SwissSign TSA Policy

Time Stamping Authority Policy

Document Type:	Time-stamping Policy
OID:	2.16.756.1.89.1.1.3.5
Author:	Information Security and Compliance
Classification:	Attribution-NoDerivs (CC-BY-ND) 4.0
Applicability:	Global
Owner:	CEO
Issue Date:	02 August 2022
Version:	2.0
Obsoletes:	v1.3.2, 25.02.2019
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Version Control

Date	Version	Comments	Author
15.01.2006	1.0.0	Initial draft	Michael Doujak
16.01.2006	1.0.1	Review	Joseph A. Doekbrijder
17.01.2006	1.0.2	Release	Michael Doujak
24.03.2006	1.0.3	Feedback of KPMG	Melanie Raemy
19.05.2006 – 25.09.2006	1.0.4 – 1.0.10	Review, Final Review, Feedback of KPMG, Added Cert Profile Reference	Michael Doujak with external QS for technical and legal support, Melanie Raemy, Björn Kanebog
09.05.2007	1.0.11	Review, Minor Changes	Björn Kanebog
15.04.2008	1.1.1	New layout, Review, Minor Changes	Björn Kanebog
20.04.2008	1.1.1	Review	Michael Doujak
16.09.2010	1.1.2	Review	Tobias Grossmann
03.11.2010	1.1.3	Review for G3 CA. New definition of TSU.	Michael Doujak
12.11.2015	1.1.4	Md5 and RipeMD160 inoperative	Cornelia Enke
21.11.216	1.2	Remove SHA1;Include TSA Issuing CA	Cornelia Enke
17.01.2017	1.3	Chapter 3 - Update VZertES, TAV and ETSI Standards	Cornelia Enke
23.03.2018	1.3.1	Only new Logo/Look and Feel Added supported fields in the request	Ingolf Rauh, Cornelia Enke
22.02.2019	1.3.2	Small changes to references, cleanup of references	Michael Guenther, Matthias Bartholdi
02.08.2022	2.0	Cryptographic algorithms, Update of references, Specification of TST components, Provisioning and rekeying of TSU certificate, TST practices, Compromise of TSA Service	Adrian Mueller, Michael Guenther

Approval by

Date	Approved by	Approved by	Version
17.01.2006	Michael Doujak	Melanie Raemy	1.0.2
22.05.2006	Michael Doujak	Melanie Raemy	1.0.6
26.09.2006	Michael Doujak	Melanie Raemy	1.0.10
21.05.2007	Melanie Raemy	Björn Kanebog	1.0.11
28.04.2008	Adrian Humbel	Björn Kanebog	1.1.1
04.02.2011	Adrian Humbel	Michael Doujak	1.1.3
25.11.2015	Reinhard Dietrich	Urs Fischer	1.1.4
21.11.2016	Reinhard Dietrich	Urs Fischer	1.2.
15.06.2018	Reinhard Dietrich	Markus Naef	1.3.1.
22.02.2019	Matthias Bartholdi	Markus Naef	1.3.2
26.07.2022	Michael Günther	Jürg Graf	2.0

digital signature

digital signature

Table of contents

1. Introduction

SwissSign AG offers a time-stamping service as part of its certification services in accordance with Swiss Digital Signature Law (ZertES). This service creates and records reliable and trustworthy digital evidence of data at a certain point in time, significantly enhancing the trustworthiness of the electronic data.

SwissSign AG has created a time-stamping authority (SwissSign TSA) to provide the time-stamping service.

This document describes the policy of the Time-stamping Authority (TSA). This TSA policy specifies the general processes and policies of the time-stamping authority for the generation of a time-stamp and its services. Additional processes and technical details are specified in more detail in the policy documents SwissSign Certificate Policy for the TSA certificates [1], SwissSign CPS Signing Services [2], the SwissSign Trust Services Practice Statement (TSPS) [3] and the Certificate, CRL and OCSP Profiles for Signing certificates [4].

