Guidelines on the delegation of registration authority activity (hereafter RA Delegation Policy)

Version: 1.0

OID: 2.16.756.1.89.1.0.7.0.1

NB: The organisation performing registration authority activity is obliged to inform its access managers concerning this Policy and to require compliance with it.

This document is subject to the SwissSign audit as an accredited certification authority and may not be altered, invalidated or amended by any side agreements.
## Approval and versions

<table>
<thead>
<tr>
<th>Author</th>
<th>Date</th>
<th>Version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingolf Rauh</td>
<td>2017-07-14</td>
<td>1.0</td>
<td>Creation</td>
</tr>
</tbody>
</table>

## Approval by

<table>
<thead>
<tr>
<th>SwissSign authorised signatory</th>
<th>Digital signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reinhard Dietrich (CISO)</td>
<td></td>
</tr>
<tr>
<td>SwissSign AG</td>
<td>Reinhard Armand Dietrich</td>
</tr>
<tr>
<td>Markus Naef (CEO)</td>
<td></td>
</tr>
<tr>
<td>SwissSign AG</td>
<td>Markus Naef</td>
</tr>
</tbody>
</table>
## Table of contents

1. Definition.................................................................................................................................................... 4
2. Contractual object................................................................................................................................... 4
3. Service Description Registration Authority........................................................................................ 4
4. Duties of the RA and restrictions relating to registration authority activity................................ 5
5. Duty to provide information of both Parties ...................................................................................... 6
6. Additional Special Regulations concerning registration activity for special types of certificate................................................................................................................................................... 6
7. Prerequisites for exercise....................................................................................................................... 6
8. Duties of the RA when dealing with certificates.................................................................................. 7
8.1 Compliance with the Subscriber Agreement Certificate Services...................................................... 7
8.2 Protection of the Registration Authority............................................................................................. 7
8.3 Adjustment of automated CMC interface.......................................................................................... 7
9. Project-specific CP/CPS........................................................................................................................ 7
10. Instruction, inspection and monitoring rights of SwissSign ............................................................... 8
11. Operational readiness and error handling .......................................................................................... 8
12. Service Level Agreement....................................................................................................................... 8
13. Duty of disclosure and delay in cooperation of the RA........................................................................ 8
14. Termination of the contract in relation to Managed PKI........................................................................ 9
15. Customer data and data protection..................................................................................................... 9
16. Liability ....................................................................................................................................................... 9
17. Export and import, international use of certificates............................................................................ 10
18. Intellectual property rights.................................................................................................................... 10
19. Amendments to the RA Delegation Policy and the Declaration of Consent to the RA Delegation Policy .................................................................................................................................... 10
20. Severability ............................................................................................................................................... 10
21. Assignment and transfer of rights and duties...................................................................................... 10
22. No "einfache Gesellschaft" [ordinary partnership]........................................................................... 10
23. Applicable law and jurisdiction............................................................................................................. 11
1. Definition

Accredited certificate service providers may delegate their task of verifying the identity of an applicant to third parties (Registration Authority, abbreviated to “RA”). “Applicant” means a person or organisation who makes an application for the issuance of a certificate (hereafter “APPLICANT”) and thus is a subscriber (hereafter SUBSCRIBER) to a certificate service of SwissSign.

Registration Authority activity is carried out on the basis of a Managed PKI order directly, through a Managed PKI order from a SwissSign reseller, or by the appointment of an external RA by SwissSign on the basis of a separate contract. The RA appoints access managers who act for it. The RA carries out its activity on its own account or on behalf of a third party organisation as APPLICANT.

Registration Authority activity for the Managed PKI service is limited to particular entries in the certificate.

2. Contractual object

The RA Delegation Policy regulates the delegation of the task of verifying the identity of SUBSCRIBERS and stipulates the terms and conditions of use in this regard.

The RA Delegation Policy is accepted by signature of the written declaration of consent to the RA Delegation Policy (hereafter the DECLARATION OF CONSENT) by the organisation performing the RA activity. A new DECLARATION OF CONSENT must be issued under the following circumstances: the change, deletion and addition of restrictions provided for under contract, e.g. designations of organisations, change of access managers and any change to the certificate issuance and verification process.

