Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

**Bundesamt für Informatik und Telekommunikation BIT**
PS/IDTR/TRB
SG-PKI

Hans W. Kramer, 3.5.2023

# Swiss Government PKI

# Time Stamping Authority - Policy

**Projektname:**
**Projektnummer:**
**Version:** V1.64
**Referenz/Aktenzeichen:** WeJ

**Status:**

| in Arbeit | in Prüfung | genehmigt zur Nutzung |
|---|---|---|
| | | x |

| **Beteiligter Personenkreis** | |
|---|---|
| Autor: | Tomaso Vasella, Jürgen Weber |
| Bearbeitung: | Cornelia Enke, Hans W. Kramer |
| Prüfung: | Hans Kramer, Marcel Suter, Pascal Joye |
| Genehmigung: | PKI Management Board |

| **Änderungskontrolle, Prüfung, Genehmigung** | | | |
|---|---|---|---|
| **Wann:** | **Version:** | **Wer:** | **Beschreibung:** |
| 21.07.2006 | X0.8 | Tomaso Vasella | Version zuhanden BIT |
| 20.08.2006 | X0.9 | Robert Dietschi | Aktualisierung |
| 13.03.2007 | V1.0 | Robert Dietschi | Freigabe |
| 13.02.2008 | V1.1 | Tomaso Vasella | Aktualisierung |
| 15.02.2008 | V1.1 | Jürgen Weber | Freigabe |
| … | … | … | … |
| 21.05.2013 | V1.2 | Jürgen Weber | Aktualisierung |
| 03.12.2013 | V1.3 | Jürgen Weber | Aktualisierung Kap. 6.2.4 nach Re-Keying |
| 27.09.2018 | V1.4 | Jürgen Weber, Cornelia Enke | Aktualisierung, Ergänzung der Änderungen der gesetzlichen Vorgaben – Revision ZertES |
| 25.02.2019 | V1.41 | Cornelia Enke | Aufnahme der unterstützen Parameter für TSA Request und TSA Response Chapter 6.3.1 |
| 07.05.2019 | V1.5 | Cornelia Enke | Ausstellung des neuen TSA Dienstezertifikats, Dokumentation in diesem Dokument und Freigabe der TSA Policy |
| 16.08.2019 | V1.6 | Cornelia Enke | Review, Ergänzung requirement gemäss ETSI EN |

| Änderungskontrolle, Prüfung, Genehmigung | | | |
|---|---|---|---|
| | | | 319 411-1 Rev 6.3-10 |
| 06.05.2021 | V1.61 | Cornelia Enke | Review, Ergänzung 4AP bei der TSA Schlüsseloperationen. |
| 31.08.2021 | V1.62 | Cornelia Enke | Ergänzung Policy Conformance für BTSP aufgenommen |
| 26.4.2023 | V1.63 | Hans W. Kramer | Jährliche Durchsicht und Anpassungen. |
| 3.5.2023 | V1.64 | Pascal Joye | Prüfung |

| Genehmigung | | | |
|---|---|---|---|
| **Wann:** | **Version:** | **Unterschrift** | **Unterschrift** |
| 31.5.2023 | V1.64 | Kramer Hans 0DOYGL<br>31.05.2023<br><br>Info: admin.ch/esignature \| validator.ch | Joye Pascal 2DFUMO<br>31.05.2023<br><br>Info: admin.ch/esignature \| validator.ch |

# Inhaltsverzeichnis

## Referenzierte Dokumente

| *Ref.* | *Beschreibung* |
|---|---|
| [1] | ETSI EN 319 421 V1.2.0 (2023-01), Policy and Security Requirements for Trust Service Providers issuing Time-Stamps<br>https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.02.00_20/en_319421v010200a.pdf |
| [2] | ETSI EN 319 422 V1.1.1 (2016-03), Time-stamping protocol and time-stamp token Profiles<br>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.<br>https://www.ietf.org/rfc/rfc3126.txt |
| [4] | Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES), 943.03<br>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 der Swiss Government PKI Root CA IV<br>http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf |
| [6] | ETSI TS 119 312 V1.4.2 (2022-02) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites<br>https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.02_60/ts_119312v010402p.pdf |
| [7] | TAV: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur, TAV Bakom; SR 943.032.1Februar 17, 2022)<br>https://www.bakom.admin.ch/dam/bakom/de/dokumente/tc/telekommunikation/tav_pta_digsig_ed2.pdf.download.pdf/TAV-PTA%20DigSig%20-%20ed2%20-%20d%20-%20bf.pdf |
| [8] | IEFT RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001<br>https://www.ietf.org/rfc/rfc3161.txt |
| [9] | IETF RFC 5816 ESSCertIDv2 Update for RFC 3161<br>https://www.ietf.org/rfc/rfc5816.txt |

## Verwendete Abkürzungen

| *Abkürzung* | *Bedeutung* |
|---|---|
| BIT | Bundesamt für Informatik und Telekommunikation |
| 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 |
| HTTP | Hypertext Transfer Protocol |

| *Abkürzung* | *Bedeutung* |
|---|---|
| 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 | Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur |
| TSA | Time Stamping Authority |
| TSU | Time Stamping Unit |
| UTC | Coordinated Universal Time |
| ZertES | Bundesgesetz über die elektronische Signatur |

# 1 Einleitung

Die Swiss Government PKI bietet als Dienstleister von qualifizierten elektronischen Signaturen gemäss Schweizerischem Signaturgesetz ZertES (Ref. [4]) einen Zeitstempeldienst (Time Stamping Service) an. Mit diesem Zeitstempeldienst kann die Existenz von digitalen Daten zu einem bestimmten Zeitpunkt vertrauenswürdig und nachvollziehbar belegt werden. Zeitgestempelte Daten können nicht unbemerkt verändert werden.