2. Scope

The present document defines operational and managerial practices of the SwissSign Time-Stamping Authority (TSA) so that subscribers and relying parties may assess the trustworthiness of the time-stamping services. The TSA policy requirements are compliant with the stipulations of Swiss Digital Signature Law and support qualified electronic signatures as defined by Swiss Digital Signature Law (ZertES) [5]. The SwissSign TSA policy is compliant with the Best practices Time-Stamp Policy (BTSP) according to ETSI EN 319 421 which is identified by the Object Identifier (OID) 0.4.0.2023.1.1.

The SwissSign time-stamping services may be applied to a SwissSign digital signature or to any application requiring positive proof of the existence of digital data at a particular point in time.

These policy requirements are based on public-key cryptography, public-key certificates (X.509), and reliable time sources.

The present document, in conjunction with the above mentioned SwissSign policy documents, may be used by independent bodies to assess the trustworthiness of this TSA and its time-stamping services.

3. References

The applicable policy documents may be obtained in their most up-to-date form at: https://repository.swisssign.com/

Reference	Document Title	Description
[1]	SwissSign CP QCP-l-qscd	Certificate Policy for Regulated Seal certificates (i.e. the TSA certificates) OID: 2.16.756.1.89.2.1.24
[2]	SwissSign CPS Signing Services	Certification Practice Statement for Signing certificates
[3]	SwissSign TSPS	Trust Services Practice Statement
[4]	SwissSign CPR Sign	Certificate, CRL and OCSP Profiles for Signing certificates
[5]	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur	ZertES; SR 943.03
[6]	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur	VZertES; SR 943.032
[7]	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur	TAV Bakom; SR 943.032.1
[8]	General Policy Requirements for Trust Service Providers	ETSI EN 319 401
[9]	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements	ETSI EN 319 411-1
[10]	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates	ETSI EN 319 411-2
[11]	Certificate Profiles; Part 1: Overview and common data structures	ETSI EN 319 412-1
[12]	Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons	ETSI EN 319 412-3
[13]	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps	ETSI EN 319 421
[14]	Time-stamping protocol and time-stamp token profiles	ETSI EN 319 422
[15]	Cryptographic Suites	ETSI TS 119 312
[16]	CMS Advanced Electronic Signatures	ETSI TS 101.733

[17]	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	RFC 3161
[18]	Electronic Signature Formats for long term electronic signatures	RFC 5126
[19]	Regulation (EU) No 910/2014 of European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. (eIDAS regulation)	eIDAS - Regulation (EU) No 910/2014
[20]	TSA – Subscriber Agreement	
[21]	TSA PKI Disclosure Statement Time Stamp Service	

4. Definitions and Abbreviations

4.1 Definitions

Additional definitions are provided in the SwissSign TSPS [3].

Term	Description
Relying Party	A Party relying on a time-stamp provided by the SwissSign TSA.
Subscriber	Individuals using the time-stamp services provided by a TSA and agreeing explicitly to its terms and conditions.
Time-stamp policy	Rules applied by the TSA, when generating a time-stamp token.
Time-stamp token	Data object that binds the existence of digital data to a particular time. This serves as positive proof that certain data existed at this particular time.
Time-stamping Authority (TSA)	Authority which issues time-stamp tokens.
TSA Disclosure Statement	Policies and practices of a TSA that require particular emphasis or disclosure to subscribers and relying parties.
TSA Practice Statement	Statement of the practices that a TSA employs in issuing timestamp tokens.
TSA system	IT Infrastructure to support the provision of time-stamping services Time-stamping unit Hardware and software components which are managed as a unit to provide time-stamp tokens from a single time source. Components may be cloned or implemented redundantly for high availability reasons.
Coordinated Universal Time	Mean solar time at the prime meridian (0°). The time scale is Time (UTC) based on the second, as defined in ETSI EN 319 421 [10] and in ITU-R Recommendation TF.460-5.
UTC(k)	Time scale realized by a laboratory “k” in close agreement with UTC, with the goal to reach ±100 ns.

4.2 Abbreviations

Additional abbreviations are provided in the SwissSign TSPS [3].