No commercial contractual relationship shall be established between SwissSign AG and the RA as a result of the DECLARATION OF CONSENT. Use of the Managed PKI shall be based exclusively on the commercial agreement in existence between the RA and SwissSign or between the Specialist Retailer and the RA. Where the agreement has been reached through a Specialist Retailer, the Specialist Retailer shall conclude the commercial agreement on its own behalf and on its own account. Under such circumstances, a Managed PKI service offered shall not constitute a joint offer by the Specialist Retailer and SwissSign, nor shall any corporate relationship come into being between them. The RA acknowledges that no legal claims against SwissSign may arise either under this RA Delegation Policy or from the usage of the Managed PKI service under the RA Delegation Policy, unless SwissSign contravenes any liability terms and conditions pursuant to section 16 “Liability”.

Where a Managed PKI has been acquired through a Specialist Retailer, this RA Delegation Policy shall take precedence over all arrangements and agreements between the Specialist Retailer and the RA.

3. Service Description Registration Authority

The RA shall cover the approval, issue and management of certificates by the access managers of the RA within the ambit of a Certification Authority (abbreviated to “CA”) in accordance with

- the detailed “Certificate Policy” or the “Certificate Practice Statement” (abbreviated to “CP/CPS”) as described in the “SwissSign Platinum CP/CPS” for platinum and qualified certificates,
- the “SwissSign Gold CP/CPS” for gold certificates, or
- the “SwissSign Silver CP/CPS” for silver certificates,

unless any project-specific “CP/CPS” has been agreed to between the parties. The applicable registration and certification processes for publicly trusted certificates shall be governed by Swiss law and the CP/CPS. The most recent versions of these documents are available at https://repository.swisssign.com.

In the basic configuration, the RA shall take on the function of Registration Authority without a hierarchically subordinate registration authority (so-called “sub-RA”). However, the Registration Authority may examine and approve each application for a certificate through a web interface.

In addition, as part of a Managed PKI order, the domains and, where applicable, organisations
specified for the Managed PKI during the setup for this RA shall be approved by SwissSign and unchangeably configured for the RA. This means that SwissSign may enable the RA to issue Managed PKI certificates also through an automated interface without further individual examination for employees, machines, customers and partners of its own organisation and consenting third parties. A requirement for this is that the client software installed at the customer for operating the automated interface shall only process examined and approved certificate application data and thus retrieve certificates issued through the automated interface.

SwissSign manages a publicly accessible directory service for the certificates it issues. The certificates approved by the RA shall be published in the directory service with its consent. The certificates shall bear the name “SwissSign” on them as issuer. This enables people to infer that there is a contractual relationship between SwissSign and the organisation specified in the certificate.

All revoked certificates, without exception, shall be published in the publicly accessible OCSP/CRL Protocol.

If the RA has been acquired e.g. through a SwissSign partner (“Specialist Retailer”), the 1st and 2nd level support for the Managed PKI service shall be provided by the Specialist Retailer. The 3rd level support by SwissSign may be used through the Specialist Retailer’s support. SwissSign shall provide 1st and 2nd level support and in doing so shall contact the access managers named in this Agreement.

Quality audits at the RA shall be charged on a time and expense basis. In the event that the RA conducts its own audit of its processes, the auditing of the verification protocols and tests using random certificate sampling shall be carried out by SwissSign free of charge. It is recommended that this audit be carried out once each year or whenever internal company processes of relevance for registration authority are altered.

Any documents and evidence that are relevant for the approval of applications for certificates must be retained for 7 years after expiration of the validity of the certificate.

The right to arrange for the issuance of certificates and to use them shall be restricted to the duration of the commercial contract concluded with SwissSign in parallel with this.

The information necessary for configuring the RA shall be defined in the DECLARATION OF CONSENT. The DECLARATION OF CONSENT shall be submitted either directly or through the SwissSign Specialist Retailer. The domains specified in the order shall be verified by SwissSign individually in order to check whether they belong to the organisation of the RA or whether the RA is authorised to make changes to them.

The DECLARATION OF CONSENT shall also regulate the authorised officers of the RA. These may be employees of the RA or authorised third parties appointed by the RA.

