PKI Disclosure Statement Time Stamp Services

Version: 1.0

OID: 2.16.756.1.89.1.1.6.1.1

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	Reinhard Armand Dietrich Qualifiziert signiert durch Reinhard Armand Dietrich Swiss Post Solutions AG Glattbrugg, 21. Juli 2017
Markus Naef (CEO) SwissSign AG	Qualifiziert signiert durch Markus Naef SwissSign AG Glattbrugg, 27. Juli 2017

Table of contents

1. Scope 4

2. CA Contact Info 4

3. Certificate type, validation process and usage 4
3.1 Intended usage 4
3.2 Validation process 4
3.3 Limitations 4

4. Limitations on trust 5

5. Duties of the SUBSCRIBER 5

6. Duties of the RELYING PARTY and examination of the certificate 5

7. Limitations on liability 6

8. Other applicable documents 6

9. Privacy Policy 7

10. Refund Policy 7

11. Applicable law, complaints and dispute resolution 7
11.1 OUT OF COURT DISPUTE RESOLUTION 7
11.2 APPLICABLE LAW AND JURISDICTION 7

12. TSP and repository licenses, trust marks, and audit 7

1. Scope

In applying for a signature service and/or timestamping service, the Subscriber to a signature service and/or timestamping service (hereafter SUBSCRIBER) consents to the Subscriber Agreement Signature and Timestamping Service (hereafter SUBSCRIBER AGREEMENT).

The SUBSCRIBER AGREEMENT shall govern the contractual relationship between the SUBSCRIBER and SwissSign AG, Sägereistrasse 25, 8152 Glattbrugg, Switzerland (hereafter SWISSSIGN) concerning the use of time stamps of SWISSSIGN and the use of signatures on certificates managed by SWISSSIGN on a fiduciary basis or on certificates made out to SWISSSIGN for third party signature use (hereafter "SERVICES").

A SUBSCRIBER also means the recipient of a time stamp and/or a signature. It may be an organisation or an individual end user. The SUBSCRIBER must ensure that the service is used in accordance with the Contract.

Signatures and time stamps shall be issued in accordance with the provisions of the SwissSign Platinum CP/CPS. The CP/CPS may be obtained in their most up-to-date form at https://repository.swisssign.com.

Compliance with the commercial contractual terms and conditions, which are the basis for usage by the SUBSCRIBER, is a prerequisite for the usage of the SERVICE. The commercial contractual terms and conditions are not an integral part of this SUBSCRIBER AGREEMENT. They may also be agreed to between third parties (e.g. Specialist Retailer, employer of the SUBSCRIBER etc.).

For contractual purposes, the SUBSCRIPTION AGREEMENT and any commercial contractual terms and conditions shall continue to apply, as shall the relevant CP/CPS for the issue of certificates. The PKI Disclosure Agreement shall not replace this and only contains a summary for information purposes of the key points of these two documents in order to facilitate understanding by SUBSCRIBERS, CERTIFICATE HOLDERS and third parties (RELYING PARTIES).

2. CA Contact Info

SwissSign AG, Switzerland:
Postal address: Sägereistrasse 25,
8152 Glattbrugg, Switzerland.
Telephone: +41 848 77 66 55
Email: helpdesk@swisssign.com

SwissSign AG, Liechtenstein:
Postal address: SwissSign AG Liechtenstein,
Meierhofstrasse 5, 9490 Vaduz, Liechtenstein
Telephone: +41 848 77 66 55
Email: helpdesk@swisssign.com

3. Certificate type, validation process and usage

3.1 Intended usage

Time stamp certificates shall be offered in accordance with EU Regulation 910/2014 ("eIDAS Regulation") and the Swiss Signatures Act ("ZertES"). Under the terms of these Regulations, they shall apply as a qualitative time stamp and confirm that a document has not been changed since the time stamp was affixed, and also indicate the correct time by this stamp. A time stamp must be affixed in conjunction with a qualitative signature.

The qualitative time stamp service under Swiss law (ZertES) is offered at http://tsa.swisssign.net or https://tsa.swisssign.net. No further user names or passwords are necessary. The qualitative time stamp service under Swiss law (ZertES) is offered at http://tsa-eu.swisssign.net or https://tsa-eu.swisssign.net.

The Time Stamp Policies shall apply to both time stamps, the most up-to-date versions of which are available at https://repository.swisssign.com.

3.2 Validation process

All users that have a commercial relationship with SwissSign are permitted to use the time stamp. Only the IP address will be checked. In the event that the time stamp service is misused from such an IP address, it will be blocked.

3.3 Limitations

The time stamp hashes may be SHA-256, SHA-384 or SHA-512.

The Swiss time stamp according to the ZertES features the following parameters:

Guidelines OID:2.16.756.1.89.1.1.3.4
Certificate Holder
CN: SwissSign TSA 2016-G22
O: SwissSign AG
C: CH
Signature algorithm: SHA256

The eIDAS compliant time stamp according to the Liechtenstein Signatures Act features the following parameters:

Not currently offered.

The maximum validity of the time stamp is 10 years.

4. Limitations on trust

The usage of the time stamp is indicated in the intended purpose specified in section 3.