Abbreviation	Description
BIPM	International Bureau of Weights and Measures (Bureau international des poids et mesures)
BSTP	Best practices Time-Stamp Policy (according to ETSI EN 319 421)
GMT	Greenwich Mean Time
IERS	International Earth Rotation Service
OID	Object IDentifier
TAI	International Atomic Time (Temps atomique international)
TSA	Time-Stamping Authority
TST	Time-Stamp Token
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

5. General Concepts

5.1 Time-Stamping Services

The time-stamping services includes two components:

- Time-stamping provision: The technical component generating time-stamp tokens.
- Time-stamping management: The service component that monitors and controls the operation of the time-stamping services. The time-stamping management guarantees that the clock used in time-stamping is correctly synchronized with UTC

5.2 Time-Stamping Authority

The SwissSign TSA issues secure time-stamp tokens (TST) for users of the time-stamping services (i.e. Subscribers as well as Relying Parties).

The SwissSign TSA assumes the overall responsibility for the provision of the time-stamping services identified in chapter 5.1. The SwissSign TSA may operate several identifiable time-stamping units (TSU's) and each TSU must have a different key (see chapter 8.3.1). Each TSU has a single time-stamp signing key active.

Within a TSU it is permissible to clone key material and to use redundant components to meet high availability requirements.

The SwissSign TSA is identified in the digital certificate used for the time-stamping services.

The Certificate Profile can be found in the document SwissSign CPR Sign – Certificate, CRL and OCSP Profiles for Signing certificates [4]. It is compliant with ETSI EN 319 412-3 and is compliant with ETSI EN 319 422 chapter 6.

5.3 Subscriber

The subscriber may be an organization or a single individual end-user.

If the subscriber is an organization, the obligations that apply to that organization also apply to its associated end-users. In any case, the organization will be held responsible if the obligations are not correctly fulfilled by the end-users; therefore, such an organization must suitably inform its end-users.

If the subscriber is an individual end-user, the end-user will be held directly responsible for the fulfillment of the obligations.

5.4 Time-Stamp Policy and TSA Practice Statement

5.4.1. Purpose

The time-stamp policy and time-stamp practice statement are defined as follows:

- TSA Policy states the issues that “must be adhered to”. Included are the rules and processes applied by the TSA when generating a time-stamp token.
- TSA Practice Statement is a declaration of “how the time-stamping service is implemented to meet the policy requirements”.
- Complementary to the processes described in the SwissSign Certification Practice Statement for Signing certificates [2], this TSA policy describes time-stamping specific processes and policies.

5.4.2. Level of Specificity

The TSA policy specifies the processes used to provide time-stamping services, adequately extending the processes which are described in the SwissSign Certification Practice Statement for Signing certificates [2].

5.4.3. Approach

The TSA Policy will focus on general processes. Technical details, such as organizational structure, operating procedures, and communication infrastructure are specified in the SwissSign Certification Practice Statement for Signing certificates [2] or additional internal documents. Internal documents are not publicly available.

6. Time-Stamp Policies

6.1 Overview

This TSA policy comprises a set of rules and processes to be used for issuing trustworthy time-stamp tokens in accordance with Swiss Digital Signature Law (ZertES) and, in particular, the rules of ETSI EN 319 421 [13].

6.2 Identification

This document is named ”SwissSign Time-Stamping Policy” as indicated on the cover page of this document.

This OID is referenced in every time-stamp issued by this TSA.

6.3 User Community and Applicability

The SwissSign AG time-stamping services meet the requirements of time-stamping qualified signatures in accordance with Swiss Digital Signature Law (ZertES) [5].

Users of this time-stamping service are only Subscribers and Relying Parties of a SwissSign digital certificate. No other restrictions are imposed. The SwissSign time-stamps may be applied to any applications requiring positive proof that certain data existed before a particular point in time.

6.4 Conformance

SwissSign AG includes a policy identifier (OID) (see chapter 6.2) in all time-stamp tokens issued by this TSA.

The conformance to this time-stamp policy is subject to periodic independent internal and external assessments.

SwissSign AG meets the obligations defined in chapter 7.1 and ensures the implementation of appropriate controls as specified in chapter 8.

7. Obligations and Liability

7.1 TSA Obligations

7.1.1. General

The SwissSign TSA ensures conformance with the requirements prescribed in this TSA policy and provides all time-stamping services in accordance with:

- the rules set forth in the SwissSign policy documents, i.e.
  - SwissSign Certificate Policy for the TSA certificates [1],
  - SwissSign CPS Signing Services [2],
  - SwissSign Trust Services Practice Statement (TSPS) [3],
  - Certificate, CRL and OCSP Profiles for Signing certificates [4]
- the stipulations of ZertES and
- the regulations of TAV-ZertES [7].

