

Relying Party Agreement

Version: 1.0

OID: 2.16.756.1.89.1.0.5.0.1

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

Author	Date	Version	Comments
Ingolf Rauh	2017-07-14	1.0	Creation

Approval by

SwissSign authorised signatory	Digital signature
Reinhard Dietrich (CISO) SwissSign AG	
Markus Naef (CEO) SwissSign AG	

Table of contents

1. Scope.....	4
2. Compliance with regulatory requirements.....	4
3. Contractual Components.....	4
4. Warranty conditions.....	4
5. Exclusions on usage.....	5
6. Legal effect of certificates, export.....	5
7. Time stamp.....	5
8. Report of misuse, theft	5
9. Reports by SWISSIGN.....	5
10. Entry into force, duration and termination, effect of termination in general.....	5
11. Customer data and data protection.....	6
12. Involvement of third parties.....	6
13. Warranty	6
14. Liability	7
15. Export and import, international use of certificates	7
16. Intellectual property rights.....	7
17. Severability.....	7
18. Amendment of the SUBSCRIBER AGREEMENT CERTIFICATE SERVICES	7
19. Assignment and transfer of rights and duties.....	8
20. Out of court dispute resolution.....	8
21. Applicable Law and Place of Jurisdiction	8

1. Scope

In receiving a signed document or using certificate-protected communication on the strength of a certificate based on one of the publicly trusted root certificates of the Swiss or Liechtenstein SwissSign Platinum CA, SwissSign Gold CA or SwissSign Silver CA of SwissSign AG, Sägereistrasse 25, 8152 Glattbrugg, Switzerland (hereafter SWISSIGN), the recipient of a signed document (hereafter RECIPIENT) or the communication partner of the certificate-protected communication consents to the Relying Party Agreement (hereafter RELYING PARTY AGREEMENT).

The RELYING PARTY AGREEMENT shall govern the warranty provided by SWISSIGN to the RECIPIENT. A SUBSCRIBER means an applicant for a SWISSIGN certificate, which acquires it from SWISSIGN and issues it in its own right or for another party (server or other person, hereafter CERTIFICATE HOLDER). For the purposes of the time stamp service, the SUBSCRIBER is the responsible recipient of the time stamp.

2. Compliance with regulatory requirements

Insofar as the issuance and management of certificates is subject to statutory requirements (e.g. in Switzerland the ZertES and OEIDI; in Liechtenstein the Signatures Act eIDAS), SWISSIGN warrants compliance with the relevant requirements and implementing provisions. SWISSIGN shall in this regard be subject to oversight by the competent bodies (Switzerland: Certification Authority; Liechtenstein: Office for Communication) whilst audits and inspections shall be carried out in accordance with the relevant standards applicable to the certificates in question (e.g. ETSI, CA Browser Forum) and statutory requirements.

3. Contractual Components

The applicable CP/CPS of the applicable trusted root certificate shall be an integral part of this Relying Party Agreement and shall take precedence in the event of any discrepancies.

The applicable CP/CPS may be obtained in their most up-to-date form at <https://www.swissign.com/en/cp-repository>.

4. Warranty conditions

Before the RECIPIENT can rely on a signature contained in a SWISSIGN certificate, it must take account of the following:

- Certificates shall be issued in accordance with the provisions of the CP/CPS for the CA of the relevant root certificate. The CP/CPS may be obtained in their most up-to-date form at <https://www.swissign.com/en/cp-repository>.
The provisions also set out details concerning the level of review, the guarantee and in general the conditions under which the certificate was issued for a signature.
- The Certificate Holder is subject to the Subscriber Conditions ("Subscriber Agreement") when issuing the certificate or time stamp, which may be obtained in their most up-to-date form at <https://www.swissign.com/en/cp-repository>.
This document also sets forth the legal framework conditions governing the use of the certificate.
- On account of the different examination criteria for the Silver, Gold and Platinum certificate classes, as described in the CP/CPS, the use of the signature should reflect the risk of the content thereby signed off. The review costs for Silver certificates are lower than for Gold certificates, whilst those for Gold certificates are lower than for Platinum certificates.

The signature on which the certificate is based and all certificates in the certificate chain must not have been revoked. SWISSIGN shall provide standard services for examining the validity of the certificate, such as CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol). Before a signature is trusted, its validity shall be verified by the RECIPIENT. Links to the CRL and OCSP are part of the certificate. CRLs are valid for a maximum of 10 days, although are updated hourly in case of European certificates from the SwissSign Liechtenstein Root and updated daily in case of certificates from the SwissSign Switzerland Root. The RECIPIENT must therefore always refer to the most recent CRL file in order to review the validity of the certificate.

