telephone

Position

Signature *)

☐ Copy of ID) (front and back)/passport is enclosed *)

Access manager 2 as authorised representative for the registration authority activity:

First name, last name

Company name

Email address

Telephone

Position

Signature *)

☐ Copy of ID (front and back)/passport is enclosed. *)

*) The copy of ID/passport is only necessary if SwissSign did not already vet the person. A signature by the access responsible is necessary in any case.

SwissSign

Access manager 3 as authorised representative for the registration authority activity:

First name, last name	
Company name	
Email address	
Telephone	
Position	
Signature *)	

☐ Copy of ID (front and back)/passport is enclosed. *)

*) The copy of ID/passport is only necessary if SwissSign did not already vet the person. A signature by the access responsible is necessary in any case.

SwissSign

5. Approval in relation to Managed PKI (please deactivate check box if not applicable)

The power of representation of the access managers for the registration authority activity according to Section 4 includes in addition without any further specific review the authorisation of the registration and publication of all certificates for the following organisations, which shall be identical to the entry in the Commercial Registry or to the proof or organisation. The name of the organisation may also be published in the publicly trusted certificate, where envisaged in the certificate. The above is subject to the proviso that certain other entries in the publicly trusted certificate which do not concern the organisation may have to be authorised (e.g. domains, names of individuals) by the Registration Authority.

Usage of the certificates issued under a Managed PKI after the commercial agreement with SwissSign or the Specialist Retailer has ended shall not be permitted. All still valid certificates must be revoked by the Registration Authority or upon payment of a fee by SWISSSIGN.

If a Specialist Retailer's contract is terminated, SwissSign shall be authorised to inform the Managed PKI Customers of the termination and, if so requested, to take the appropriate steps to ensure that the service can continue to be provided.

Organisation:

Street address of the registered office of the Registration Authority organisation:

Registered office of the Registration Authority organisation (post code, locality):

Registered office of the Registration Authority organisation (country):

6. Approval and Declaration of Consent

The Registration Authority hereby states its consent to the RA Delegation Guidelines and the Subscriber Terms and Conditions Certificate Services. It further acknowledges that SwissSign will issue certificates based on the requests for certificates approved by it.

The Registration Authority hereby confirms the accuracy of all configuration parameters for registration authority activity specified in Annex 1 and charges SwissSign with their implementation.

The Registration Authority shall inform SwissSign in writing by using the change form in case of any changes in the access managers.

SwissSign

7. Signatures

The authorised signatories of the Registration Authority as specified in the proof of organisation shall sign on behalf of the Registration Authority organisation:

Locality

Date

Signature of authorised signatory 1

Where applicable, signature of authorised signatory 2

Last name, first name, position in block capitals

Last name, first name, position in block capitals

Email

Telephone

☐ Copy of ID/passport is enclosed

Email

Telephone

☐ Copy of ID/passport is enclosed

SwissSign

Notes and comments concerning the vetting process for this Declaration of Consent

Please ensure that, in cases involving a Managed PKI, the Managed PKI order was placed directly or via the Specialist Retailer.

The vetting process will take less time if

- All persons signing this Declaration of Consent (access manager and representatives of the organisation) enclose a copy of their ID/passport or sign by SuisseID digitally.
- Those responsible for the Registration Authority organisation as stated in the Commercial Registry or official proof of organisation shall sign.

As far as the representatives of the organisation cannot be found in the Commercial Registry or proof of organisation, we shall also contact your HR organization or the representative of your organisation as stated in the Commercial Registry or proof of organisation in order to verify authority to sign this Contract. Please account for several additional days or weeks of processing time, depending upon the availability of the people who are to be contacted. Please speed up the domain authority check by keeping up to date the whois database with the name of your own domains and organisation. Requests covering more than 10 domains should be subject to an automated domain review (swisssign-check procedure, email or DNS entry). Please note that our experience shows that verification via telephone, in particular for the representatives of an organisation, can take several weeks due to difficultly in accessing these persons. If copies of ID, any domain entries in whois in Annex I (or alternatively swisssign-check/DNS entries) and signatures of registered representatives of the organisation are available, the review and the setup will only take a couple of days.

Checklist and return
Before returning the declaration of consent, please check the following checklist:

- ☐ Did you prepare a declaration per additional organization to be covered by this Managed PKI?
- ☐ Did you fill out the Registration Authority process? (Section 3)
- ☐ Have the right access managers signed? (Section 4)
- ☐ Did you enclose copies of the IDs/passports of all access managers signing? (Section 4)
- ☐ Are those signing the Contract authorised to sign and can this be corroborated by the Commercial Registry extract? (Section 7)
- ☐ Did you enclose copies of the IDs/passports of all persons signing the Contract? (Section 7)
- ☐ Are you sending the original hard copy of the document by post?
- ☐ Sign up for the RSS notification feed through system status reports (recommended)

Please hand over this document to the Specialist Retailer who sold you the Managed PKI solution. If there is a direct commercial agreement with SwissSign, send the document by ordinary mail to:

SwissSign AG
Sales & Partner Management
Sägereistrasse 25
8152 Glattbrugg
Switzerland

If not already done the associated commercial order must be transmitted directly or via the reseller electronically to **contracts@swisssign.com** or also by ordinary mail to the above address. SwissSign will confirm the receipt of the Setup Agreement and contract by email.