This TSA Policy and the SwissSign policy documents are an integral part of the agreements between SwissSign AG, the Subscribers, and the Relying Parties.

7.1.2. TSA Obligations towards Subscribers

The SwissSign TSA guarantees that time-stamp tokens are issued in accordance with the following:

- The TSA operates in accordance with all relevant regulations, especially those stipulated and defined by the Swiss Digital Signature Law.
- The time-stamping unit (TSU) is in accordance with a minimum UTS time accuracy of +/- 1 second.
- SwissSign AG undertakes periodic independent internal and external assessments of its compliance with Swiss Digital Signature Law (ZertES).
- The SwissSign TSA provides a time-stamping service of high availability backed up by redundant infrastructure. The availability is guaranteed as long as none of the following occur: planned technical interruptions, natural disasters, wars, acts of terrorism, strikes, failures of the Internet or other causes of interruption as stipulated in the SwissSign Trust Services Practice Statement (TSPS) [3] in chapter 9.

7.2 Subscriber Obligations

The subscriber shall accept the “End-User Agreement for SwissSign Platinum TSA”, before using the Timestamp Service of SwissSign AG.

The subscriber shall use the Time-stamping service only in compliance with chapter 4 of ETSI 319 422 “Requirements for a TSP client”.

The subscriber shall verify that the time-stamp token has been correctly signed by the time-stamp authority and that the private key used to sign the time-stamp token has not been revoked.

7.3 Relying Party Obligations

When relying on a time-stamp token, the Relying Party shall verify that the time-stamp token was correctly signed and that the private key used to sign the time-stamp token has not been revoked.

During the validity period of the TSU's certificate, the validity of the signing key can be verified on the SwissSign CRL.

If the verification takes place after expiry of the certificate's validity period, the relying party shall check whether the employed hash function, algorithms, and cryptographic key lengths can still be deemed secure.

For further terms and conditions applicable to Relying Parties, refer to the TSA Disclosure Statement in chapter 8.1.2 and to other agreements between the parties.

7.4 Liability

SwissSign AG operates its TSA in accordance with this TSP, SwissSign policy documents and the terms of other binding agreements between SwissSign AG and the TSA service users. SwissSign AG endeavors to provide high availability of its services, but makes no express or implied representations or warranties to uninterrupted services or accuracy of the time-stamp services.

SwissSign AG is only liable for damages to Subscribers or Relying Parties that result from SwissSign's failure to comply with Swiss Digital Signature Law (Article 17 ZertES). SwissSign AG must supply evidence that they have adhered to applicable laws, rules, and regulations.

SwissSign AG shall in no event be liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law. SwissSign AG shall not be liable for any damages resulting from infringements by the Subscriber or the Relying Party on the applicable terms and conditions, including the exceeding of the transaction limit.

SwissSign AG shall under no circumstances be liable for damages that result from force majeure events as detailed in chapter 7.1.2. of this TSA Policy and in chapter 9.16.5 in SwissSign Trust Services Practice Statement (TSPS) [3]. SwissSign AG shall take commercially reasonable measures to mitigate the effects of force majeure in due time. Any damages resulting from any delay caused by force majeure will not be covered by SwissSign AG.

The detailed liability limitations applicable to the parties are specified in the SwissSign Certificate Policy for the TSA certificates [1], SwissSign CPS Signing Services [2] and the

SwissSign Trust Services Practice Statement (TSPS) [3], each in chapter 9.

8. Requirements on TSA Practices

The TSA operates its services in accordance with the rules established in this TSP, the SwissSign policy documents and additional internal documents defining technical, operational and procedural requirements.

It is in the sole discretion of SwissSign AG to provide the TSA services to a Requester.

8.1 Practice and Disclosure Statement

8.1.1. TSA Practice Statement

The TSA practice statement defines how SwissSign AG is to adhere to the relevant requirements, identified in the SwissSign policy documents and internal documents.

