Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF

Federal Office of Information Technology, Systems and Telecommunication FOITT
PS/IDTR/TRB
SG-PKI

October 14, 2025

Swiss Government PKI

Time Stamping Authority - Policy

Version	V1.65		
Autor:	WeJ/EnCo		
Status:	In progress	Under review	Approved for use
			x

Persons involved	
Author:	Tomaso Vasella, Jürgen Weber
Editing:	Cornelia Enke, Hans W. Kramer
Review:	Hans Kramer, Marcel Suter, Pascal Joye
Approval:	PKI Management Board

Change control, review, approval			
When:	**Version:**	**Who:**	**Description:**
July 21, 2006	X0.8	Tomaso Vasella	Version for BIT
Aug 20, 2006	X0.9	Robert Dietschi	Update
Mar 13, 2007	V1.0	Robert Dietschi	Approval
Feb 13, 2008	V1.1	Tomaso Vasella	Update
Feb 15, 2008	V1.1	Jürgen Weber	Approval
May 21, 2013	V1.2	Jürgen Weber	Update
Dec. 3, 2013	V1.3	Jürgen Weber	Update to section 6.2.4 following re-keying
Sep 27 2018	V1.4	Jürgen Weber, Cornelia Enke	Update, addition of changes to legal requirements – revision of ZertES
Feb 25, 2019	V1.41	Cornelia Enke	Inclusion of supported parameters for TSA request and TSA response Chapter 6.3.1
May 7, 2019	V1.5	Cornelia Enke	Issuance of the new TSA service certificate, documentation in this document, and approval of the TSA policy.
Aug. 16 2019	V1.6	Cornelia Enke	Review, addition of requirement in accordance with ETSI EN 319 411-1 Rev 6.3-10
May 6 2020	V1.61	Cornelia Enke	Review, addition 4AP for TSA key operations.
Aug 31 2021	V1.62	Cornelia Enke	Addition of policy conformance for BTSP included.

Change control, review, approval			
Apr. 26, 2023	V1.63	Hans W. Kramer	Annual review and adjustments.
May 3, 2023	V1.64	Pascal Joye	Review
Oct 14 2025	V1.65	Cornelia Enke	Review and corrections in accordance with the Improvementregister translated to english

Approval			
When:	**Version:**	**Signature**	**Signature**
10/14/2025	V1.65	Roth Beat 0RQGGW 14.10.2025 Info: admin.ch/esignature | validator.ch Trust Product Manager Beat Roth	Zuercher Roger UXJMSB 15.10.2025 Info: admin.ch/esignature | validator.ch Trust Business Owner Roger Zürcher

Table of contents

Referenced Documents

Ref	Description
[1]	ETSI EN 319 421 V1.3.1 (2025-07) Policy and Security Requirements for Trust Service Providers issuing Time-Stamps https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.03.01_60/en_319421v010301p.pdf
[2]	ETSI EN 319 422 V1.1.1 (2016-03), Time-stamping protocol and time-stamp token Profiles https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf
[3]	IETF RFC 3126, Electronic Signature Formats for long term electronic signatures, September 2001. https://www.ietf.org/rfc/rfc3126.txt
[4]	Federal Act on Certification Services in the Field of Electronic Signatures (Federal Act on Electronic Signatures, ZertES), 943.03 https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/2016/752/20200101/de/pdf-a/fedlex-data-admin-ch-eli-cc-2016-752-20200101-de-pdf-a-1.pdf
[5]	CPS of the Swiss Government PKI Root CA IV http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf
[6]	ETSI TS 119 312 V1.5.1 (2024-12) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.05.01_60/ts_119312v010501p.pdf
[7]	TAV: Technical and Administrative Regulations on Certification Services in the Field of Electronic Signatures, TAV Bakom; SR 943.032.1 August 20, 2025) https://www.bakom.admin.ch/dam/de/sd-web/Y1ItViDHdlxR/TAV%202025_dt_definitive%20pour%20signature.pdf
[8]	IEFT RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001 https://www.ietf.org/rfc/rfc3161.txt
[9]	IETF RFC 5816 ESSCertIDv2 Update for RFC 3161 https://www.ietf.org/rfc/rfc5816.txt

Abbreviations used

Abbreviation	Meaning
BIT	Federal Office of Information Technology, Systems and Telecommunication
BTSP	Best practices for time-stamp policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
GPS	Global Positioning System