SwissSign

Annex 1 to the Subscriber Terms and Conditions Registration Authority

The Registration Authority shall be configured as follows:

1. General email address for notices from the Registration Authority

As part of the registration authority activity, the persons who have access authorisation shall receive emails, for example, concerning the status of the certificates. SwissSign shall send these emails to the following general email address of the Registration Authority, e.g. it-info@example.com:

2. Pre-existing account with SwissSign

The REGISTRATION AUTHORITY SUBSCRIBER already has an existing account on the certificate management platform "swisssign.net", which it would like to continue to use. The existing account is:

3. Publication of the certificates by SwissSign

- (●) The REGISTRATION AUTHORITY SUBSCRIBER wishes to publish its certificates in the general directory of www.swisssign.net (LDAP), so that everyone can look up the certificates and everyone can communicate with it using public key encryption.
- ( ) The REGISTRATION AUTHORITY SUBSCRIBER does not wish to publish its certificates.

4. SSL certificates Extended Validation (EV) to be set up

- ☐ **SSL Gold EV**, extended organisation validated, <domain>, www.<domain>
- ☐ **SSL Gold EV multi-domain**, extended organisation validated, up to 200 domain entries.

5. SSL certificates Organisation Validation (OV) to be set up

- ☐ **SSL Gold**, organisation validated, <domain>, www.<domain>
- ☐ **SSL Gold Multi-Domain**, organisation validated, up to 200 domain entries.
- ☐ **SSL Gold Wildcard,** organisation validated, all sub-domains (without main domains)**.**

6. SSL certificates Domain Validation (DV) to be set up

- ☐ **SSL Silver**, key usage "client/server authentication", domain validated, <domain>, www.<domain>
- ☐ **SSL Silver Wildcard**, domain validated, all sub-domains (without main domain).

SwissSign

7. Domains to be set up for publicly trusted SSL certificates

Enter the domains in portal swisssign.net with appropriate user account as the person responsible for access in the menu «MPKI domains» and prove the access by changing a file in the domain or a change in the DNS entry.

You hereby warrant that in the DNS entries (CAA) of the specified domains either SwissSign is registered as the issuing certification authority or there are no restrictions regarding the issuing certification authorities. Details on the necessary entries can be found at https://sslmate.com/caa/. You ensure that, during the term of your managed PKI contract, you do not introduce any restrictions on SwissSign as the issuing certification authority for these domains in the DNS record

8. E-Mail certificates to be submitted

Email ID Silver (corresponds to class 1) for signature and encryption

- ☐ **Email ID Silver,** email address validated (Web GUI and partner application)
- ☐ **Email ID Silver,** email address validated, organisation, country (partner application only)
- ☐ **E-Mail ID Silver,** email address validated, organisation, canton/federal state, country (partner application only)

Email ID Gold (corresponds to class 2/3)

- ☐ **Email ID Gold,** email address and organisation validated, first name/last name, email address, organisation, province, country validated for **signature, authentication and encryption** (Web GUI and partner application)
- ☐ **Email ID Gold,** email address and organisation validated, first name/last name, email address, organisation, canton/federal state/province, country validated only for **signature and encryption**, "Office Management certificate" (Web GUI and partner application)
- ☐ **Email** certificate based on the signature procedure RSASAA-PSS (connforming to Edi@Energy)

9. It should be possible to acquire email certificates by ...

- ☐ **... web interface** (access by access certificate for the certificate platform), request and issuance manually through web interface.
- ☐ **... automatic interface (CMC)**, here the following partner solution will be used:

NB: When using Silver email certificates on the partner solution mentioned above the certificate in the OU field additionally has the following entry:

- NA -

SwissSign

10. Domains to be set up for publicly trusted E-Mail certificates

Enter the domains in portal swisssign.net with appropriate user account as the person responsible for access in the menu «MPKI domains» and prove the access by changing a file in the domain or a change in the DNS entry.

You hereby warrant that in the DNS entries (CAA) of the specified domains either SwissSign is registered as the issuing certification authority or there are no restrictions regarding the issuing certification authorities. Details on the necessary entries can be found at https://sslmate.com/caa/. You ensure that, during the term of your managed PKI contract, you do not introduce any restrictions on SwissSign as the issuing certification authority for these domains in the DNS record

11. Codesigning certificates to be set up (Currently not orderable)

☐ Codesigning certificate incl. up to 10 stamps per day. The registration authority confirms having generated the private/public key pair on a HSM or smartcard conforming to FIPS level 140-2 level 2 or Common Criteria EAL4+ and that the keys will be kept on this device.

The following list shows the admitted devices and services:

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Please attach a photo of your HSM showing the type plate in detail and enter the following HSM data:

Supplier or Service Provider (e.g. in case of cloud service):	
Device or service type:	
Device ID or service contract ID:	

12. Private certificates not publicly trusted

☐ **Private certificates not trusted** for internal use e.g. as device certificate or internal authentication as specified in paragraph 14.

13. Notification concerning end of validity of a certificate

○ **No notification at all,** since e.g. the client system is for auto-enrolment or mailgateway will take over notifications or renewals

○ **Notification only to the access managers,** but no notification to the certificate owner, 10 and 30 days before end of validity of the certificate.

◉ **Certificate owners and access managers will be notified,** 10 and 30 days before end of validity.

The access manager shall be always informed via the e-mail account which is configured in the Registration Authority account. If notification is to be regulated otherwise for particular certificate types, please state this in the "comments" field.

SwissSign

14. Special project-specific types of certificate or other comments

☐ Project-specific certificates have been agreed to when setting up this Registration Authority or other agreements have been reached.

Please specify characteristics precisely or leave the field blank:

To be filled in by SwissSign:

For project-specifically agreed certificate types, the stamp and signature of the product management is required after submission of this declaration of consent.

Date:	
Stamp, Signature	