The defined procedures and their correct implementation by SwissSign AG are audited by the official auditors of SwissSign in accordance with the Swiss Digital Signature Law (ZertES) [5].

This TSA Practice Statement and other relevant documentation will be published on: http://repository.swisssign.com.

The TSA Disclosure Statement is included in chapter 8.1.2 of this TSA policy document. Internal documents are not to be published.

Amendments to this TSA Practice or other published documents are implemented according to the provisions set forth in the SwissSign Certificate Policy for the TSA certificates [1], SwissSign CPS Signing Services [2] and the SwissSign Trust Services Practice Statement (TSPS) [3], each in chapter 9.12.

8.1.2. TSA Disclosure Statement

The terms and conditions, set forth herein, are binding to all Subscribers and Relying Parties using

SwissSign time-stamping services. Other documents, which form integral part of this TSP, such as the SwissSign policy documents can be found on the SwissSign website http://repository.swisssign.com/.

- The SwissSign TSA is a service of SwissSign AG, certified under Swiss Digital Signature Law ZertES as a qualified certification service provider.
- For contact information, refer to SwissSign CPS Signing Services [2] chapter 1.5.2 (Contact persons).
- Each time-stamping token issued by SwissSign Time-stamping service includes the policy objectidentifier defined in chapter 6.2 (Identification).
- The cryptographic algorithms employed and the length of cryptographic keys are as follows:
    - Hash-algorithms: SHA-2, i.e.
        - SHA256 (OID: 2 16 840 1 101 3 4 2 1) and
        - SHA512 (OID: 2 16 840 1 101 3 4 2 3)
    - signing algorithm:
        - sha256WithRSAEncryption(OID: 1 2 840 113549 1 1 11)
        - with at least 2048 bit key length
- These algorithms are supported in accordance with TAV-ZertES [7] and ETSI TS 119 312 [15].The cryptographic algorithms are chosen according to ETSI EN 319 321 [13] and ETSI TS 119 312 [15].
- The TSA ensures time accuracy compliant with the minimum UTC time accuracy standards of +/- 1 second. The SwissSign TSA will not issue time-stamp tokens if the time accuracy is no longer secured.
- The SwissSign time-stamping service may be limited to Subscribers of a valid SwissSign AG qualified digital certificate.
- Subscriber obligations are described in chapter 7.2 (Subscriber Obligations) of this document.
- The use of the following fields in the time-stamping request is supported:
    - the reqPolicy;
    - the nonce; and
    - the certReq
- The following fields are present in the time-stamping answer:
    - the reqPolicy;
    - the nonce; and
    - the certReq

- A Relying Party's obligations and information on how Relying Party can verify the trustworthiness of the TST are described in chapter 7.3 (Relying Party Obligations) of this document.
- SwissSign AG may oblige Subscribers and Relying Parties to comply with additional End-User Agreements that are compliant with Swiss Digital Signature Law ZertES and the SwissSign policy documents to the extent permitted by Swiss law.
- SwissSign AG may charge fees for the services offered by SwissSign TSA.
- SwissSign AG maintains records on the operations of the SwissSign TSA, in accordance with chapter 5.4 (Audit logging procedures) of the SwissSign Trust Services Practice Statement (TSPS) [3].
- SwissSign AG is only liable for damages to Subscribers and Relying Parties in connection with valid SwissSign qualified certificates relied upon in accordance with Swiss Digital Signature Law. The limitations of liability are defined in chapter 7.4 of this document, in the respective chapter 9 of the SwissSign Certificate Policy for the TSA certificates [1], SwissSign CPS Signing Services [2] and the SwissSign Trust Services Practice Statement (TSPS) [3]and other service agreements with users.
- The laws of Switzerland shall govern this time-stamping service. The details on applicable law and dispute resolution procedures related to the SwissSign TSA are defined in the respective chapter 9 of the SwissSign Certificate Policy for the TSA certificates [1], SwissSign CPS Signing Services [2] and the SwissSign Trust Services Practice Statement (TSPS) [3] and in other applicable agreements.

The SwissSign AG TSA conformity with applicable laws and regulations is assessed by the auditors of SwissSign according to Swiss Digital Signatures Law (ZertES) .