Dazu wird der Hashwert der zu stempelnden Daten zum Zeitstempel-Dienst gesendet. Der Zeitstempel-Dienst erzeugt ein Zeitstempel-Objekt (Token), das den Hashwert und die aktuelle Zeit enthält. Dieses Objekt wird vom Zeitstempel-Dienst digital signiert, damit wird dessen Integrität geschützt.

Dieses Dokument beschreibt die Time-Stamping Authority Policy (nachfolgend TSA Policy) des Zeitstempeldienstes der Swiss Government PKI. Die TSA Policy spezifiziert generelle Prozesse, die vom Zeitstempeldienst während dem Erstellen von signierten Zeitstempeln verwendet werden.

Detaillierte Spezifikationen der Prozesse sind im Certification Practice Statement CPS (Ref. [5]) zu finden.

Zeitstempel, die gemäss dieser TSA Policy erstellt wurden, können verwendet werden, um den Zeitpunkt einer digitalen Beglaubigung vertrauenswürdig zu dokumentieren.

Struktur und Inhalt dieser Policy sind gemäss ETSI EN 319 421 (Ref. [1]) aufgebaut.

# 2 Geltungsbereich

Dieses Dokument umschreibt die, durch die TSA der Swiss Government PKI erbrachten Leistungen, sowie die damit zusammenhängenden Betriebs- und Management-Prozesse.

Dies erlaubt es den Empfängern bzw. Benutzern von Zeitstempel-Objekten (Relying Parties) sowie den Benutzern des Zeitstempel-Dienstes (Subscriber), die Vertrauenswürdigkeit des Zeitstempel-Dienstes der Swiss Government PKI zu beurteilen.

Die Anforderungen an den Zeitstempel-Dienst für elektronische Signaturen ergeben sich aus dem Schweizerischen Signaturgesetz (ZertES). Die Zeitstempel-Dienste können aber auch für alle anderen Applikationen verwendet werden, die einen Beweis für die Existenz von Daten zu einem bestimmten Zeitpunkt erfordern.

# 3 Allgemeine Konzepte

## 3.1 Zeitstempel-Dienste

Zeitstempel-Dienste bestehen ausfolgenden Komponenten:

- Technische Komponenten, welche die Zeitstempel-Objekte (Tokens) erstellen
- Verwaltung der Zeitstempel-Objekte
  Diese Komponente überwacht und kontrolliert den Zeitstempel-Betrieb einschliesslich der Synchronisation mit einer UTC Referenzzeitquelle.
- Der Zeitstempeldienst entspricht den Anforderungen der «best practices for time-stamp policy» Services (BTSP), wie in ETSI EN 319 421 [1] definiert.

## 3.2 NTP-Dienste BIT

Das BIT unterhält eine NTP (Network Time Protocol) Infrastruktur, um den PKI-Kunden eine genaue Zeit für seine Dienste/Applikationen zu liefern.

Das BIT stellt dazu sowohl in einem ersten Rechenzentrum als auch in einem zweiten Rechenzentrum eine Stratum-1 und eine Stratum-2-Umgebungen zur Verfügung.
Die Stratum-1-Umgebung besteht aus je drei Zeitservern, die mit je einer Funkantenne, einer GPS- und einer Multiband-Antenne (Satellitenantennen) verbunden sind.

Die beiden Zeitserver mit Satellitenantennen werden am jeweiligen Standort mit einem Rubidium Oszillator verbunden. Das Rubidium-Modul ist mit dem Referenzsignal des zugehörigen Server-Gehäuse verbunden und wird mit diesem Signal gesteuert, solange sich das vorgeschaltete System im synchronisiertem Zustand befindet.

Falls die Referenzuhr ihre Synchronisationsquelle verliert, liefert das Rubidium-Modul die Sync-Referenz für das System auf der Grundlage der Holdover Performance.

Die Stratum-2-Umgebung besteht aus je vier Zeitservern, die ihre Zeit mit den drei Stratum-1-Servern und mit den offiziellen Schweizer Zeitservern von Metas synchronisieren.

Die beiden Rechenzentren sind komplett standortunabhängig und stellen die Zeit für die Clientsysteme der jeweiligen Standorte zur Verfügung.

## 3.3 NTP Implementation im BIT

(Detaillierte Informationen auf begründete Anfrage.)

## 3.4 Zeitstempel-Autorität

Die Zeitstempel-Autorität (TSA) erzeugt Zeitstempel-Objekte für die Benutzer des Zeitstempel-Dienstes (Empfänger des Zeitstempel-Objektes und Benutzer des Zeitstempel-Dienstes). Die TSA umfasst die technischen und organisatorischen Komponenten zur Sicherstellung des Zeitstempel-Dienstes (insbesondere der Time Stamping Unit, TSU) und die Informations- und Kommunikationsinfrastruktur.