If for technical reasons no CRL file or OCSP service is available, the RECIPIENT must estimate itself how long it is able to rely on the validity of the signature. This shall also take account of the related transactions and the attendant risk. Confidence should not be granted for longer than 10 days.

The validity of SWISSIGN certificates shall be limited to the validity period of the certificate less 10 days. The RECIPIENT must therefore always check whether the certificate is still valid.

For signed documents it is necessary to verify that the documents have not been altered after the signature was affixed.

Signature review applications should indicate that the signature is reliable under the circumstances indicated herein. In particular, the identity of the certificate holder should be correctly indicated. Pseudonyms should be designated as such within signature review applications. Pseudonyms shall be designated in the certificate by the prefix "pseudo:" in the subject line.

It is necessary to ensure that the certificate does not contain transaction limits that would preclude the usage of the certificate in relation to a transaction.

5. Exclusions on usage

SWISSIGN certificates are not intended for usage within highly critical infrastructure. Decisions that could result directly or indirectly in personal injury or significant damage to property should not be taken automatically on the basis of SWISSIGN certificate signatures. Such situations include but are not limited to: the operation of power stations, weapons systems, flight control systems, etc.

Responsibility for the risk assessment and usage of the certificate within a particular deployment scenario shall lie with the RECIPIENT.

Signatures that are no longer valid must not be used.

6. Legal effect of certificates, export

The RECIPIENT acknowledges that digitally signed documents may, depending upon the

applicable legislation, have the same legal effect as documents signed by hand.

The RECIPIENT acknowledges that the deployment and use of digital certificates and the exchange of digitally signed and/or encrypted data outside Switzerland, Liechtenstein and the EU/EEA 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, Liechtenstein or EU 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. Clarification of matters in this respect shall be a matter under all circumstances for the RECIPIENT.

7. Time stamp

SWISSIGN provides a time stamp service, which is governed by the Time Stamping Policy. This may be obtained in its most up-to-date form at <https://www.swisssign.com/en/cp-repository>. The RECIPIENT must satisfy itself that the time stamp certificate on which the time stamp is based was valid at the time of signature and that the signature was affixed correctly.

8. Report of misuse, theft

Should the RECIPIENT ascertain that a certificate has been misused or stolen, it must report this promptly to the support service of SWISSIGN:

helpdesk@swisssign.com.

The report must contain contact information (telephone, email). The support service shall then contact the RECIPIENT directly.

9. Reports by SWISSIGN

SWISSIGN shall report any relevant incidents, including in particular also compromising, misuse, changes to the algorithm etc. on its system status page <https://www.swisssign.com/en/systemstatus>.

10. Entry into force, duration and termination, effect of termination in general

The Contract shall take effect upon the issuance of the certificate and shall apply for the duration

thereof. It shall end upon expiry of the certificate in question or upon revocation (withdrawal).

The validity of the certificate shall expire upon termination of the Contract. Time stamps and signatures affixed shall remain valid unless and until the signature certificates have been revoked. Any certificates that are still valid shall be revoked.

Notice of termination must always be given in writing.

11. Customer data and data protection

SWISSSIGN undertakes to comply with the data protection legislation applicable to its relevant CA.

The data contained in the certificate shall be regarded as publicly available data.

The data required to provide the services shall be saved and treated as confidential by SWISSSIGN. The data collected as part of inspection activity, including in particular personal data, may only be used for the purpose and to the extent required to perform and implement the CERTIFICATE SERVICE. Usage for other purposes or disclosure to any third parties is strictly prohibited. The above shall not apply to disclosure to authorised instructed third parties (e.g. in the event of a control, external registration activity) or in accordance with official requirements. Authorised instructed third parties shall be subject to data protection rules in the same manner as SWISSSIGN.

The security technology used to protect data shall correspond to the state of the art.

The SUBSCRIBER and CERTIFICATE HOLDER undertakes to comply with the provisions of data protection legislation that is locally applicable to it as well as the data protection provisions of the applicable CP/CPS (see 3).

In order to ensure compliance with statutory requirements, as the certification and registration authority, SWISSSIGN must retain all certificate holder data, documentation and audit information for a minimum period of 11 years after expiration of a certificate.

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.

12. Involvement of third parties

SWISSSIGN may engage third parties at any time to perform its services.

13. Warranty

SWISSSIGN warrants to the RECIPIENT of a signature:

- That all information contained in the certificate attributes is correct and has been reviewed in accordance with the applicable CP/CPS,
- That these certificates have only been issued by SWISSSIGN to the party that requested the certificate or that only that party has been enabled to download them.