Abbreviation	*Meaning*
HTTP	Hypertext Transfer Protocol
NTP	Network Time Protocol
OID	Object Identifier
RFC	Request for Comments
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest Shamir Adleman Algorithm
SHA	Secure Hash Algorithm
TAV	Technical and administrative regulations on certification services in the field of electronic signatures
TSA	Time Stamping Authority
TSU	Time Stamping Unit
UTC	Coordinated Universal Time
ZertES	Federal Act on Electronic Signatures

1 Introduction

. This time stamping service can be used to reliably and verifiably prove the existence of digital data at a specific point in time. Time-stamped data cannot be altered without detection.

To do this, the hash value of the data to be stamped is sent to the time stamping service. The time stamping service generates a time stamp object (token) that contains the hash value and the current time. This object is digitally signed by the time stamping service to protect its integrity.

This document describes the Time Stamping Authority Policy (hereinafter TSA Policy) of the Swiss Government PKI time stamping service. The TSA Policy specifies general processes used by the time stamping service when creating signed time stamps.

The detailed controls of the processes can be found in the respectively Certification Practice Statement CPS.

The structure and content of this policy are based on ETSI EN 319 421.

2 Scope

This document describes the services provided by the TSA of the Swiss Government PKI, as well as the associated operational and management processes. This allows recipients or users of time stamp objects (relying parties) and users of the time stamp service (subscribers) to assess the trustworthiness of the Swiss Government PKI's time stamp service.

The requirements for the time stamp service for electronic signatures are set out in the Swiss Electronic Signature Act (ZertES). However, the time stamp service can also be used for all other applications that require proof of the existence of data at a specific point in time.

3 General concepts

3.1 Time stamp service

Time stamp service consist of the following components:

- Technical components that creates the time stamp objects (tokens)
- Management of time stamp objects
  This component monitors and controls timestamp operations, including synchronization with a UTC reference time source.
- The time stamp service complies with the guidelines and security requirements for trust service providers that issue qualified time stamps, as defined in ETSI EN 319 421 and ETSI EN 319 411-1.

3.2 NTP services BIT

The BIT maintains a NTP (Network Time Protocol) infrastructure to provide PKI customers with accurate time for their services/applications.

The BIT provides a Stratum 1 and a Stratum 2 environment in its computer centers.
The Stratum 1 environment consists of three time servers, each connected to a radio antenna, a GPS antenna, and a multiband antenna (satellite antennas).

The two time servers with satellite antennas are connected to a rubidium oscillator at their respective locations. The rubidium module is connected to the reference signal of the associated server housing and is controlled by this signal as long as the upstream system is in a synchronized state.

If the reference clock loses its synchronization source, the rubidium module provides the sync reference for the system based on its holdover performance.

The Stratum 2 environment consists of four time servers each, which synchronize their time with the three Stratum 1 servers and with the official Swiss time servers from Metas.

The two data centers are completely location-independent and provide the time for the client systems at the respective locations.

3.3 NTP implementation at BIT

(Detailed information available upon request.)

3.4 Time stamp authority

The BIT Time Stamping Authority (TSA) generates qualified time stamps**.** Qualified time stamps are a special type of electronic time stamp. These time stamps provide legally binding proof of exactly when a digital document or file was created or modified.

The TSA of the BIT:

- proves the time at which a document existed,
- is provided with a digital signature so that it cannot be manipulated retrospectively.
- is issued by the SG-PKI as an officially recognized and certified trust service provider,
- is considered a qualified timestamp as evidence in court – similar to a notary stamp.

The TSA comprises the technical and organizational components for ensuring the time stamping service as well as the information and communication infrastructure.

3.5 Users (subscribers)

Time stamp service users can be legal entities (organizations) or natural persons. Time stamp service users are responsible for the correct use of time stamp service.

3.6 TSA Policy and Practice Statement

3.6.1 Purpose

The Time Stamping Policy defines "what must be complied with," while the Time Stamping Practice Statement defines "how it is complied with." This chapter covers the Time Stamping Policy (TSA Policy), which describes the general requirements that the Swiss Government PKI time stamping service must meet. The Time Stamping Practice Statement is defined in Chapter 6.1.

3.6.2 Level of detail

The TSA Policy specifies general processes used by the time stamp service during the creation of signed time stamps. The TSA Policy, together with the respectively CPS, provides an overview of the trustworthiness of the TSA service.
More detailed specifications of these processes are described in the Certification Practice Statement CPS of the Swiss Government PKI Root CA IV.

