Time-stamping Policy

Für die „Time-Stamping Authority“ der Swisscom IT Services Finance S.E.

Version: 3.1

Datum: 27. Januar 2022

Swisscom IT Services Finance S.E. ("Swisscom ITSF")

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
3.0	17.02.2020	Kerstin Wagner	Erstellung einer TP EU aus der TP v3.8
3.0	15.07.2020	QTSP Board	Freigabe
3.1	11.01.2022	Kerstin Wagner	Anpassung der Adresse von Swisscom ITSF, der CRL und OCSP Informationen sowie Ergänzung des Aufbaus des Zeitstempel Tokens (Kap 4.5.3), Update der Versionen in Kap. 1.1 und 8.1
3.1	27.01.2022	QTSP Board	Freigabe

Referenzierte Dokumente

[eIDAS-VO]	Europäische Verordnung über elektronische Identifizierung, Authentisierung und Vertrauensdienste (Nr. 910/2014)
[SVG]	Österreichisches Signatur- und Vertrauensdienstegesetz
[SVV]	Österreichische Signatur- und Vertrauensdiensteverordnung
[ETSI TS 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319 401]	General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI EN 419 411-2]	Policy and security requirements for TSPs; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319 412-5]	Certificate Profiles, Part 5: QCStatements
[ETSI EN 319 421]	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[ETSI EN 319 422]	Time-stamping protocol and electronic time-stamp profiles
[RFC 3161]	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[RFC 3647]	IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework"
[RFC 3739]	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
[CP/CPS]	Zertifikatsrichtlinien von Swisscom ITSF zur Ausstellung von Zertifikaten der Klassen Diamant und Saphir
[Addendum]	zum [CP/CPS]: Profile der Zertifikate, Widerrufslisten und Online Statusabfragen
[NB]	Nutzungsbestimmungen
[Rollenkonzept]	Rollenkonzept SDCS
[Sicherheitskonzept]	Sicherheitskonzept SDCS

Inhaltsverzeichnis Timestamping Policy Swisscom IT Services Finance SE

1 Einleitung

Dieses Dokument beschreibt die Time-stamping Policy (Zeitstempel Richtlinien, nachfolgend "TP") von Swisscom IT Services Finance S.E. (nachfolgend "Swisscom ITSF") als Time-stamping Authority (TSA) zur Ausgabe von Zeitstempel-Objekten gemäss der europäischen Verordnung über elektronische Identifizierung, Authentisierung und Vertrauensdienste [eIDAS-VO] und dem österreichischen Signatur- und Vertrauensdienstegesetz [SVG].

Swisscom ITSF bietet als Vertrauensdienstanbieter neben dem Zertifizierungsdienst für die Ausstellung von fortgeschrittenen und qualifizierten digitalen Zertifikaten zur Nutzung für fortgeschrittene und qualifizierte elektronische Signaturen auch einen qualifizierten Zeitstempeldienst an. Mit diesem Zeitstempeldienst kann die Existenz von digitalen Informationen zu einem bestimmten Zeitpunkt zuverlässig und nachvollziehbar belegt werden.

Diese TP bezieht sich auf die Zertifikatklasse „Time-Stamping“. Diese Zertifikate und die zugehörigen Signaturen erfüllen die Anforderungen, welche die [eIDAS-VO] an qualifizierte Zeitstempel stellt.

1.1 Überblick

Diese TP wurde von Swisscom ITSF zu folgendem Zweck erstellt:

- Erfüllung der Anforderungen an einen Vertrauensdienstanbieter von qualifizierten elektronischen Zeitstempeln gemäss [eIDAS-VO]
- Beschreibung der Dienstleistungen, Rollen, Einschränkungen und Verpflichtungen bei der Verwendung von qualifizierten elektronischen Zeitstempeln von Swisscom ITSF
- Sicherstellung der Interoperabilität bei der Benutzung des Time-stamping Services von Swisscom ITSF.

Die Struktur dieser TP orientiert sich an den Vorgaben des [RFC 3647].

Diese TP entspricht den folgenden Standards des Europäischen Instituts für Telekommunikationsnormen für einen qualifizierten Vertrauensdienstanbieter:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [ETSI EN 319 401]
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; [ETSI EN 319 421]

Um die internationale Zusammenarbeit mit anderen Vertrauensdienstanbietern zu ermöglichen, können die [CP/CPS] und diese TP in andere Sprachen übersetzt werden; massgeblich ist in jedem Fall die deutsche Version in der jeweils aktuellen Fassung.