4. Duties of the RA and restrictions relating to registration authority activity

SwissSign hereby authorises the RA to perform the task of Registration Authority as defined in Section 1. Each RA shall have the following fundamental obligations under this RA Delegation Policy:

The RA shall in particular assume responsibility for verifying the identity of applicants for certificates. In cases involving non-qualified and publicly trusted certificates, the registration and examination processes agreed to under contract shall be complied with. Publicly trusted certificates are certificates with a root certificate that is regarded as trusted by the producers of brows-
ers, operating systems and applications. These are subject e.g. to the CP/CPS as specified in Section 3.

In doing so, the Registration Authority shall comply with the testing requirements for providing the service as stipulated by SwissSign in the Declaration of Consent and in accordance with the instructions of SwissSign in individual cases.

Authorisation to operate the Registration Authority shall be limited to the authorised access managers named in the Declaration of Consent to this Subscriber Agreement.

SwissSign has selected the RA and authorised it to operate a Registration Authority, having duly considered and checked its professional abilities and its resources in terms of finances and personnel. The RA must throughout the term of this Agreement guarantee at all times that the services will be provided securely, reliably and on a long-term basis.

The RA shall only deploy carefully selected and reliable employees who have been trained in the careful and safe handling of certificates and data protection. It shall replace employees who do not display the requisite care or expertise in handling certificates or who otherwise adversely affect or jeopardise contractual performance. When doing so it shall pay particular attention to the interest of SwissSign in maintaining continuity.

The RA shall only deploy employees who have the necessary authorisations to provide the services in accordance with the Declaration of Consent.

The RA shall notify SwissSign in writing of the name and function of the employees who are used to perform the contract.

The RA must inform SwissSign immediately of any material facts that restrict or jeopardise its capacity for action, such as, for example, if there are not enough authorised persons available (minimum: one person).

The RA must inform SwissSign immediately if an authorised access manager no longer works for the organisation of the RA or is declared by the latter to be no longer responsible for the verification of identity.

The same authorised agents may be deployed for more than one Registration Authority, which agents may serve more than one organisation through one single access. These Registration Authorities must ensure that the contents of certificates are not mixed up between different organisations (e.g. domains approved for organisation A must not be indicated in a certificate for organisation B).

All changes to the configuration of the Managed PKI must be reported using the SwissSign change request available on the website www.swisssign.com, unless they can be reported online through the website www.swisssign.net. If the Managed PKI have been purchased from a reseller of SwissSign, requests for changes should be submitted through the reseller.

5. **Duty to provide information of both Parties**

The Parties shall inform each other at regular intervals of any circumstances or events that may be important for implementing this Contract. The other party must be notified immediately of any extraordinary circumstances or in cases of particular urgency. Important general information concerning RA operation shall be published regularly by SwissSign on the system status page https://www.swisssign.com/en/systemstatus and alerts to such information may be subscribed to on that page.

6. **Additional Special Regulations concerning registration activity for special types of certificate**

SwissSign may adopt special regulations to govern the RA's Registration Authority activity for special types of certificate. In the event of any inconsistency, these Special Regulations shall take precedence over those in Section 4.

7. **Prerequisites for exercise**

After all information for configuring the RA has been examined, SwissSign shall implement the setup of the Managed PKI for the RA and shall first start to issue the access certificates required to access the system.
The access managers of the RA shall receive from SwissSign the access certificates required to access the system, along with the requisite password sent at the same time for the private key to said access certificate. The access certificates and the relevant password constitute the means of access.

An RA delegation shall contain a maximum of three access certificates for access by the access managers named in the DECLARATION OF CONSENT and the renewal of these certificates after their expiry as long as the contract is valid. The RA may apply for access certificates for additional access managers. The price shall correspond to the webshop price of an E-mail ID Gold certificate. An application may then be made to SwissSign to also approve these certificates for access. For machine interfaces, the access certificate used to protect communications shall likewise be included in the service. In this case the access manager shall be responsible for correctly deploying this certificate in an application with a machine interface and for properly applying for certificates using the application via this interface.