Der Signierschlüssel der TSA wird verwendet, um Zeitstempel-Objekte zu signieren.

## 3.5 Benutzer (Subscribers)

Die Zeitstempel-Dienst Benutzer können juristische (eine Organisation) oder natürliche Personen sein. Eine Organisation ist verantwortlich für die Tätigkeiten ihrer Mitarbeiter, es wird deshalb von ihr erwartet, dass sie ihre Mitarbeiter über die korrekte Nutzung von Zeitstempeln informiert.

## 3.6 TSA Policy und Practice Statement

### 3.6.1 Zweck

Die Zeitstempel Policy definiert „was eingehalten werden muss“, während das Zeitstempel Practice Statement definiert, „wie es eingehalten wird“. Dieses Dokument ist die Zeitstempel Policy (TSA Policy), das die allgemeinen Anforderungen beschreibt, denen der Swiss Government PKI Zeitstempeldienst genügen muss. Das Zeitstempel Practice Statement ist in Kapitel 6.1 definiert.

### 3.6.2 Detaillierungsgrad

Die TSA Policy spezifiziert generelle Prozesse, die vom Zeitstempeldienst während des Erstellens von signierten Zeitstempeln verwendet werden. Die TSA Policy erlaubt es, sich zusammen mit der CPS ein Bild über die Vertrauenswürdigkeit des TSA-Dienstes zu machen. Detailliertere Spezifikationen dieser Prozesse sind im Certification Practice Statement CPS (Ref. [5]) zu finden.

### 3.6.3 Vorgehen

Diese Policy spezifiziert generelle Prozesse. Sie beschreibt keine technischen Details in Bezug auf die Informations- und Kommunikations-Infrastruktur, die Betriebsorganisation und Schutzvorkehrungen.

Sie beschreibt nicht die Umgebung, in der der Zeitstempel-Dienst betrieben wird. Diesbezügliche technische und operationelle Details sind in der CPS (Ref. [5]) oder anderen internen Dokumenten beschrieben.

# 4 TSA Policy

## 4.1 Übersicht

Diese TSA Policy ist eine Zusammenstellung von Prozessen, die zur vertrauenswürdigen Erzeugung und Verwaltung von Zeitstempel-Objekten und als Vorschrift für das Sicherheitsniveau der TSA verwendet werden.

Generelle Regeln sind im Kapitel 3.6 „TSA Policy und Practice Statement“ in diesem Dokument beschrieben.

Zeitstempel-Objekte werden mit einer Genauigkeit von 1 Sekunde oder besser ausgegeben. Sie können über eine HTTP Schnittstelle angefordert werden.

Die Zeitstempel Authority, die den Zeitstempel-Dienst der Swiss Government PKI betreibt, gibt Zeitstempel-Objekte gemäss der Spezifikation von ETSI EN 319 422 [2] aus. Jedes Zeitstempel-Objekt beinhaltet die Kennung dieser Policy. Die Kennung ist im Kapitel 4.2 „Kennung“ beschrieben.

## 4.2 Kennung

Die Kennung (Object Identifier, OID) dieser Policy lautet: **2.16.756.1.17.3.5.2.4**
Diese Kennung ist in jedem Zeitstempel-Objekt vorhanden.
(Bemerkung: Bis am 14.12.2022,1700 Uhr UTC wurde die Kennung 2.16.756.1.17.3.2.18 gemäss einer früheren Version dieses Dokumentes verwendet.)

## 4.3 Anwendbarkeit

Diese Policy ist so ausgelegt, dass der Zeitstempel-Dienst den gesetzlichen Anforderungen für qualifizierte digitale Signaturen (ZertES, Ref. [4]) entspricht.

## 4.4 Konformität

Erstellte Zeitstempel-Objekte beinhalten die Kennung, die im Kapitel 4.2 „Kennung“ beschrieben ist.

Die TSA  versichert die Einhaltung der Vorschriften während der Ausübung der Dienste, die im Kapitel 5.1 „Verpflichtungen der TSA“ beschrieben sind. Im Weiteren versichert die TSA die Zuverlässigkeit der Kontroll-Mechanismen, die im Kapitel 6 „TSA Prozesse“ beschrieben sind.

# 5 Verpflichtungen und Haftung

## 5.1 Verpflichtungen der TSA

### 5.1.1 Allgemeine Verpflichtungen

Dieses Kapitel enthält alle Verpflichtungen, Verbindlichkeiten, Garantien und Verantwortungen der TSA, ihrer Zeitstempel-Dienst Bezüger und der Zeitstempel-Objekt Empfänger. Die Verpflichtungen und Verantwortungen werden durch gegenseitige Verträge geregelt, die zwischen den Parteien abgeschlossen werden.

Die Swiss Government PKI verpflichtet sich als TSA alle im Rahmen dieser TSA Policy und in der jeweils zugehörigen CPS (Ref. [5]) beschriebenen Aufgaben zur Umsetzung der Vorgaben des ZertES und der weiteren Ausführungsbestimmungen (TAV, Ref. [7]) durchzuführen.