1.2 Identifikation des Dokuments

Titel:	Swisscom Digital Certificate Services – Time-stamping Policy (TP) für die „Time-Stamping Authority“.
Version:	3.1
Object Identifier:	2.16.756.1.83.100.4.5: Time-stamping Policy (Österreich)

Die OID der Swisscom Digital Certificate Services basiert auf der vom schweizerischen Bundesamt für Kommunikation (BAKOM) zugeteilten RDN.

1.3 Beteiligte der Swisscom Digital Certificate Services

1.3.1 Certificate Authorities (CA)

Root CA

Die Swisscom Root CA ist an keinem Netzwerk angeschlossen und wird nur dann gestartet, wenn sie benötigt wird. Die Root-CA stellt ausschliesslich Zertifikate für unmittelbar nachgelagerte Certificate Authorities (CA) der Swisscom aus.

Unter der Swisscom Root-CA werden die nachfolgenden CAs betrieben;

Time-stamping Service CA (TSS CA)

Zum Ausstellen und Signieren der Zertifikate der Time-stamping Units (TSUs). Sie entspricht der Definition für qualifizierte elektronische Zeitstempel von Art. 42 [eIDAS-VO] sowie [ETSI EN 319 421].

Die Profile für die Zertifikate und Widerrufslisten (CRL) sind im Addendum zum [CP/CPS] detailliert beschrieben.

1.3.2 Time-stamping Unit (TSU)

Unter der Time-stamping Service CA unterhält Swisscom mehrere TSUs. Diese TSUs signieren die Time-stamping Token.

Für den Betrieb der TSUs und die Funktionstrennung gelten die Vorgaben der [ETSI EN 319 401].

Die Profile für die Zertifikate und Widerrufslisten (CRL) sind im Addendum zur [CP/CPS] detailliert beschrieben.

1.3.3 Zeitstempelersteller

Der Zeitstempelersteller sind UID-Einheiten insb. juristische Person. Diese sind verantwortlich für die Tätigkeiten ihrer Mitarbeiter. Es wird deshalb von ihr erwartet, dass sie ihre Mitarbeiter über die korrekte Nutzung von Zeitstempeln informiert. Bei der Verwendung von automatisierten Verfahren zur Anbringung von Zeitstempeln müssen technische Kontrollen zur Überprüfung der Zeitstempel angebracht werden.

1.3.4 Zeitstempel-Objekt Empfänger (Relying Party)

Der Zeitstempel-Objekt Empfänger (nachfolgend Relying Party) ist eine juristische oder natürliche Person, die ein Interesse daran hat, den Zeitpunkt und die Integrität einer Information zu überprüfen. Dazu vertraut diese auf den Zeitstempel eines vertrauenswürdigen Dritten, um den Daten und Angaben des Subscriber zu vertrauen. Zur Prüfung der Gültigkeit des Zeitstempels und der Integrität der Daten muss der Empfänger folgende Prüfungen durchführen:

- Vergleich des neu errechneten Hash-Wertes mit dem Hash im Zeitstempel-Objekt
- Überprüfen, ob die Zertifikats-Kette bis zum Root Zertifikat korrekt ist.

Diese Überprüfung kann z.B. mittels Adobe Reader gemacht werden.

1.4 Nutzung der Zertifikate (Certificate Usage)

Die im Rahmen dieser TP definierte ausstellende CA, deren privaten Schlüssel und die ausgestellten Zertifikate werden ausschliesslich zum Signieren der Zertifikate der TSUs verwendet.

Die privaten Schlüssel und die Zertifikate der TSUs können lediglich zur Erstellung von Zeitstempel-Signaturen benutzt werden.

Mittels eines Zeitstempels kann bewiesen werden, dass Daten zu einem bestimmten Zeitpunkt existiert haben und seither nicht mehr verändert wurden (z.B. Archivierung von Daten des elektronischen Geschäftsverkehrs oder eingescannte Papierdokumente).

1.5 Verwaltung der Time-stamping Policy

Herausgeberin dieses Dokuments ist:

Swisscom IT Services Finance S.E.
Swisscom Trust Services
Mariahilfer Strasse 123/3
A-1060 Wien

Änderungen dieser TP werden durch das QTSP Board der Swisscom Digital Certificate Services genehmigt.