SwissSign shall notify the access managers of the RA that setup has been successfully completed and that access has been activated.

SwissSign shall be authorised to block access to the Managed PKI without prior notice and without any consequences in terms of cost if the RA breaches any contractual or statutory duties, the security of the system is no longer guaranteed, or the RA or Specialist Retailer is in default with payment.

The RA may arrange for access via SwissSign to be blocked at any time. Specialist Retailers may also arrange for access of the RA of any customer to the Managed PKI to be blocked by SwissSign at any time.

8. Duties of the RA when dealing with certificates

8.1 Compliance with the Subscriber Agreement Certificate Services

The RA shall ensure compliance with the Subscriber Agreement Certificate Services (see Declaration of Consent and paragraph 4) for access certificates and all PARTICIPANT certificates approved by it. It shall also inform the SUBSCRIBER in the event that its certificate has been revoked.

8.2 Protection of the Registration Authority

The RA shall ensure by means of appropriate technical and organisational measures that the data processed by the RA is protected against unauthorised processing (e.g., also by deactivating access that is not required, etc.). SwissSign may define special security requirements at any time. The RA shall disclose its security system relating to the Registration Authority activity at any time to the extent that SwissSign requests this for the purpose of monitoring compliance with this Agreement.

8.3 Adjustment of automated CMC interface

The RA shall, pursuant to new security or statutory requirements, agree to implement within a reasonable period a new release of any automated CMC interface that is installed, unless the web-based interface is used. The CMC interface shall be used for the purpose of automated requesting, revocation and administration of certificates.

SwissSign shall be authorised to block access to the Managed PKI without prior notice and without any consequences in terms of cost if the RA breaches any contractual or statutory duties, the security of the system is no longer guaranteed, or the RA or Specialist Retailer is in default with payment.

The RA acknowledges that any violation of the duty of care will result in financial loss and/or other adverse consequences for SwissSign, particularly in cases involving publicly trusted certificates, such as e.g. the exclusion from root programmes or subjection to sanctions in the event of endorsements/certifications, or adverse regulatory consequences.

9. Project-specific CP/CPS

SwissSign may stipulate in a project-specific CP/CPS special rules and obligations to be complied with in issuing certificates for the RA. Multiple project-specific CP/CPS may be stipulated where there are different certificate types.
Both the regulatory requirements and the requirements of the CA browser forum and of all application or browser manufacturers for the recognition of trustworthy certificates must be followed in the project-specific CP/CPS for publicly trusted certificates.

SwissSign shall consult the RA prior to any planned changes in the project-specific CP/CPS for publicly trusted certificates and shall take due consideration of its concerns.

Project-specific CP/CPS are annexed to the DECLARATION OF RECOGNITION.

10. Instruction, inspection and monitoring rights of SwissSign

SwissSign may at any time order changes to the verification processes and any necessary measures, including stipulating deadlines for implementing them, and issue further instructions regarding the duties of the Registration Authority.

SwissSign shall have the right at any time to monitor or arrange for another party to monitor compliance with this Agreement. SwissSign shall carry out checks in situ during ordinary office hours and with reasonable advance notice. The RA shall for this purpose allow inspection of all necessary documents and systems. SwissSign states its willingness to sign the standard non-disclosure and data protection agreements of the RA for this purpose if necessary. SwissSign shall bear the costs arising for itself or any third party engaged by it when exercising this right of inspection and monitoring unless the result of such monitoring justifies the imposition of the costs on the RA. SwissSign may in particular at any time with reasonable advance notice monitor or arrange for another party to monitor whether the identity verifications are being properly carried out and whether the requirements for providing the services are being complied with. SwissSign shall inform the RA promptly of any planned checks and the result thereof.

The RA shall itself audit the process of its own Registration Authority annually and shall make the results available to SwissSign upon request unless otherwise provided in the Annexes. SwissSign may review these results based on a random sampling of certificates issued to the RA. The RA may also at its own cost appoint a qualified auditor or SwissSign to perform the audit.

11. Operational readiness and error handling

The Registration Authority shall be declared to be operationally ready once SwissSign has provided the RA with the necessary access data.