The maximum time difference compared to the UTC time reference may amount to +- 1 second. If no time reference is available, no time stamp will be issued.

All data contained in the activity log (data concerning the certificate lifecycle) will be retained for 11 years.

5. Duties of the SUBSCRIBER

The SUBSCRIBER must ensure compliance with the terms of the SUBSCRIPTION AGREEMENTS. These require the SUBSCRIBER in particular to comply with the following duties:

The number of time stamps that may be received is not subject to any technical limitation. The SUBSCRIBER undertakes not to exceed the quota announced or ordered or the available quota of time stamps without liaising with SWISSSIGN.

The SUBSCRIBER shall report all IP addresses intended for usage with the time stamp service to SWISSSIGN in the event that it wishes to use up more than the available quota. Changes shall be announced in good time (one month in advance).

The client software of the SUBSCRIBER used shall be deployed in accordance with the recommendations of SWISSSIGN and must feature secure cryptographic functions. In the event of doubt, SWISSSIGN shall be questioned in advance regarding the deployment of the client software.

The maximum performance guaranteed for retrieval by the SUBSCRIBER shall not be exceeded.

The SUBSCRIBER shall examine the SWISSSIGN revocation list (CRL) in order to ensure that the time stamp certificate has not been revoked.

The SUBSCRIBER must inform all relevant recipients of a timestamped document ("Relying Party") of the time stamp policy and the opportunities to review the time stamp in accordance with the following Section.

6. Duties of the RELYING PARTY and examination of the certificate

The Relying Party 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.

- The signature on which the certificate is based and all certificates in the certificate chain must not have been revoked. SwissSign 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 should be verified by the RELYING PARTY. Links to the CRL and OCSP are part of the certificate. CRLs are valid for a maximum of 10 days, although are updated daily. The RELYING PARTY must therefore always refer to the most recent CRL file in order to verify the validity of the certificate.
- If for technical reasons no CRL file or OCSP service is available, the RELYING PARTY 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 may not be granted for longer than 10 days.

- The validity of SwissSign certificates shall be limited to the validity period of the certificate less 10 days. The RELYING PARTY must therefore always check whether the certificate is still valid.
- For signed documents it is necessary to ensure that the documents have not been changed since the signature was affixed.
- Standard applications should indicate that the signature is reliable under the circumstances indicated in the last point. In particular, the identity of the certificate holder should be correctly indicated.
- SWISSSIGN time stamps 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 SwissSign 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 RELYING PARTY.
- Signatures that are no longer valid must not be used.
- During usage under the eIDAS the RELYING PARTY must ensure pursuant to ETSI standard 319 421 that the SWISSSIGN time stamp certificate is listed as a qualified certificate on the eIDAS Trusted List.

7. Limitations on liability

Limitations on liability are set forth in the CP/CPS. All qualified certificates and seal certificates of Platinum Root CA are subject to the statutory liability limit laid down in the ZertES (Swiss qualified certificates) and the eIDAS (EU qualified certificates).

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

The liability provisions of the CP/CPS apply to third parties.

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

The SUBSCRIBER shall fully indemnify SWISSSIGN from all third party 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 SWISSSIGN 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 for certificates signed by the Swiss CA, whilst the provisions governing liability set forth in the Liechtenstein Signatures Act shall apply in relation to certificates signed by the Liechtenstein CA.

8. Other applicable documents

The following documents shall be relevant for the SUBSCRIBER and the CERTIFICATE HOLDER along with the RELYING PARTY, the most recently updated version of which may be found at https://repository.swisssign.com:

- CP/CPS Platinum certification guidelines and implementing provisions of SwissSign CA.
- Time Stamp Policy (TSA Policy)
- Subscriber Agreement TSA and Signing Service provisions setting out the rights and duties of the SUBSCRIBER and CERTIFICATE HOLDER in relation to a certification service.

- Relying Party Agreement provisions setting out the rights and duties of a RELYING PARTY.

9. Privacy Policy

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

As a matter of principle, under the time stamp service the SUBSCRIBER will only transfer a hash of its document data, from which the contents of the document cannot be reconstructed. The IP address shall also be transferred.

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 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.

10. Refund Policy

Signatures that have already been affixed may be refunded in accordance with the commercial GTCs. The most recently updated version may be downloaded from www.swisssign.com/agb.

11. Applicable law, complaints and dispute resolution

All complaints must be submitted to SwissSign using the contact form at www.swisssign.com/contact.

11.1 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.

11.2 APPLICABLE LAW AND JURISDICTION

The legal relationship resulting from the SUBSCRIPTION 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.

12. TSP and repository licenses, trust marks, and audit

Insofar as the issuance and management of time stamps is subject to statutory requirements (e.g. in Switzerland the ZertES and OEIDI; in Liechtenstein the Signatures Act EiDAS), SWISSSIGN warrants compliance with the relevant requirements and implementing provisions. SWISSSIGN shall in this regard be subject to oversight by the competent bodies (Switzerland: certification authority KPMG Switzerland; Liechtenstein: Office for Communication with audit by TÜV IT Nord, Germany) 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.