3.6.3 Procedure

This policy specifies general processes. It does not describe technical details relating to the information and communication infrastructure, the operational organization, or protective measures.

It does not describe the environment in which the time stamp service is operated. The relevant technical and operational details are described in the respectively CPS.

4 TSA Policy

4.1 Overview

This TSA Policy is a compilation of processes used for the trustworthy generation and management of time stamp objects and as a guideline for the security level of the TSA.

General rules are described in the chapter 3.6TSA Policy and Practice Statement in this document.

Time stamp objects are issued with an accuracy of 1 second or better. They can be requested via an HTTP interface.

Each time stamp object contains the identifier of this policy.

4.2 Identifier

The identifier (Object Identifier, OID) of this policy is: **2.16.756.1.17.3.5.2.4**

4.3 Applicability

This policy is designed to ensure that the time stamp service complies with the legal requirements for qualified digital signatures (ZertES).

4.4 Compliance

Created timestamp objects contain the identifier described in the chapter 4.2 Identifier.

The TSA ensures compliance with the regulations during the performance of the services described in the chapter 5.1Obligations of the TSA. Furthermore, the TSA ensures the reliability of the control mechanisms described in the chapter 6TSA processes.

5 Obligations and liability

5.1 Obligations of the TSA

5.1.1 General obligations

This chapter contains all obligations, liabilities, guarantees, and responsibilities of the TSA and its timestamp service users. The obligations and responsibilities are accepted by using the TSA service.

As a TSA, the Swiss Government PKI undertakes to perform all tasks described in this TSA Policy and in the respectively CPS for the implementation of the requirements of the ZertES and the further implementing provisions.

The CPS and the TSA Policy are an integral part of the agreement between the Swiss Government PKI and the time stamp service users.

Swiss Government PKI guarantees that all requirements for the TSA, including the processes and procedures relating to the issuance of time stamp objects, system reviews, and security audits, are complied with in accordance with the processes described in Chapter 6TSA processes.

The configuration of the TSP systems is regularly reviewed for compliance with applicable legal and regulatory requirements. The maximum time between two reviews is one year.

5.1.2 TSA obligations towards time stamp users

The Swiss Government PKI grants permanent access to the Swiss Government PKI time stamp service refer to chapter 5.3.

Planned service restrictions will be announced on the Swiss Government PKI website.

Furthermore, Swiss Government PKI guarantees the following:

- Establishment and operation of a reliable information and communication infrastructure.
- Compliance with property rights, licenses, or similar laws.
- The services offered comply with generally accepted standards as described in Chapter 4.1Overview in this document.
- The timestamp objects issued are correct.
- The accuracy in relation to UTC time is ±1 second or better. The accuracy estimated by the NTP daemon of the TSA server is output in the accuracy field in accordance with RFC 3161 - 2.4.2. Response Format. If the accuracy is worse than ±1 second, an error message is output in accordance with RFC 3161 - 2.4.2. Response Format. This corresponds to ETSI EN 319 421 - OVR-5.1-03 and ETSI 319 422 – 4.2.2 Fields to be supported.

5.2 Obligations of the time stamp service user

The time stamp service user is obliged to check the validity and duration of validity of the CA certificate and the TSA signature certificate. If the time stamp is checked after the validity of the TSA signature certificate has expired, the time stamp service user must do the following:

- Check whether the serial number of the TSA signature certificate has been included in the CRL
- Check whether the hash function specified in the time stamp object is still secure
- Check whether the length of the TSA's cryptographic keys and the algorithms used are still considered secure

The information about the issuing CA and the access points for status verification is contained in the timestamp certificate itself and specifies the source of this information.

5.3 Guarantee

The Swiss Government PKI is responsible to time stamp service users for the careful and contractual provision of the agreed services, except in the event of planned technical interruptions and in the absence of an accurate time base, force majeure, natural events, acts of

war, strikes, unforeseeable official restrictions, and hacker attacks or virus infections (including Trojan horses and similar) affecting the user of the time stamp service.

5.4 Liability

In accordance with Art. 17 ZertES, the Swiss Government PKI is liable to the holder of the signature key and third parties who have relied on a valid qualified timestamp for any damage they suffer if the Swiss Government PKI has failed to fulfill its obligations under the Signature Act and the implementing regulations. The Swiss Government PKI bears the burden of proof for having fulfilled its obligations under the ZertES and the implementing provisions.