The RA shall check access and the issuance of certificates. It shall review the certificates after issuance in order to ensure that they are correct and shall immediately report any errors. Any incorrect or incomplete details shall be notified to SwissSign in writing before the certificates are used by the applicant. Subsequent errors must also be reported as soon as they are discovered. No liability will be accepted for any consequential losses. If an error message has been transmitted, SwissSign shall have the right either to rectify the loss by means of an update or to carry out a new installation. Faulty certificates that have been issued shall be declared by SwissSign to be invalid and may be replaced. Any further claims are expressly excluded.

12. Service Level Agreement

The Service Level Agreement shall be stipulated in the direct commercial agreement between SwissSign and the RA or in the commercial agreement between SwissSign and the Specialist Retailer.

13. Duty of disclosure and delay in cooperation of the RA

The RA must notify SwissSign immediately within one business day of the discovery of any actual or suspected irregularities concerning the contractual activity as Registration Authority. This shall also include accusations, reports and complaints made against the RA as a result of certificates issued.

SwissSign shall be authorised to suspend registration authority services or Managed PKI services in general with immediate effect if services which the RA has failed to provide as required under contract are not provided within a grace period set by SwissSign or if the RA declares prior to the expiry of such a grace period that it
will be unable to provide the service or to do so within the grace period. The granting of such a grace period shall have no effect on the consequences of the default that has already occurred. SwissSign shall still have the option of claiming damages.

14. **Termination of the contract in relation to Managed PKI**

In the event of a Managed PKI, usage of the certificates after the commercial agreement with SwissSign or the Specialist Retailer has ended shall not be permitted. All certificates that are still technically valid must be revoked by the SUBSCRIBER, the RA or upon payment of a fee by SwissSign.

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

15. **Customer data and data protection**

SwissSign undertakes to comply with the provisions of Swiss data protection legislation. The RA undertakes to comply with the provisions of the locally applicable data protection legislation and to abide by the applicable CP/CPS as stated in the Declaration of Consent. The data required to provide the services shall be saved and treated as confidential by SwissSign. State of the art security technology shall be used to protect data from unauthorised processing or unauthorised access.

Personal data may only be processed for the purpose and to the extent required to perform and implement the agreement. In particular, the data collected from the Registration Authority in relation to the Registration Authority activity may only be used by the RA for the purpose of performing this agreement. Usage for other purposes or disclosure to third parties is strictly prohibited. The above shall not apply if SwissSign expressly consents in writing (e.g. in the event of an audit by an authorised third party).

The data protection level in Switzerland has been confirmed by the European Commission as adequate. The requirement for the lawful transmission of data from member states of the European Union to Switzerland, namely that there must be an adequate level of data protection in the location in the third country where the data is received, has consequently been met.

16. **Liability**

SwissSign shall bear full liability for the Registration Authority towards the approval body that is to supervise it pursuant to Art. 16 ZertES and in accordance with ETSI rules.

SwissSign shall bear full liability towards the RA for any losses occasioned by it to the RA unless SwissSign proves that it was not at fault. Liability for minor negligence is excluded. The provisions on liability set forth in the CP/CPS in accordance with the Declaration of Consent shall apply to third parties.

Neither party shall bear liability for the proper functioning of third party systems, and in particular of the internet. SwissSign shall not be liable for the systems and software used by the RA.

The RA shall bear liability towards SwissSign for any losses attributable in any way to the non-compliance or inadequate compliance with its contractual obligations, unless it proves that it was not at fault. It shall in addition bear joint and several liability along with the Specialist Retailer for any losses caused by it or the Specialist Retailer to SwissSign in relation to the setup and operation of these Managed PKI unless it proves that neither it nor the Specialist Retailer was at fault. Liability for minor negligence is excluded for the contractual obligations set forth in chapters 1, 2, 12, 17, 20, 21, 22 and 23.

The RA shall fully indemnify SwissSign from all third party claims resulting from use in breach of contract or unlawful or improper use of the service by the RA. In such an eventuality, this shall include an obligation to fully indemnify SwissSign against legal defence costs (e.g. court and lawyers’ fees).