1.6 Schlüsselwörter und Begriffe

Schlüsselwörter und Begriffe sind dem Kapitel 1.6 der [CP/CPS] zu entnehmen.

1.7 Abkürzungen

CA	Certificate Authority
CP/CPS	Zertifikats-Richtlinien (Certificate Policy und Certification Practice Statement)
eIDAS-VO	Europäische Verordnung über elektronische Identifizierung, Authentisierung und Vertrauensdienste
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol, Online Dienst zum Abfragen der Gültigkeit von Zertifikaten, gemäss RFC 6960
SDCS	Swisscom Digital Certificate Services
TP	Time-Stamping Policy
TSA	Time-Stamping Authority
TSS	Time-Stamping Service
TSU	Time-stamping Unit
UTC	Universal Coordinated Time (ehemals GMT)

2 Veröffentlichungen und Verantwortung für den Verzeichnisdienst

Die Angaben sind dem [CP/CPS], Kapitel 2, zu entnehmen.

3 Verpflichtungen

Dieses Kapitel enthält alle Verpflichtungen, Verbindlichkeiten, Garantien und Verantwortungen der:

- Time-Stamping Authority (TSA),
- Zeitstempelersteller und
- Zeitstempel-Objekt Empfänger (Relying Party).

Die Verpflichtungen und Verantwortungen werden durch gegenseitige Verträge geregelt, die zwischen den Parteien abgeschlossen werden.

3.1 Verpflichtungen der Time-stamping Authority (TSA)

Swisscom ITSF verpflichtet sich, alle im Rahmen dieser TP und der zugehörigen [CP/CPS] beschriebenen Aufgaben zur Umsetzung der Vorgaben der [eIDAS-VO] und der zugehörigen technischen Standards [ETSI EN 319 401] sowie [ETSI EN 319 421] einzuhalten

Swisscom ITSF garantiert, dass alle Anforderungen an die TSA, einschliesslich Abläufe und Verfahren bezogen auf die Ausgabe der Zeitstempel-Objekte, Reviews der Systeme und Sicherheits-Audits, in Übereinstimmung mit den Prozessen in Kapitel 4 eingehalten werden.

3.1.1 TSA Verpflichtungen gegenüber Zeitstempelersteller

Swisscom ITSF garantiert permanenten Zugang zum Zeitstempel-Dienst (7x24h), ausser bei geplanten technischen Unterbrüchen und beim Fehlen einer genauen Zeitbasis, bei Unterbrüchen aufgrund höherer Gewalt, Naturereignissen (z.B. Blitzschlag in kritische Geräte, Elementarereignisse), Streik oder unvorhersehbaren behördlichen Restriktionen.

Während Wartungsfenstern können Service-Einschränkungen auftreten. Technische Unterbrüche werden in separaten Dokumenten über die Wartungen der Installationen und Systeme beschrieben.

Im Weiteren garantiert Swisscom ITSF folgendes:

- Betrieb und Ausbau einer zuverlässigen Informations- und Kommunikations-Infrastruktur.
- Einhaltung von Eigentumsrecht, Lizenzen oder ähnlichen Gesetzen.
- Die angebotenen Dienste stimmen mit den Vorschriften überein, wie sie in Kapitel 4 beschrieben sind.
- Die ausgestellten Zeitstempel-Objekte enthalten eine korrekte Zeit und entsprechen dem definierten Format.

3.2 Verpflichtung der Subscriber

Subscriber müssen beim Bezug der Zeitstempel Objekte die digitale Signatur der TSU darauf überprüfen, ob das TSU Zertifikat nicht ungültig erklärt worden ist. Die aktuelle Bezugsadresse für OCSP ist im TSU-Zertifikat angegeben.

3.3 Verpflichtungen der Relying Party

Die Relying Party ist verpflichtet, die Signatur des Zeitstempel-Objektes zu prüfen. Anschliessend kann der selbst erzeugte Hash-Wert mit dem im Zeitstempel-Objekt enthaltenen Hash-Wert verglichen werden. Stimmen diese überein, ist die Integrität des Dokumentes gewährleistet. Für den Fall, dass Überprüfung der Integrität des Dokumentes nach Ablauf der Gültigkeitsdauer des Zertifikates der TSU stattfindet, muss die Relying Party folgendes unternehmen:

- Überprüfen, ob das für das Zeitstempel-Objekt verwendete Zertifikat noch gültig ist.