The Swiss Government PKI is not liable for damages resulting from non-compliance with or exceeding a restriction when using the time stamp (in accordance with Art. 7 para. 3 ZertES and Art. 17 para. 3 ZertES).

In all other cases, the Swiss Government PKI shall be liable as follows:

- In the event of breaches of the agreement, for the proven damage, unless it can prove that it is not at fault.
- Damages caused intentionally or through gross negligence will be compensated without limitation.
- In the case of slight negligence, liability for financial losses shall be limited to the equivalent of the services agreed during the current contract year, up to a maximum of CHF 50,000 per claim and calendar year.

Under no circumstances shall Swiss Government PKI be liable for consequential damages, lost profits, or data loss.

6 TSA processes

The controls implemented for the operation of the TSA are described in the CPS of the Swiss Government PKI Root CA IV, Chapter 5, Infrastructural, organizational, and personnel security measures.

6.1 TSA processes and declarations

6.1.1 TSA processes (TSA Practice Statement)

- Procedures, control mechanisms, and technical infrastructure to ensure a controlled, uninterrupted, and reliable service form the basis for TSA operation. The detailed controls are described in the CPS of the Swiss Government PKI Root CA IV, Chapter 6.6, Life Cycle of Security Measures.
- The CPS of the Swiss Government PKI Root CA IV defines the rules for the operation of the time stamp service, together with other internal documents.
- Minor changes with no or minimal impact on users are implemented directly by the Swiss Government PKI. Major changes are implemented in consultation with the recognition authority and after approval by the recognition authority.

Changes are recorded in a journal. All users will be announced by publishing the respectively information on the official Swiss Government PKI website.

There is a formal approval procedure for this TSA policy and any changes thereto.

6.1.2 TSA declarations

- Contact information for the time stamp service is contained in the CPS of the Swiss Government PKI Root CA IV Chapter 1.5.2 Contact Person.
- Each time stamp object issued by the Swiss Government PKI time stamp service contains the policy identifier as described in chapter4.2Identifier.
- The cryptographic algorithms used and their key lengths are based on the publications referenced in the TAV of ETSI EN 119 312. At the time of writing, these are:
    - Hash algorithms
        - SHA-256 (OID: 2.16.840.1.101.3.4.2.1)
        - SHA-384 (OID: 2.16.840.1.101.3.4.2.2)
        - SHA-512 (OID: 2.16.840.1.101.3.4.2.3)
    - Key length
        - 3072 bits
- Signature algorithm
    - sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
- The accuracy of the time used in the timestamp object is at least ± 1 second deviation from UTC (Universal Time Coordinated) time. If the time difference is greater, the service will be suspended.
- The obligations of timestamp service users are described in the chapter 5.2 Obligations of the time stamp service user.
- The obligations of timestamp object recipients are described in the chapter5.2 Obligations of the time stamp service user.
- Verification of timestamp objects is described in chapter 5.2 Obligations of the time stamp service user.
- Log data is stored and archived in accordance with Chapter 5.4 Security Monitoring of the CPS of the Swiss Government PKI Root CA IV.
- The Swiss Government PKI grants time stamp service users the right to pass this document on to third parties without modification. No further rights are granted.
  In particular, the distribution of modified versions and the transfer to other documents or publications is not permitted without the written consent of the Swiss Government PKI.
- The time stamp service is a service provided by the Swiss Government PKI, which is certified in accordance with the Swiss Electronic Signature Act (ZertES).
- The insurance coverage of Swiss Government PKI also extends to statutory liability claims for pure financial losses under Art. 17 ZertES within the scope of the Swiss Government PKI's terms of use, which are provided to the certificate holder. Costs incurred by the insured companies in the event of a possible cessation of business activities in accordance with Art. 14 ZertES are also insured. A combined sublimit of CHF 2 million per event and CHF 8 million per insurance year applies to the aforementioned damages and costs.
- All disputes arising from this TSA Policy in which Swiss Government PKI is involved shall be submitted for final decision to a three-member arbitration tribunal based in Bern in accordance with the provisions of the Concordat on Arbitration. The arbitral tribunal shall be

appointed by the President of the Commercial Court of the Canton of Bern. The proceedings before the arbitral tribunal shall be governed by the Civil Procedure Code of the Canton of Bern, unless the Concordat on Arbitration applies. The proceedings shall be conducted in German.
However, the contracting parties undertake to make every reasonable effort to settle the dispute amicably before referring it to the arbitration tribunal. To this end, they may engage the services of a mediator to be jointly appointed.
Such an attempt at mediation shall have no effect on statutory limitation periods.