Both Parties shall be liable for the conduct of their auxiliary agents and any third parties who are involved (such as subcontractors and suppliers) in the same manner as for their own.
In the event of personal injury, the Parties shall bear liability irrespective of fault. The Parties shall not under any circumstances bear liability in particular for indirect or consequential losses, data loss, additional expense or claims by third parties, lost profit or unrealised savings, or losses resulting from late delivery or service provision.

In the case of minor negligence (according to the Federal Act on the Amendment of the Swiss Civil Code §100, clause 2) by the customer under this Agreement, the damage per fraudulent authorized and issued certificate is limited to the amount of liability due pursuant to CP / CPS (cf. 3) or according to court order order.

17. Export and import, international use of certificates

The export and/or import and the use of certificates are subject to certain regulations and restrictions pursuant to Swiss law or the relevant applicable national law. In particular, certificates may not be purchased from persons or organisations from countries listed on the website https://www.swisssign.com/export under the heading "Export Restrictions".

The RA acknowledges that the deployment and use of digital certificates and the exchange of digitally signed and/or encrypted data outside Switzerland is subject to foreign jurisdictions and that therefore different effects may result, which may be more or less extensive than is the case under Swiss law. The exchange of encrypted data and the export/import of cryptographic software or cryptographic data storage media are also subject to statutory restrictions in certain foreign countries. In the case of a direct agreement with SwissSign, it shall be the responsibility of the RA or the SUBSCRIBER to clarify the legal position in this regard.

18. Intellectual property rights

No intellectual property rights (such as copyright, trademark, design or patent rights etc.) shall be transferred to the RA by the SwissSign service.

Where additional material is provided along with the service (documentation, devices or external software), all intellectual property rights over the material provided by SwissSign shall remain with SwissSign or the third parties with rights there-over. The RA shall receive a non-exclusive, non-transferable licence to use such material in line with the contractual object, which shall be limited to the contractual term. The Specialist Retailer and/or the RA shall not have any rights to make changes or further developments.

19. Amendments to the RA Delegation Policy and the Declaration of Consent to the RA Delegation Policy

Amendments and additions to the RA Delegation Policy must be made in writing by a new DECLARATION OF CONSENT or any other form stipulated by SwissSign for the relevant amendments.

Notwithstanding the above, technical parameters within the DECLARATION OF CONSENT or its annexes may be subjected to substantive amendment by change forms, which will be provided by SwissSign.

20. Severability

If individual provisions of the Agreement (including annexes) prove to be invalid or unlawful, this shall not affect the validity of the remainder of the Agreement. Should this occur, the relevant term shall be replaced by a valid term that is as close as possible in financial terms.

21. Assignment and transfer of rights and duties

The RA may not assign or pledge any claims against SwissSign without the written consent of SwissSign.

The RA and SwissSign shall not be entitled to assign or transfer any rights and duties arising under this Contract.

22. No "einfache Gesellschaft" [ordinary partnership]

The Parties expressly declare that they shall not establish an "einfache Gesellschaft" [ordinary partnership] within the meaning of Art. 530 Swiss Code of Obligations or any other corporate relationship. The Parties shall refrain from giving third parties the impression that they have established an "einfache Gesellschaft" [ordinary partnership] with the other party.
The sole purpose of the cooperation between the Parties is to provide services for consideration in accordance with individual reciprocal contracts.

The Parties have no shared organisation, infrastructure or resources and do not pursue a common purpose. The Parties are separate and independent companies and operate in the market as such. The Parties are not obliged to pay contributions of any kind or to make any subsequent contributions. Participation in profits or losses is excluded. Each Party shall bear its own risks and expenses. Neither party is authorised to act on behalf of the other party.

23. Applicable law and jurisdiction

Swiss law shall apply exclusively. The above is subject to the law of Liechtenstein governing signatures for certificates that have been issued and signed by the Liechtenstein CA. The provisions of the UN Convention on Contracts for the International Sale of Goods of April 11, 1980 (Vienna Convention, “CISG”) shall not apply.

The courts of Zurich, Switzerland shall have exclusive jurisdiction. For Specialist Retailers and RA USERS with a foreign place of residence or registered office, the place of debt enforcement and exclusive jurisdiction for all proceedings shall be Zurich.