- In der aktuellen TP überprüfen, ob die Hash-Funktion, die im Zeitstempel-Objekt vermerkt ist, noch sicher ist.
- In der aktuellen TP überprüfen, ob die Länge der von der TSA verwendeten kryptografischen Verfahren (Schlüssellänge und Algorithmen), noch als sicher gelten.

Weitere Verpflichtungen der Relying Party sind in Kapitel 1.3.4 und in weiteren Vereinbarungen zwischen den Parteien beschrieben.

4 TSA Verfahren

4.1 Kryptografische Algorithmen und Schlüssellängen

Die eingesetzten kryptografischen Algorithmen und deren Schlüssellängen orientieren sich an den Veröffentlichungen der ETSI (siehe [ETSI TS 119 312]) und sind mindestens:

- RSA 8192 SHA256WithRSAandMGF1 für den CA 4 Root-Key
- RSA 4096 SHA256WithRSAandMGF1 für die CAs der nachfolgenden Stufe (Level 1) und die TSS CA
- RSA 3072 SHA-256 für Enduser Zertifikate und die Zertifikate der TSUs

Weitere Details (wie z.B. Padding-Algorithmen) sind im [Addendum] Profile der Zertifikate, Widerrufslisten und Online Statusabfragen definiert.

4.2 Unterstützte Hash-Algorithmen

Die folgenden Hash-Algorithmen werden unterstützt:

- SHA-256
- SHA-384
- SHA-512

Falls der Zeitstempel-Request einen anderen Hash-Algorithmus enthält, wird der Zeitstempel-Request zurückgewiesen. Die Rückweisung erfolgt durch den entsprechenden Status im resultierenden Zeitstempel-Objekt.

4.3 Zugriff und Authentisierung

Zur Sicherstellung der Nachvollziehbarkeit gewährt Swisscom ITSF nur authentisierten Benutzern Zugriff auf den Zeitstempel-Dienst. Momentan wird folgendes Authentisierungsverfahren unterstützt:

- All-in Signing Service mit Basic Authentication über SSL/TLS

4.4 Schlüsselmanagement

Die Zertifikate von Swisscom Digital Certificate Services haben folgende Gültigkeitszeiträume:

- Zertifikat der Root-CA maximal 20 Jahre
- Zertifikate der Issuing CAs inkl. TSS CA maximal 10 Jahre
- Zertifikate der TSUs maximal 3 Jahre

Die Verfahren und Kontrollen zum Lebenszyklus und Sicherung (Backup) der eingesetzten HSM und der privaten Schlüssel der TSS CA und TSUs entsprechen den in der [CP/CPS] beschriebenen Verfahren.

Auf der TSS CA oder einer TSU ist jeweils nur ein einziger Signaturschlüssel aktiv.

Die TSS CA verwendet ihren eigenen privaten Schlüssel (Signaturschlüssel). Der private Schlüssel einer TSS CA wird in zwei redundanten kryptografischen Modulen gehalten, er ist auf diesen beiden kryptografischen Modulen jedoch mit demselben öffentlichen Schlüssel verknüpft.

Jede TSU verwendet ihr eigenes Zertifikat und ihr eigenes Schlüsselpaar (Signatur- und Prüfschlüssel).

Die Zertifikate der TSS CA und der TSUs werden auf dem in der [CP/CPS] definierten Verzeichnis (Repository) publiziert.

4.5 Zeitstempel

Zeitstempel werden erst ausgestellt, wenn das Zertifikat der ausstellenden TSU im kryptografischen Modul (HSM) hinterlegt ist und werden nur ausgestellt, solange das Zertifikat der ausstellenden TSU gültig ist.

4.5.1 Genauigkeit

Die Genauigkeit der Zeit, die im Zeitstempel-Objekt verwendet wird, beträgt maximal 500 ms Abweichung von der UTC (Universal Time Coordinated) Zeit.

Im Falle, dass die Referenz-Uhr keine zuverlässige Zeitbasis mehr hat oder die Zeitdifferenz des Zeitservers zur UTC Zeit grösser als 500 ms ist, wird ein Alarm ausgelöst und der Service automatisch eingestellt, da die TSA in diesem Fall nicht mehr im Stande ist, die Zeit gemäss Kapitel 4.5.1 "Genauigkeit" zu liefern. Es werden keine Zeitstempel-Objekte mehr generiert, bis die Referenz-Uhr wieder kalibriert ist.

4.5.2 Zeitstempel-Requests

Das Format der Zeitstempel-Requests ist im [RFC 3161] beschrieben.