Das Certification Practice Statement (Ref. [5]) und die TSA Policy sind integraler Bestandteil der Verträge zwischen der Swiss Government PKI und den Zeitstempel-Dienst Benutzern. Die Swiss Government PKI garantiert, dass alle Anforderungen an die TSA, einschliesslich

der Abläufe und Verfahren bezogen auf die Ausgabe der Zeitstempel-Objekte, Reviews der Systeme und Sicherheits-Audits in Übereinstimmung mit den Prozessen in Kapitel 6 „TSA Prozesse“ eingehalten werden.

Die Konfiguration der TSP-Systeme wird regelmäßig in Bezug auf ihre Konformität zu den geltenden gesetzlichen und normativen Regelungen überprüft. Das maximale Zeitdauer zwischen zwei Überprüfungen beträgt ein Jahr.

### 5.1.2 TSA Verpflichtungen gegenüber Zeitstempel-Benutzern

Die Swiss Government PKI gewährt permanenten Zugang zum Swiss Government PKI Zeitstempeldienst (möglichst 24x7), ausser bei geplanten technischen Unterbrüchen und beim Fehlen einer genauen Zeitbasis, höherer Gewalt, Naturereignissen (z.B. Blitzschlag, Elementarereignisse), kriegerischen Ereignissen, Streik, unvorhersehbaren behördlichen Restriktionen sowie Hackerattacken oder Virenbefall (inkl. trojanische Pferde u.ä.) beim Benutzer des Zeitstempel-Dienstes.

Geplante Service-Einschränkungen werden auf der Webseite der Swiss Government PKI angekündet.

Im Weiteren garantiert die Swiss Government PKI Folgendes:

- Aufbau und Betrieb einer zuverlässigen Informations- und Kommunikations-Infrastruktur.
- Einhaltung von Eigentumsrecht, Lizenzen oder ähnlichen Gesetzen.
- Die angebotenen Dienste stimmen mit allgemein akzeptierten Normen überein, wie sie in Kapitel 4.1 „Übersicht“ in diesem Dokument beschrieben sind.
- Die ausgestellten Zeitstempel-Objekte sind korrekt.
- Die Genauigkeit in Bezug auf die UTC Zeit beträgt ±1 Sekunde oder besser. Die durch den NTP Daemon des TSA-Servers geschätzte Genauigkeit wird im Feld «accuracy» gemäss [8], «2.4.2. Response Format» ausgegeben. Im Falle, dass die Genauigkeit schlechter ist als ±1 Sekunde, wird eine Fehlermeldung gemäss [8], «2.4.2. Response Format» ausgegeben. Dies entspricht [1], OVR-5.1-03 und [2] .»2.2 Fields to be supported».

## 5.2 Verpflichtungen der Zeitstempel-Dienst Benutzer

Bezüger von Zeitstempel Objekten müssen beim Bezug der Zeitstempel Objekte die digitale Signatur der Zeitstempel-Authority überprüfen und die CRL daraufhin überprüfen, ob das TSA Zertifikat revoziert worden ist.

Die aktuelle CRL kann unter der Bezugsadresse, die im CPS [5] Kapitel „2.1 Verzeichnisdienst“ aufgeführt ist, bezogen werden.

## 5.3 Verpflichtungen der Zeitstempel-Objekt Benutzer

Die Verpflichtung des Zeitstempel-Objekt Empfängers besteht in der Überprüfung der Signatur des Zeitstempel-Objektes. Der Zeitstempel-Objekt Empfänger muss die Gültigkeit und die Dauer der Gültigkeit des CA Zertifikates überprüfen. Falls die Überprüfung des Zeitstempels nach Ablauf der Gültigkeit des Zertifikates der TSA stattfindet, muss der Zeitstempel-Objekt Empfänger Folgendes unternehmen:

- Überprüfen, ob die TSA Kennung in die CRL aufgenommen wurde
- Überprüfen, ob die Hash-Funktion, die im Zeitstempel-Objekt vermerkt ist, immer noch sicher ist
- Überprüfen, ob die Länge der kryptografischen Schlüssel der TSA und die verwendeten Algorithmen immer noch als sicher betrachtet werden

Die Informationen zur ausstellende CA und zu den Zugriffspunkten fur Statusüberprüfung sind im Zeitstempelzertifikat selbst enthalten und geben die Bezugsquelle dieser Informationen an.

## 5.4 Gewährleistung

Die Swiss Government PKI steht gegenüber Zeitstempel-Dienstbenutzern für die sorgfältige und vertragsgemässe Erbringung der vereinbarten Leistungen ein. Die Swiss Government PKI bemüht sich um eine hohe Verfügbarkeit der Dienste, kann jedoch keine Gewährleistung für ein unterbruchs- und störungsfreies Funktionieren übernehmen.

## 5.5 Haftung

Die Swiss Government PKI haftet gemäss Art. 17 ZertES der Inhaberin oder dem Inhaber des Signaturschlüssels und Drittpersonen, die sich auf ein gültiges qualifiziertes Zertifikat verlassen haben, für Schäden, die diese erleiden, falls die Swiss Government PKI den Pflichten aus dem Signaturgesetz sowie den Ausführungsvorschriften nicht nachgekommen ist. Die Swiss Government PKI trägt die Beweislast dafür, den Pflichten aus dem ZertES und den Ausführungsvorschriften nachgekommen zu sein.