8.2 Key Management Life Cycle

8.2.1. TSA Key Generation

SwissSign AG generates the cryptographic keys in a physically secured environment by personnel in trusted roles. Algorithms, the resulting key length and signature algorithms are described in chapter 8.1.2. of this document.

The SwissSign TSA keys are generated obeying the same procedures and at the same time as are the keys for SwissSign Signing Services CAs.

The key management life cycle of the TSA keys is identical to that of the subsidiary CA's of SwissSign AG. Specific documentation can be found in chapter 6 in the SwissSign Trust Services Practice Statement (TSPS) [3].

8.2.2. TSU Private Key Protection

The SwissSign TSA ensures that the confidentiality and integrity of their keys is maintained. In particular the HSM module meets the requirements of FIPS 140-2 Level 3.

8.2.3. TSU Public Key Distribution

The SwissSign TSU certificate is issued with a level of security that is equivalent to the ones described for the SwissSign CA, more details are defined in SwissSign CPS Signing Services [2]. The signed timestamp tokens are provided with the TSU certificate attached. In addition, relevant information can be found on the SwissSign ldap directory and the SwissSign web sites, see also chapter 6 of the SwissSign CPS Signing Services [2].

8.2.4. Re-keying TSU's Key

The SwissSign TSA keys shall be replaced on a yearly basis. In addition, they shall be replaced before the expiration of their validity period, if the chosen algorithm, key length or other relevant security measures are no longer state-of-the-art.

8.2.5. End of TSU Key Life Cycle

The SwissSign TSA ensures that the private keys are not used beyond their expiration date. Time-stamps cannot be issued with expired private keys. Expired keys are destroyed as described in SwissSign CPS Signing Services [2] chapter 6.

8.2.6. Life Cycle Management of the Cryptographic Module Used to Sign Time-Stamps

SwissSign AG has established procedures to ensure that hardware security modules for non-repudiation services are not tampered with during shipment and storage. Installation and activation of signing keys in cryptographic hardware is performed only by personnel in trusted roles. Additional internal documentation describes the handling and procedures of HSM. The SSCD life cycle management is described in the SwissSign CPS Signing Services [2] chapter 6.

8.3 Time-Stamping

8.3.1. Time-Stamp Token

SwissSign TSA issues time-stamp tokens in accordance with RFC 3161 [17].

The TST includes[1]

Field/shortname	Explanation
policy	The TST includes an identifier for the Time-stamping Policy.
genTime	The time at which the time-stamp token has been created by the TSA
Accuracy	The accuracy of the included time (genTime) in milliseconds
tsa	The TST includes an identifier for the TSA and TSU.
messageImprint	The TST shall include a representation (i.e. hash value) of the digital data being time-stamped.
signature	The TST shall include the digital signature of the SwissSign TSA.

The TST does not include:

- Ordering Field
- extensions

In particular, the TST practices follows the principles below:

- The date and time can be traced to UTC-defined reliable time source.
- The time included in the TST shall be synchronized with the UTC within the accuracy of +/- 1 second.
- If the SwissSign time-stamp clock is not within the stated accuracy no TST shall be issued.
- The TST is signed using a key exclusively for the purposes of time-stamping.
- The TSU issues time-stamps only after its signature verification (public key) certificate is loaded into the TSU. The TSA verifies that the obtained signature verification (public key) certificate is correctly signed.
- The time-stamp generation system rejects any attempt to issue time-stamps when the end of the validity of the TSU private key has been reached.

8.3.2. Clock Synchronization with UTC

The SwissSign TSA uses its own network time server, which is synchronized with three independent time sources to achieve synchronization with UTC within the declared accuracy of +/-1 second.

Controls are in place to detect changes in clock calibration and/or synchronization problems that threaten to compromise the declared accuracy.

The TSA ensures correct handling of leap seconds during the last minute of the day when the leap second is scheduled to occur.

[1] Please note: Not all fields mandatory according to RFC 3166 section 2.4.2 are listed.

8.4 TSA Management and Operation

8.4.1. Security Management

The SwissSign TSA security management is described in the respective chapter 5 and 6 of SwissSign Certificate Policy for the TSA certificates [1], SwissSign CPS Signing Services [2] and the SwissSign Trust Services Practice Statement (TSPS) [3].