Feld X.509	Werte, OID's	Bemerkungen
version	1,	Version 2
MessageImprint		
hashAlgorithm	AlgorithmIdentifier SHA-256 SHA-384 SHA-512	Hash Algorithmus, der zur Erstellung des Hash-Wertes benutzt wurde
hashedMessage	[OCTEC STRING]	Hash-Wert
reqPolicy	{ 2 16 756 1 83 100 4 5 }	optional: OID dieser TP
nonce	[INTEGER]	optional: Request, dieses Nonce im resultierenden Zeitstempel-Objekt einzutragen
certReq	[BOOLEAN]	Default FALSE: Request, das Zertifikat im resultierenden Zeitstempel-Objekt zu integrieren.
extensions	IMPLICIT Extensions	optional

4.5.3 Zeitstempel-Token

Feld X.509	Werte, OID's	Bemerkungen
version	1,	Version 2
serialNumber	[Integer]	positive Zahl
issuer	{ "CN= Swisscom TSU 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
TimeStampResponse		
PKIStatusInfo	- granted (0), a TimeStampToken, as requested, is present. - grantedWithMods (1), a TimeStampToken, with modifications, is present. - rejection (2), - waiting (3), - revocationWarning (4), a revocation is imminent - revocationNotification (5), a revocation has occurred	PKIStatus
PKIFailureInfo	- badAlg (0), unerkannter oder nicht unterstützter Algorithmus Identifier. - badRequest (2), Transaktion nicht erlaubt oder unterstützt. - badDataFormat (5), die übermittelten Daten haben ein falsches Format. - timeNotAvailable (14), die Zeitquelle der TSA ist nicht verfügbar. - unacceptedPolicy (15), die angeforderte TSA-Richtlinie wird von der TSA nicht unterstützt. - unacceptedExtension (16), die angeforderte Erweiterung wird von der TSA nicht unterstützt. - addInfoNotAvailable (17), die angeforderten zusätzlichen Informationen konnten nicht verstanden werden oder sind nicht verfügbar. - systemFailure (25), die Anfrage kann aufgrund eines Systemfehlers nicht bearbeitet werden (z.B. wenn das Ende der Gültigkeit des privaten Schlüssels der TSU erreicht ist),	optional
policy	{ 2 16 756 1 83 100 4 5 },	OID dieser TP, wie im Request
MessageImprint		
hashAlgorithm	AlgorithmIdentifier	wie im Request
hashedMessage	[OCTEC STRING]	Hash-Wert wie im Request
nonce	[INTEGER]	optional, wie im Request
genTime	GeneralizedTime	Zeitstempel
accuracy	500ms	Genauigkeit
ordering	[BOOLEAN]	Default FALSE
extensions	IMPLICIT Extensions	optional
QCStatement	{ 0 4 0 19422 1 1 },	tsts-EuQCompliance
TSU Certificate	Zertifikat der signierenden TSU	
signingTime	UTCTime	Zeitpunkt der Signatur
signingCertificate	Issuer	ESSCertID
signature	`..... `B }	3072 bit, BIT STRING

4.6 Zeitsynchronisierung mit UTC

Die Zeitkalibrierung wird automatisch vorgenommen. Für die Zeitbasis werden zwei verschiedene externe Zeitsignale korreliert, um sicherzustellen, dass die interne Zeit mit der koordinierten Weltzeit (UTC) synchron ist. Die bei Swisscom ITSF eingesetzte Time-Stamping Infrastruktur besitzt technische Vorrichtungen, um die synchronisierte Zeit innerhalb der deklarierten Genauigkeit zu halten. Swisscom ITSF verfügt auch über Vorkehrungen, um unautorisierte Manipulationen der Uhr zu verhindern.

Die Zeitbasis wird über das Network Time Protocol (NTP) auch an alle Server der Swisscom PKI verteilt.

Das Auftreten einer Leap-second handelt die Zeitserver Appliance selbständig ab.

4.7 TSA Management und Betrieb

4.7.1 Sicherheitsmanagement

Alle Angelegenheiten, die das Sicherheitsmanagement der TSA betreffen, sind in der [CP/CPS] im Detail beschrieben.

4.7.2 Klassifizierung und Betrieb der Systeme

Die Beschreibung der Methoden und Massnahmen zur Sicherstellung der Verfügbarkeit und Stabilität der Swisscom Digital Certificate Services sind im [CP/CPS] Kapitel 5.1 „Infrastrukturelle Sicherheitsmassnahmen“ zu finden.