Die Swiss Government PKI haftet nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung (gemäss Art. 7. Abs 3 ZertES und Art. 17 Abs. 3 ZertES) des Zertifikats ergeben.

In allen andern Fällen haftet die Swiss Government PKI wie folgt:

- Bei Vertragsverletzungen für den nachgewiesenen Schaden, sofern sie nicht beweist, dass sie kein Verschulden trifft.
- Absichtlich oder grobfahrlässig verschuldete Schäden werden unbegrenzt ersetzt.
- Bei leichter Fahrlässigkeit wird für Vermögensschäden bis zum Gegenwert der während des laufenden Vertragsjahres vereinbarten Leistungen, höchstens bis CHF 50‘000 je Schadenereignis und Kalenderjahr gehaftet.

In keinem Fall wird für Folgeschäden, entgangenen Gewinn und Datenverluste gehaftet.
Die Swiss Government PKI haftet nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung (gemäss Art. 7. Abs 3 ZertES und Art. 17 Abs. 3 ZertES) des Zertifikats ergeben.

# 6 TSA Prozesse

Die für den Betrieb der TSA implementierten Kontrollen sind im CPS (Ref. [5]) Kapitel 5 „Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen“ beschrieben.

# 6.1 Prozesse und Deklarationen

## 6.1.1 Prozesse der TSA (TSA Practice Statement)

- Verfahren, Kontroll-Mechanismen und technische Infrastruktur zur Sicherstellung eines kontrollierten, unterbruchsfreien und zuverlässigen Services sind die Basis für den TSA Betrieb. Die detaillierten Kontrollen sind im CPS [5] Kapitel 6.6 „Lebenszyklus der Sicherheitsmassnahmen“ beschrieben.
- Im CPS (Ref. [5]) sind - zusammen mit anderen internen Dokumenten - die Regeln für den Betrieb des Zeitstempel-Dienstes definiert.
- Kleinere Änderungen ohne oder mit minimaler Auswirkung auf die Benutzer werden durch die Swiss Government PKI direkt umgesetzt. Grössere Änderungen werden in Absprache mit der Anerkennungstelle und nach Genehmigung durch die Anerkennungsstelle durchgeführt.

Änderungen werden in einem Journal festgehalten. Alle Benutzer werden 30 Tage vor Inkraftsetzung grösserer Änderungen via e-Mail informiert, falls die e-Mail Adresse bekannt ist. Zusätzlich werden Änderungen gemäss Kapitel 5.1.2 veröffentlicht.
Es besteht ein formelles Genehmigungsverfahren für diese TSA Policy und Änderungen davon.

## 6.1.2 Deklarationen der TSA

- Kontaktinformationen zum Zeitstempel-Dienst sind im CPS (Ref. [5]) Kapitel 1.5.2 „Kontaktperson“ enthalten.
- Jedes Zeitstempelobjekt, das vom Swiss Government PKI Zeitstempeldienst ausgegeben wird, beinhaltet die Kennung der Policy, wie sie im Kapitel 4.2 „Kennung“ beschrieben ist.
- Die eingesetzten kryptografischen Algorithmen und deren Schlüssellängen orientieren sich an den in den TAV (Ref. [7]) referenzierten Veröffentlichungen der ETSI EN 319 422 (Ref. [2]) . Zum Zeitpunkt der Erstellung des vorliegenden Dokumentes sind dies:
    - Hash Algorithmen
        - 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)
    - Schlüssellänge
        - 2048 bit
- Algorithmus für die Signatur
    - sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
- Die Genauigkeit der Zeit, die im Zeitstempel-Objekt verwendet wird, ist im Minimum ±1 Sekunde Abweichung von der UTC (Universal Time Coordinated) Zeit. Ist die Zeitdifferenz grösser, wird der Dienst eingestellt.
- Verpflichtungen der Zeitstempel-Dienst Benutzer sind im Kapitel 5.2 „Verpflichtungen der Zeitstempel-Dienst Benutzer“ beschrieben.
- Verpflichtungen des Zeitstempel-Objekt Empfänger sind im Kapitel 5.3 „Verpflichtungen der Zeitstempel-Objekt Benutzer“ beschrieben.
- Verifikation der Zeitstempel-Objekte ist in Kapitel 5.3 „Verpflichtungen der Zeitstempel-Objekt Benutzer“ beschrieben.