- The TSA complies with this "Time Stamp Policy." The implementation and processes have been audited and certified by the certification body KPMG AG.

6.2 Life cycle of key management

6.2.1 Generation of the TSA key

TSA keys are generated in a hardware security module certified according to FIPS 140-2, Level 3 or CEN EN 419 221-5. The TSA signature certificate meets the requirements of ETSI EN 319 411 and is issued in accordance with RFC3161. The keys are generated by trusted personnel and trusted roles. The requirements for personnel are described in the CPS of the Swiss Government PKI Root CA IV, Chapter 5.3 Personnel Security Measures.
The approved TSA hash and encryption algorithms are described in Chapter 6.1.2TSA declarations.

6.2.2 Protection of the TSA private key

The HSM module used for certification meets the requirements of the TAV:

HSM: SafeNet Luna SA
- FIPS 140-2, Level 3

6.2.3 Distribution of the TSA public key

TSA certificates containing the public key are signed by the Swiss Government PKI CA. The publication of the certificates is described in the CPS of the Swiss Government PKI Root CA IV, Chapter 2.1 Directory Service.

6.2.4 Re-keying of the TSA key

The TSA signature certificate is reissued annually and signed by the Swiss Government Regulated CA 02.
The process for renewing the TSA signature certificate is logged. The TSA signature certificate that is no longer in use and the associated cryptographic key material is decommissioned. The renewal and decommissioning log is archived.

6.2.5 End of the TSA key lifecycle

The procedure for destroying TSA keys is described in the CPS of the Swiss Government PKI Root CA IV, Chapter 6.2.10 "Destruction of Private Keys."

6.2.6 Management of the hardware security module life cycle

The Swiss Government PKI has processes in place to prevent tampering with hardware security modules during transport and storage. Basic functional tests are performed in accordance with the dual control principle. Installation and initialization/commissioning are carried out by trusted persons in accordance with the dual control principle in a physically protected environment. The key material is deleted in accordance with the manufacturer's instructions.

6.2.7 Uniqueness

Only a single currently valid TSA signature certificate is in operation.

6.3 Time stamp

6.3.1 Time stamp object (token)

The format of the timestamp objects is described in RFC 3161.

Each timestamp object issued by the Swiss Government PKI timestamp service has an identifier for this policy (Chapter4.2Identifier) and a serial number for unique identification.

The date and time in the timestamp object can be traced back to a recognized time source. The date and time in the timestamp object are provided with the accuracy described in Chapter 6.1.2TSA declarations.

If the reference clock no longer has a reliable time base, an alarm is triggered and the service is suspended because, in this case, the TSA is no longer able to provide the time with an accuracy in accordance with Chapter 6.1.2 TSA declarations. No more timestamp objects are generated until the reference clock is recalibrated.

Timestamp objects contain the hash value that is included in the request to the timestamp service. The timestamp object is signed with a key that is used exclusively for the timestamp service.

If a flag is set in the timestamp request to integrate the timestamp service certificate into the timestamp token, the timestamp service certificate is integrated into the resulting timestamp object.

If the timestamp request contains an ID (PolicyID) other than the ID mentioned in chapter 4.2Identifier, the timestamp request is rejected. The rejection is indicated by the corresponding status in the generated timestamp object.
If the timestamp request contains a hash algorithm other than those described in chapter6.1.2TSA declarations, the timestamp request is rejected. The rejection is indicated by the corresponding status in the generated timestamp object.

If the timestamp request is not formatted in accordance with RFC 3161, the timestamp request is rejected. The rejection is indicated by the corresponding status in the generated timestamp object.

The use of the following attributes in the timestamp request is supported:
- reqPolicy
- nonce
- certReq

6.3.2 Time synchronization with UTC

Time calibration is performed automatically. Several NTP time servers are used for this purpose. The time signals are obtained from several independent sources. The time stamp units used in the Swiss Government PKI have technical devices to keep their synchronized time within the declared accuracy.