The SUBSCRIBER shall examine the material provided, including in particular the certificates provided, following their issuance and report any defects or incorrect and/or incomplete information promptly (within no more than 7 working days), and under all circumstances prior to the first usage. If evident defects are not reported promptly following receipt, and latent defects not promptly after discovery, the rights relating to defects shall be deemed to have been forfeited. The SUBSCRIBER shall bear the burden of proving the time when the defects objected to were discovered and that the report was made promptly.

In the event that a defect is reported, SWISSSIGN shall be entitled to choose between rectification and replacement. Defective certificates shall be declared invalid and replaced by new certificates. Any further rights as to defects are expressly excluded.

SWISSSIGN does not provide any warranty regarding the compatibility of the certificates provided with non-Swiss law and reserves the right to refuse requests for certificates from the SUB-

SCRIBER where these run contrary to statutory export restrictions or limitations or compliance requirements of SWISSIGN.

14. Liability

SWISSIGN shall bear full liability towards the SUBSCRIBER for any losses occasioned by it to the SUBSCRIBER unless SWISSIGN proves that it was not at fault. Liability for minor negligence is excluded.

The liability provisions of the CP/CPS apply to third parties (see 3).

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

The SUBSCRIBER shall fully indemnify SWISSIGN from all third parties' claims resulting from use in breach of contract or unlawful or improper use of the CERTIFICATE SERVICE. The indemnification shall include also the obligation to hold SWISSIGN fully harmless against legal defence costs (e.g. procedural costs and legal 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 be liable for any fault. Under no circumstances shall the Parties be liable 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.

The provisions governing liability set forth in the Swiss Federal Act on Electronic Signatures and in Article 59a of the Swiss Code of Obligations shall apply under all circumstances on a priority basis.

15. Export and import, international use of certificates

The SUBSCRIBER acknowledges that the exporting or importing and usage of CERTIFICATE SERVICES from, to or in countries subject to

sanctions and embargoes is prohibited (cf. <https://www.swissign.com/en/export>).

The SUBSCRIBER acknowledges that the deployment and use of digital certificates and the exchange of digitally signed and/or encrypted data outside Switzerland, Liechtenstein and the EU/EEA 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, Liechtenstein or EU 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. Clarification of matters in this respect shall be a matter under all circumstances for the SUBSCRIBER.

16. Intellectual property rights

No intellectual property rights (such as copyright, trademark, design or patent rights etc.) shall be transferred to the SUBSCRIBER by the CERTIFICATE SERVICE. All intellectual property rights over the material provided by SWISSIGN (documentation, devices, software etc.) shall remain the property of SWISSIGN or the third parties with rights thereto. The SUBSCRIBER 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 SUBSCRIBER shall not have any rights to make changes or further developments.

17. Severability

If individual terms of this SUBSCRIBER AGREEMENT are found to be invalid or unlawful, this shall not affect the validity of the Contract. Should this occur, the relevant term shall be replaced by a valid term that is commercially equivalent as far as possible.

18. Amendment of the SUBSCRIBER AGREEMENT CERTIFICATE SERVICES

SWISSIGN reserves the right to amend this Subscriber Agreement Certificate Services at any time.

The relevant amended version shall be published on the website <https://www.swissign.com/en/cp-repository> in good time before it comes into effect and shall

be notified through the system status page:
<https://www.swissign.com/en/systemstatus>.

The amended SUBSCRIBER AGREEMENT shall be deemed to have been approved unless the SUBSCRIBER objects in writing within one month. An objection shall be deemed to constitute notice of termination of the Contract and shall automatically result in its dissolution.

19. Assignment and transfer of rights and duties

The SUBSCRIBER may not assign or pledge any claims against SWISSIGN without the written consent of SWISSIGN.

The SUBSCRIBER shall not have the right to assign or transfer the rights and obligations pursuant to this Agreement.

20. Out of court dispute resolution

The Parties shall endeavour to resolve disputes amicably before applying to the ordinary courts and undertake to participate in out of court dispute resolution procedures prescribed by law, to the extent of their statutory duties.

21. Applicable Law and Place of Jurisdiction

The legal relationship resulting from this SUBSCRIBER AGREEMENT shall be governed exclusively by Swiss law. 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") are excluded under all circumstances.

The courts of Zurich, Switzerland shall have exclusive jurisdiction. For Subscribers and Certificate Holders with a foreign place of residence or registered office, the place of debt enforcement and exclusive jurisdiction for all civil proceedings shall be Zurich, Switzerland.