- Log-Daten werden gemäss Kapitel 5.4 „Sicherheitsüberwachung“ der CPS (Ref. [5]) gespeichert und archiviert.
- Die Swiss Government PKI räumt Zeitstempel-Dienst Benutzern das Recht ein, dieses Dokument unverändert an Dritte weiter zu geben. Weitergehende Rechte werden nicht eingeräumt.
  Insbesondere sind die Weitergabe veränderter Fassungen und die Überführung in andere Dokumente oder Publikationen ohne schriftliche Zustimmung der Swiss Government PKI nicht zulässig.
- Der Zeitstempel-Dienst ist eine Dienstleistung der Swiss Government PKI, die gemäss dem Schweizerischen Signaturgesetz ZertES (Ref. [4]) zertifiziert ist.
- Der Versicherungsschutz der Swiss Government PKI erstreckt sich im Rahmen der Nutzungsbestimmungen der Swiss Government PKI, die dem Zertifikatsinhaber ausgehändigt werden, auch auf gesetzliche Haftpflichtansprüche für reine Vermögensschäden aus Art. 17 ZertES. Kosten, die die versicherten Unternehmungen bei einer allfälligen Einstellung der Geschäftstätigkeit gemäss Art. 14 ZertES zu tragen haben, sind ebenfalls versichert. Für die erwähnten Schäden und Kosten gilt eine gemeinsame Sublimite von CHF 2 Mio. pro Ereignis und CHF 8 Mio. pro Versicherungsjahr.
- Alle sich aus der vorliegenden TSA Policy ergebenden Streitigkeiten, an denen die Swiss Government PKI beteiligt ist, sind nach den Bestimmungen des Konkordates über die Schiedsgerichtsbarkeit einem Dreierschiedsgericht mit Sitz in Bern zur endgültigen Entscheidung zu unterbreiten. Die Bestellung des Schiedsgerichts erfolgt durch den Präsidenten des Handelsgerichts des Kantons Bern. Das Verfahren vor dem Schiedsgericht richtet sich nach der Zivilprozessordnung des Kantons Bern, soweit nicht das Konkordat über die Schiedsgerichtsbarkeit zur Anwendung gelangt. Die Verhandlung wird in deutscher Sprache geführt.
  Die Vertragspartner verpflichten sich jedoch, vor Anrufung des Schiedsgerichts alle zumutbaren Anstrengungen zu unternehmen, den Streit einvernehmlich beizulegen. Sie können sich dazu eines gemeinsam zu bestimmenden Mediators bedienen.
  Ein solcher Vermittlungsversuch hat keine Auswirkung auf gesetzliche Verjährungsfristen.
- Die TSA ist konform zur vorliegenden „Time-Stamp Policy“. Die Implementation und die Prozessabläufe wurden durch die Zertifizierungsstelle KPMG AG auditiert und beglaubigt.

## 6.2 Lebenszyklus des Schlüsselmanagements

### 6.2.1 Erzeugung des TSA Schlüssels

Die TSA Schlüssel werden in einem Hardware Security Module erzeugt, das gemäss FIPS 140-2, Level 3 oder CEN EN 419 221-5 zertifiziert ist. Die Schlüssel werden durch vertrauenswürdiges Personal und vertrauenswürdige Rollen erzeugt. Die Beschreibung der Anforderungen des Personals in im CPS (Ref. [5]) Kapitel 5.3 „Personelle Sicherheitsmassnahmen“ beschrieben.
Die Umgebung der TSA-Schlüssel-Erzeugungist im CPS (Ref. [5]) beschrieben.
TSA-Hash- und -Verschlüsselungs-Algorithmen sind im Kapitel 6.1.2 „Deklarationen der TSA“ beschrieben.

### 6.2.2 Schutz des TSA-Private-Key

Das eingesetzten HSM-Modul für die Zertifizierung, genügen den Anforderungen der TAV (Ref. [7]):

HSM: SafeNet Luna SA

- FIPS 140-2, Level 3

### 6.2.3 Verteilung des TSA Public Key

TSA Zertifikate, die den Public Key beinhalten, werden von der Swiss Government PKI CA signiert. Die Publikation der Zertifikate ist im CPS (Ref. [5]) Kapitel 2.1 „Verzeichnisdienst“ beschrieben.

### 6.2.4 Re-Keying des TSA Schlüssels

Das TSA-Zertifikat wird ungefähr jährlich neu erstellt und von der „Swiss Government Regulated CA 02“ signiert.

Das TSA-Zertifikat wird mindestens alle 2 Jahre erneuert. Die Häufigkeit ist abhängig von der Anzahl ausgestellter Zeitstempel-Objekte. Werden sehr viele Zeitstempel-Objekte ausgestellt, so wird das Re-Key Verfahren mehr als einmal pro Jahr durchgeführt. Der Public Key wird gemäss CPS (Ref. [5]) 6.3.1 „Archivierung öffentlicher Schlüssel“ archiviert. Der nicht mehr benutzte Private Key wird gelöscht und nicht archiviert.

### 6.2.5 Ende des TSA Schlüssel-Lebenszyklus

Das Verfahren für die Zerstörung der TSA Schlüssel ist im CPS (Ref. [5]) Kapitel 6.2.10 „Vernichtung der Privaten Schlüssel“ beschrieben.

### 6.2.6 Verwaltung des Lebenszyklus des Hardware Security Moduls

Die Swiss Government PKI verfügt über Prozesse zur Verhinderung von Manipulationen an Hardware Security Modulen während Transport und Lagerung. Grundlegende Funktionstests werden ausgeführt unter Einhaltung des 4-Augen-Prinzips. Installation und Initialisierung/Inbetriebnahme erfolgen durch vertrauenswürdige Personen im 4-Augen Prinzip in einer physisch geschützten Umgebung. Das Schlüsselmaterial wird gemäss Herstellerangaben gelöscht.