4.7.3 Personelle Sicherheitsmassnahmen

Anforderungen an das Personal sowie die Rollen, die das Personal einnehmen wird, sind im [CP/CPS] Kapitel 5.3 „Personelle Sicherheitsmassnahmen“ beschrieben.

4.7.4 Infrastrukturelle Sicherheitsmassnahmen

Die Beschreibung der infrastrukturellen Sicherheitsmassnahmen sind in [CP/CPS] Kapitel 5.1 „Infrastrukturelle Sicherheitsmassnahmen“ beschrieben.

4.7.5 Betrieb

Der Zeitstempel-Dienst von Swisscom ITSF verfügt über betriebliche Kontrollen gemäss [ETSI EN 319 401]. Die betrieblichen Kontrollen werden im [CP/CPS] und in eigenständigen Dokumenten, die nicht veröffentlicht werden, geregelt.

4.7.6 Zutrittskontrolle

Die Zutrittskontrollen werden im [CP/CPS] Kapitel 5.1.2 “Zutrittskontrolle” und in eigenständigen Dokumenten, die nicht veröffentlicht werden, geregelt.

4.7.7 Vertrauenswürdiger Einsatz und Unterhalt der Systeme

Das Schlüsselmaterial des Zeitstempel-Dienstes von Swisscom ITSF wird ausschliesslich in vertrauenswürdiger Umgebung gemäss [CP/CPS] Kapitel 6 "Technische Sicherheitsmassnahmen" generiert.

4.7.8 Kompromittierung des Zeitstempel Dienstes

Im Falle eines Kompromittierung oder einer vermuteten Kompromittierung des privaten Schlüssels der TSU oder eines Verlustes der Zeit-Kalibrierung wird der Zeitstempel-Dienst eingestellt und Swisscom ITSF stellt allen Teilnehmern und vertrauenden Parteien eine Beschreibung der aufgetretenen Kompromittierung und Informationen zur möglichen Identifikation der fehlerhaften Zeitstempel-Token zur Verfügung. Die Informationen werden auf dem Swisscom Repository publiziert.

Im Falle einer Kompromittierung des privaten Schlüssels der TSU werden die Verfahren gemäss [CP/CPS] Kapitel 5.7 „Kompromittierung und Wiederherstellung“ durchgeführt.

4.7.9 Einstellung des Zeitstempel Dienstes

Im Falle der Einstellung des Betriebes des Zeitstempel-Dienstes von Swisscom ITSF werden die Verfahren gemäss [CP/CPS] Kapitel 5.8 „Einstellung des Betriebes“ durchgeführt.

4.7.10 Einhaltung der gesetzlichen Vorschriften

Der Zeitstempel-Dienst der Swisscom ITSF wird gemäss europäischer Gesetzgebung, insbesondere der [eIDAS-VO] betrieben.

4.7.11 Logging

4.7.11.1 Allgemeines

Der Zeitstempel-Dienst von Swisscom ITSF verfügt über ein Ereignis Journal, das alle Ereignisse in Zusammenhang mit der Ausstellung von Zeitstempel-Objekten aufzeichnet.

- Alle Zeitstempel-, Schlüsselmanagement- und Zeitsynchronisations-Ereignisse werden mit der genauen Zeit geloggt.
- Die erfolgreiche Ausstellung der Zeitstempel-Objekte wird aufgezeichnet, dabei wird das gesamte Zeitstempel-Objekt geloggt.
- Die Vertraulichkeit und Integrität der Logdateien werden gemäss den definierten Prozessen der [CP/CPS] sichergestellt.
- Die geloggten und archivierten Zeitstempel Objekte können im Rechtsfall auf Anfrage innert 30 Tagen zur Verfügung gestellt werden.
- Alle Zeitstempel-, Schlüsselmanagement- und Zeitsynchronisations-Ereignisse werden für 35 Jahre nach Ablauf der Gültigkeit des Zeitstempel-Objektes aufbewahrt.
- Elektronische Log-Dateien werden auf einen zentralen Syslog Server übertragen und so gegen Zugriff, Löschung und Manipulation geschützt. Die Logdateien sind nur den Systemadministratoren zugänglich.