The Swiss Government PKI has measures in place to prevent unauthorized manipulation of the clock.

6.4 TSA administration and operation

6.4.1 Security management

All matters relating to security management are described in the CPS of the Swiss Government PKI Root CA IV Chapter 5.2 Organizational Security Measures.

6.4.2 Classification and management of the facility

Descriptions of methods and measures for the continuity and stability of the Swiss Government PKI are described in the CPS of the Swiss Government PKI Root CA IV, Chapter 5.1 Infrastructural Security Measures.

6.4.3 Personnel security measures

Requirements for personnel and the roles that personnel will assume are described in the CPS of the Swiss Government PKI Root CA IV Chapter 5.3 Personnel Security Measures.

6.4.4 Physical and infrastructural security

The description of the infrastructural security measures is provided in the CPS of the Swiss Government PKI Root CA IV Chapter 5.1 Infrastructural Security Measures.

6.4.5 Operation

The Swiss Government PKI time stamp service has security procedures in accordance with ETSI EN 319 421. These documents are not publicly available and are periodically audited by internal and external auditors.

6.4.6 Access control

Access controls are regulated in the CPS of the Swiss Government PKI Root CA IV, Chapter 5.1.2 Access Control.

6.4.7 Trustworthy use and operation of the systems

Key generation for the Swiss Government PKI Time Stamping Service is carried out exclusively in a trusted environment as described in Chapter 6.1.2TSA declarations.

The systems comply with one of the following or equivalent standards:

- FIPS 140-2 Level 3

All changes to the systems are monitored and recorded in an event log.

6.4.8 Compromise of the TSA service

In the event of a compromise of the timestamp service key, the procedures set out in CPS of the Swiss Government PKI Root CA IV Chapter 5.7 Compromise and Recovery are carried out.

6.4.9 Discontinuation of the TSA service

In the event of discontinuation of the Swiss Government PKI time stamp service, the procedures set out in CPS of the Swiss Government PKI Root CA IV, Chapter 5.8 Discontinuation of Operations will be followed.

6.4.10 Compliance with legal requirements

The Swiss Government PKI time stamp service is operated in accordance with Swiss legislation and ZertES.

6.4.11 TSA logging

6.4.11.1 General

The Swiss Government PKI time stamp service has an event log that records all events related to the issuance of a time stamp object:

- The successful issuance of timestamp objects is logged: date, time, message imprint, hash algorithm, serial number, and leap second information, if applicable.
- Errors in the processing of a time stamp request are logged.
- Confidentiality and integrity are ensured in accordance with the defined processes of the CPS of the Swiss Government PKI Root CA IV.
- The log files relating to time stamp service operations are secured in accordance with the defined procedures of the CPS of the Swiss Government PKI Root CA IV.
- The logged and archived timestamp objects can be made available upon request in the event of a legal dispute.
- All time stamp, key management, and time synchronization events are logged with the exact time.
- All time stamp, key management, and time synchronization events are stored for 11 years.
- Electronic log files are transferred to an external server and thus protected against access, deletion, and manipulation, and are only accessible to system and network administrators.
- **As a TSA, the BIT is responsible for measures** to protect confidential information. Data may only be processed within the scope of service provision and may only be passed on to third parties if a confidentiality agreement has been signed in advance and the employees entrusted with the tasks have been obliged to comply with the legal provisions on data protection. For audit or review purposes, documents may be inspected in the presence of the SG PKI security officer or a named representative.

6.4.11.2 TSA Key Management

All events in the life cycle of the TSA signature key are logged. In particular, key generation, key renewal, key backup, and key destruction are performed in 4 AP.

All events in the life cycle of TSA certificates are logged.

6.4.11.3 Time synchronization

All events of the time stamp server relating to calibration are logged. These include, for example, manual calibrations and the handling of leap seconds. In addition, the history of the deviation of the time server from UTC time (drift) is logged.

All evidence of loss of synchronization of the time server with UTC time is logged.

6.5 Organization

Infrastructural, organizational, and personnel security measures can be found in the CPS of the Swiss Government PKI Root CA IV, Chapter 5. Individual areas may be covered in separate documents that are not necessarily published. All security measures comply with the requirements of the ZertES, the TAV, and the documents referenced therein, in particular ETSI EN 319 421.

6.5.1 Cost

The fees are listed in the framework agreement between the Swiss Government PKI and its customers.