## 6.3 Zeitstempel

### 6.3.1 Zeitstempel-Objekt (Token)

Das Format der Zeitstempel-Objekte ist in RFC 3161 (Ref. [8]) und in [2] beschrieben.

Jedes Zeitstempel-Objekt, das vom Zeitstempel-Dienst der Swiss Government PKI ausgegeben wird, besitzt eine Kennung dieser Policy (Kapitel 4.2 „Kennung“) sowie eine Seriennummer für die eindeutige Identifizierung.

Datum und Zeit im Zeitstempel-Objekt können zu einer anerkannten Zeitquelle zurückverfolgt werden. Datum und Zeit im Zeitstempel-Objekt sind mit der in Kapitel 6.1.2 „Deklarationen der TSA“ beschriebenen Genauigkeit versehen.

Falls die Referenz-Uhr keine zuverlässige Zeitbasis mehr besitzt, wird ein Alarm ausgelöst und der Dienst eingestellt, weil die TSA in diesem Fall nicht mehr im Stande ist, die Zeit mit einer Genauigkeit gemäss Kapitel 6.1.2 „Deklarationen der TSA“ zu liefern. Es werden keine Zeitstempel-Objekte mehr generiert, bis die Referenz-Uhr wieder kalibriert ist.

Zeitstempel-Objekte beinhalten den Hash-Wert, der im Antrag an den Zeitstempel-Dienst mitgeliefert wird. Das Zeitstempel-Objekt wird mit einem Schlüssel signiert, der ausschliesslich für den Zeitstempel-Dienst verwendet wird.

Falls im Zeitstempel-Request ein Flag gesetzt ist, um das Zeitstempel-Dienst Zertifikat im Zeitstempel-Token zu integrieren, wird das Zeitstempel-Dienst-Zertifikat im resultierenden Zeitstempel-Objekt integriert.

Falls der Zeitstempel-Request eine andere Kennung (PolicyID) als die in Kapitel 4.2 „Kennung“ erwähnte Kennung enthält, wird der Zeitstempel-Request zurückgewiesen. Die Rückweisung erfolgt durch den entsprechenden Status im erzeugten Zeitstempel-Objekt.
Falls der Zeitstempel-Request einen anderen Hash-Algorithmus als die in Kapitel 6.1.2 „Deklarationen der TSA“ beschriebenen enthält, wird der Zeitstempel-Request zurückgewiesen. Die Rückweisung erfolgt durch den entsprechenden Status im erzeugten Zeitstempel-Objekt.

Falls der Zeitstempel-Request nicht gemäss RFC 3161 (Ref. [8]) formatiert ist, wird der Zeitstempel-Request zurückgewiesen. Die Rückweisung erfolgt durch den entsprechenden Status im erzeugten Zeitstempel-Objekt.

Die Verwendung der folgenden Attribute in der Zeitstempelanforderung wird unterstützt::

- reqPolicy
- nonce
- certReq

(konform zu [8]).

### 6.3.2 Zeitsynchronisierung mit UTC

Die Zeitkalibrierung wird automatisch vorgenommen. Dazu werden mehrere NTP Time Server eingesetzt. Die Zeitsignale werden von mehreren unabhängigen Quellen bezogen. Die in der Swiss Government PKI eingesetzten Time Stamp Units besitzen technische Vorrichtungen, um ihre synchronisierte Zeit innerhalb der deklarierten Genauigkeit zu halten.

Die Swiss Government PKI verfügt über Vorkehrungen, um unautorisierte Manipulationen der Uhr zu verhindern.

## 6.4 TSA Verwaltung und Betrieb

### 6.4.1 Sicherheitsmanagement

Alle Angelegenheiten, die das Sicherheitsmanagement betreffen, sind im CPS (Ref. [5]) Kapitel 5.2 „Organisatorische Sicherheitsmassnahmen“ beschrieben.

### 6.4.2 Klassifizierung und Verwaltung der Anlage

Beschreibungen über Methoden und Massnahmen für die Kontinuität und Stabilität der Swiss Government PKI sind im CPS (Ref. [5]) Kapitel 5.1 „Infrastrukturelle Sicherheitsmassnahmen“ beschrieben.

### 6.4.3 Personelle Sicherheitsmassnahmen

Anforderungen an das Personal sowie die Rollen, die das Personal einnehmen wird, sind im CPS (Ref. [5]) Kapitel 5.3 „Personelle Sicherheitsmassnahmen“ beschrieben.

### 6.4.4 Physische und infrastrukturelle Sicherheit

Die Beschreibung der infrastrukturellen Sicherheitsmassnahmen sind im CPS (Ref. [5]) Kapitel 5.1 „Infrastrukturelle Sicherheitsmassnahmen“ beschrieben.

### 6.4.5 Betrieb

Der Swiss Government PKI Zeitstempel-Dienst verfügt über Sicherheitsabläufe gemäss ETSI EN 319 421(Ref. [1]). Diese Dokumente sind nicht öffentlich zugänglich und werden periodisch durch die interne und externe Revision auditiert.

### 6.4.6 Zutrittskontrolle

Die Zutrittskontrollen werden im CPS (Ref. [5]) Kapitel 5.1.2 “Zutrittskontrolle” geregelt.