8.4.2. Asset Classification and Management

The SwissSign TSA ensures that information and other assets receive appropriate security treatment as defined in the respective chapter 5 and 6 of SwissSign Certificate Policy for the TSA certificates [1], SwissSign CPS Signing Services [2] and the SwissSign Trust Services Practice Statement (TSPS) [3].

8.4.3. Personnel Security

The personnel security controls of the SwissSign TSA are defined in SwissSign Trust Services Practice Statement (TSPS) [3] chapter 5.3.

8.4.4. Physical and Environmental Security

SwissSign AG ensures the physical and environmental security of its TSA as defined in SwissSign Trust Services Practice Statement (TSPS) [3] chapter 5.1.

8.4.5. Operations Management

The SwissSign TSA maintains adequate operational controls in compliance with ETSI EN 319 421 . These documents and policies are internal and not publicly available and are periodically assessed by internal and external reviews to ensure compliance and effectiveness of these controls.

8.4.6. System Access Management

SwissSign TSA has adequate access controls in place as defined in the SwissSign Trust Services Practice Statement (TSPS) [3] chapter 5.

8.4.7. Trustworthy Systems Deployment and Maintenance

The TSA keys and its services are produced in a trustworthy environment. The systems and products used by SwissSign AG to provide adequate services are in accordance with the required levels of assurance. SwissSign AG ensures to undertake adequate analysis of security requirements and has respective changecontrol procedures in place.

8.4.8. Compromise of TSA Service

In the case of a compromise of a private key of the TSA service of SwissSign AG the procedures defined in SwissSign Trust Services Practice Statement (TSPS) [3] chapter 5.7 will be executed. No time-stamp tokens will be issued if the TSA private key is compromised. If the required accuracy of the minimum UTC time accuracy of +/- 1 second is compromised, no time-stamp tokens will be issued until the calibration is restored. In case that timestamps have been issued without the required minimum accuracy the according period is evaluated and included in the relevant information as described below. In case of a key compromise of the TSA Unit a procedure is elaborated and all timestamps or affected hashes that have been signed legitimately by the compromised key will be published by SwissSign in order to provide a means of validation.

Relevant information is made available to Subscriber and Relying Parties on the SwissSign web page. Additionally, the subscribers will be informed by e-mail as soon as possible.

8.4.9. TSA Termination

The termination of the SwissSign TSA is handled according to the procedures defined for SwissSign CA termination in the SwissSign Trust Services Practice Statement (TSPS) [3] chapter 5.8.

8.4.10. Compliance with Legal Requirements

The SwissSign TSA services complies with the requirements of the Swiss Digital Signature Law (ZertES) and other relevant rules and regulations. SwissSign AG ensures that adequate measures are taken against unauthorized or unlawful processing of personal

data. SwissSign AG also ensures complete confidentiality of personal data and other information contributed by users to the TSA unless permitted by written agreement, by law, or by court order in accordance with applicable Data Protection Law.

8.4.11. Recording of Information Concerning Operation of Time-Stamping Services

Records concerning the operation of the time-stamping service are written and safeguarded in the same manner as records concerning the SwissSign AG Certificate Authority operation. The respective controls ensure integrity, confidentiality and the required archiving of all records as stipulated in the SwissSign policy documents.

SwissSign AG ensures that adequate measures are taken against unauthorized or unlawful processing of its records unless permitted by written agreement, by law or by court order in accordance with applicable Data Protection Law.

Record logging of life cycle management events of the SwissSign TSA keys is performed in the same manner as it is with the keys of the SwissSign Signature Services issuing CAs. The CA life cycle management is described in the SwissSign Trust Services Practice Statement (TSPS) [3] in chapter 4.

The TSA also logs relevant events related to clock synchronization in its TSU including synchronization of a TSU's clock to UTC as well as events relating to detection of loss of synchronization.

8.5 Organizational

The organization that maintains the SwissSign TSA is the same one that maintains the subsidiary CAs of the SwissSign Signing Services CAs. The organizational, technical, and personal security measures are defined in the SwissSign Trust Services Practice Statement (TSPS) [3] and in accordance with relevant other laws and regulations as defined in this TSP.