4.7.11.2 Schlüssel Management

Folgende Ereignisse werden geloggt:

- Alle Ereignisse des Life-Cycles der Zertifikate der TSS CA und der TSUs.
- Alle Ereignisse des Life-Cycles der TSS CA und TSU Signaturschlüssel, insbesondere Schlüsselerzeugung, Schlüsselerneuerung, Schlüsselbackup und Schlüsselvernichtung.

4.7.11.3 Zeitsynchronisierung

Folgende Ereignisse werden geloggt:

- Alle Ereignisse des Zeitstempel-Servers in Bezug auf die Kalibrierung.
- alle Nachweise über den Verlust der Synchronisierung der Zeit des Zeitservers mit der UTC Zeit.
- Verlauf der Abweichung der Zeit des Zeitservers zur UTC-Zeit.

5 Organisation

Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen sind dem [CP/CPS] Kapitel 5 zu entnehmen.

6 Konformitätsprüfung (Compliance Audits) und andere Assessments

Die Services, Prozesse und Sicherheitsmassnahmen basieren auf den folgenden Gesetzen und Regularien:

- die CP/CPS der Swisscom Digital Certificate Services sowie zugehörige Dokumente wie Sicherheitskonzept, Rollenkonzept etc.
- diese Time-stamping Policy
- Verordnung (EU) 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO), in der Fassung vom 29.01.2015
- Österreichisches Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz (SVG) vom 1. Juli 2016
- Österreichische Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung (SVV) vom 2. August 2016
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers; [ETSI EN 319 401] (2018-04)
- Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; [ETSI EN 319 421] (2016-03)
- Time-stamping protocol and time-stamp token profiles; [ETSI EN 319 **422]**) (2016-03)

Die Einhaltung der Vorschriften wird von der zuständigen Prüfstelle regelmässig verifiziert.

7 Rahmenvorschriften

Die Regelungen sind dem [CP/CPS], Kapitel 9 zu entnehmen.

Time-stamping Policy CH

Für die „Time-Stamping Authority“ der Swisscom (Schweiz) AG

Version: 1.1

Datum: 27. Januar 2022

Swisscom (Schweiz) AG. ("Swisscom")

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
1.0	24.09.2020	Ingolf Rauh	Überarbeitung bez. der neuen Zeitstempel
1.0	18.01.2021	QTSP Board	Freigabe
1.1	13.01.2022	Kerstin Wagner	Update der Versionen in Kap. 1.1. und 8.1
1.1	27.01.2022	QTSP Board	Freigabe

Referenzierte Dokumente

[ETSI TS 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319 401]	General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI EN 419 411-2]	Policy and security requirements for TSPs; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319 412-5]	Certificate Profiles, Part 5: QCStatements
[ETSI EN 319 421]	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[ETSI EN 319 422]	Time-stamping protocol and electronic time-stamp profiles
[RFC 3161]	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[RFC 3647]	IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework"
[RFC 3739]	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
[CP/CPS]	Zertifikatsrichtlinien von Swisscom zur Ausstellung von Zertifikaten der Klassen Diamant und Saphir
[Addendum]	zum [CP/CPS]: Profile der Zertifikate, Widerrufslisten und Online Statusabfragen
[NB]	Nutzungsbestimmungen
[Rollenkonzept]	Rollenkonzept SDCS
[Sicherheitskonzept]	Sicherheitskonzept SDCS
[TP Swisscom ITSF]	Timestamping Policy für die „Time-Stamping Authority“ der Swisscom IT Services Finance S.E.
[ZertES]	Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, [ZertES]), Stand am 1. Januar 2017
[VZertEs]	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate, (Verordnung über die elektronische Signatur, [VZertES])
[TAV]	Anhang der Verordnung des BAKOM vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Technische und administrative Vorschriften [TAV])

Inhaltsverzeichnis Timestamping Policy Swisscom (Schweiz) AG

1 Einleitung

Dieses Dokument beschreibt die Time-stamping Policy (Zeitstempel Richtlinien, nachfolgend "TP") von Swisscom (Schweiz) AG (nachfolgend "Swisscom") als Time-stamping Authority (TSA) zur Ausgabe von Zeitstempel-Objekten gemäss dem schweizerischen Bundesgesetz über elektronische Signaturen [ZertES]

Swisscom bietet als Zertifizierungsdienstanbieterin neben dem Zertifizierungsdienst für die Ausstellung von fortgeschrittenen und qualifizierten digitalen Zertifikaten zur Nutzung für fortgeschrittene und qualifizierte elektronische Signaturen auch einen qualifizierten Zeitstempeldienst an. Mit diesem Zeitstempeldienst kann die Existenz von digitalen Informationen zu einem bestimmten Zeitpunkt zuverlässig und nachvollziehbar belegt werden.