## 6.4.7 Vertrauenswürdiger Einsatz und Betrieb der Systeme

Die Schlüssel-Erzeugung des Swiss Government PKI Zeitstempel-Dienstes wird ausschliesslich in vertrauenswürdiger Umgebung wie im Kapitel 6.1.2 „Deklarationen der TSA“ erzeugt.

Die Systeme genügen einem der folgend genannten oder äquivalenten Standards:

- FIPS 140-2 Level 3

Alle Änderungen an den Systemen werden überwacht und in einem Ereignis-Journal aufgezeichnet.

## 6.4.8 Kompromittierung des TSA Dienstes

Im Falle einer Kompromittierung des Schlüssels des Zeitstempeldienstes werden die Verfahren gemäss CPS (Ref. [5]) Kapitel 5.7 „Kompromittierung und Wiederherstellung“ durchgeführt.

## 6.4.9 Einstellung des TSA Dienstes

Im Falle der Einstellung des Betriebes des Swiss Government PKI Zeitstempeldienstes werden die Verfahren gemäss CPS (Ref. [5]) Kapitel 5.8„Einstellung des Betriebes“ durchgeführt.

## 6.4.10 Einhaltung der gesetzlichen Vorschriften

Der Zeitstempel-Dienst der Swiss Government PKI wird gemäss Schweizerischer Gesetzgebung und ZertES (Ref. [4]) betrieben.

## 6.4.11 TSA Logging

### 6.4.11.1 Allgemeines

Der Swiss Government PKI Zeitstempel-Dienst verfügt über ein Ereignisjournal, das alle Ereignisse in Zusammenhang mit der Ausstellung eines Zeitstempel-Objektes aufzeichnet:

- Die erfolgreiche Ausstellung der Zeitstempel-Objekte wird geloggt: Datum, Zeit, «message imprint», Hash-Algorithmus, Seriennummer, allenfalls Schaltsekunden-Information.
- Fehler bei der Bearbeitung eines Zeitstempel-Requests werden geloggt.
- Die Vertraulichkeit und Integrität werden gemäss den definierten Prozessen der CPS (Ref. [5]) sichergestellt.
- Die Logdateien bezüglich der Zeitstempeldienst Operationen werden gemäss den definierten Verfahren der CPS (Ref. [5]) sichergestellt.
- Die geloggten und archivierten Zeitstempel Objekte können im Rechtsfall auf Anfrage zur Verfügung gestellt werden.
- Alle Zeitstempel, Schlüsselmanagement und Zeitsynchronisations-Ereignisse werden mit der genauen Zeit geloggt.

- Alle Zeitstempel, Schlüsselmanagement und Zeitsynchronisations-Ereignisse werden für 11 Jahre aufbewahrt.
- Elektronische Log-Dateien werden auf einen externen Server übertragen und so gegen Zugriff, Löschung und Manipulation geschützt und sind nur den System- und Netzwerkadministratoren zugänglich.
- **Das BIT trägt als TSA die Verantwortung für Massnahmen** zum Schutz vertraulicher Informationen. Daten dürfen nur im Rahmen der Diensterbringung bearbeitet und an Dritte nur weitergegeben werden, wenn zuvor eine Vertraulichkeitserklärung unterzeichnet wurde und die mit den Aufgaben betrauten Mitarbeiter auf Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet wurden. Zu Audit- oder Revisionszwecken können Dokumente im Beisein des Security Officers der SG PKI oder eines namentlich benannten Vertreters eingesehen werden.

#### 6.4.11.2 TSA Schlüssel Management

Alle Ereignisse des Lebenszykluses der TSA Signaturschlüssels werden geloggt. Insbesondere Schlüsselerzeugung, Schlüsselerneuerung, Schlüsselbackup und Schlüsselvernichtung.
Schlüsselerzeugung, Schlüsselerneuerung, Schlüsselbackup und Schlüsselvernichtung finden im 4 AP statt.

- Alle Ereignisse des Lebenszykluses der TSA Zertifikate werden geloggt.

#### 6.4.11.3 Zeitsynchronisierung

Es werden alle Ereignisse des Zeitstempel-Servers in Bezug auf die Kalibrierung geloggt. Dies sind beispielsweise manuelle Kalibrierungen und die Handhabung von Schaltsekunden. Im Weiteren wird der Verlauf der Abweichung der Zeit des Zeitservers zur UTC-Zeit (Drift) geloggt.

Es werden alle Nachweise über den Verlust der Synchronisierung der Zeit des Zeitservers mit der UTC Zeit geloggt.

## 6.5 Organisation

Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen sind dem CPS (Ref. [5]) unter Paragraph 5 zu entnehmen. Einzelne Bereiche können in eigenständigen Dokumenten vorliegen, die nicht zwingend veröffentlicht werden. Alle Sicherheitsmassnahmen entsprechen den Vorgaben des ZertES (Ref. [4]), den TAV (Ref. [7]) sowie den dort referenzierten Dokumenten, insbesondere dem ETSI EN 319 421 (Ref. [1]).

### 6.5.1 Kosten

Die Gebühren sind im Rahmenvertrag zwischen der Swiss Government PKI und ihren Kunden aufgeführt.