Diese TP bezieht sich auf die Zertifikatklasse „Time-Stamping“. Diese Zertifikate und die zugehörigen Signaturen erfüllen die Anforderungen, welche das Gesetz an qualifizierte Zeitstempel stellt.

Swisscom (Schweiz) AG erzeugen und verwalten das Zeitstempelzertifikat über die Swisscom IT Services Finance S.E. (Swisscom ITSF) als zugelassener Vertrauensanbieter in Wien, Österreich. Insofern referenziert das Dokument in den einzelnen Kapiteln auf die Timestamping Policy der Swisscom IT Services Finance S.E. (nachfolgend „TP Swisscom ITSF“). Bei Referenzen auf die CP/CPS gilt die CP/CPS für Diamant und Saphir Zertifikate der Schweiz [CP/CPS]

1.1 Überblick

Siehe Kapitel 1.1 [TP Swisscom ITSF]

Abweichend vom dort genannten Zweck werden nicht die Anforderungen an einen Vertrauensdiensteanbieter von qualifizierten elektronischen Zeitstempel gemäss eIDAS, sondern die Anforderungen an einen Zertifizierungsdiensteanbieter von qualifizierten elektronischen Zeitstempeln gemäss ZertES erfüllt

1.2 Identifikation des Dokuments

Siehe Kapitel 1.2 [TP Swisscom ITSF]

1.3 Beteiligte der Swisscom Digital Certificate Services

Siehe Kapitel 1.3 [TP Swisscom ITSF]

1.4 Nutzung der Zertifikate (Certificate Usage)

Siehe Kapitel 1.4 [TP Swisscom ITSF]

1.5 Verwaltung der Time-stamping Policy

Herausgeberin dieses Dokuments ist:

Swisscom (Schweiz) AG
Swisscom Trust Services
Pfingstweidstrasse 51
8005 Zürich

Änderungen dieser TP werden durch das QTSP Board der Swisscom Digital Certificate Services genehmigt.

1.6 Schlüsselwörter und Begriffe

Schlüsselwörter und Begriffe sind dem Kapitel 1.6 der [CP/CPS] zu entnehmen.

1.7 Abkürzungen

CA	Certificate Authority
CP/CPS	Zertifikats-Richtlinien (Certificate Policy und Certification Practice Statement)
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
SDCS	Swisscom Digital Certificate Services
TP	Time-Stamping Policy
TSA	Time-Stamping Authority
TSS	Time-Stamping Service
TSU	Time-stamping Unit
UTC	Universal Coordinated Time (ehemals GMT)
ZertES	Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, [ZertES]), Stand am 1. Januar 2017

2 Veröffentlichungen und Verantwortung für den Verzeichnisdienst

Die Angaben sind dem [CP/CPS], Kapitel 2, zu entnehmen.

3 Verpflichtungen

Siehe Kapitel 3 [TP Swisscom ITSF].

4 TSA Verfahren

Siehe Kapitel 4 [TP Swisscom ITSF] mit Ausnahme von Kapitel 4.7.10 «Einhaltung der gesetzlichen Vorschriften», diese sind wie folgt:

Der Zeitstempel-Dienst der Swisscom wird gemäss schweizerischer Gesetzgebung, insbesondere dem [ZertES] betrieben.

5 Organisation

Infrastrukturelle, organisatorische und personelle Sicherheitsmassnahmen sind dem [CP/CPS] Kapitel 5 zu entnehmen.

6 Konformitätsprüfung (Compliance Audits) und andere Assessments

- die [CP/CPS] der Swisscom Digital Certificate Services sowie zugehörige Dokumente wie Sicherheitskonzept, Rollenkonzept etc.
- diese Time-stamping Policy
- Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, Stand am 1. Januar 2017
- Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate, (Verordnung über die elektronische Signatur, VZertES) vom 23. November 2016
- Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate, Inkrafttreten 1.1.2017

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers; [ETSI EN 319 401] (2018-04)
- Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; [ETSI EN 319 421] (2016-03)
- Time-stamping protocol and time-stamp token profiles; [ETSI EN 319 422]) (2016-03)

7 Rahmenvorschriften

Die Regelungen sind der [CP/CPS], Kapitel 9 zu entnehmen.