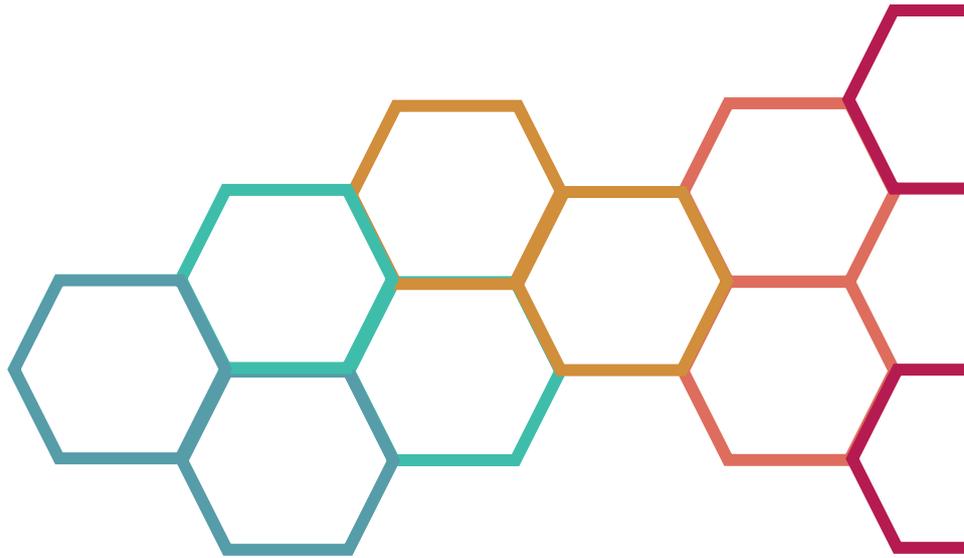


Timestamping Policy der SIGN8 GmbH



Version: 1.1
Datum: 25.11.2024

Dokumentationshistorie

Version	Anmerkung	Datum
1.0	Erweiterung des Dokuments im Rahmen der Prüfung der Einhaltung der Vorgaben der Verordnung (EU) Nr. 2024/1183 des europäischen Parlamentes und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 hinsichtlich der Schaffung eines europäischen Rahmens für die digitale Identität.	09.10.2024
1.1	Erweiterung des Dokuments zur Erfüllung weiterer ETSI Anforderungen	25.11.2024

1.	Einleitung.....	1
1.1.	Überblick.....	1
1.2.	Name und Kennung des Dokumentes	2
1.3.	Abkürzungen.....	2
1.4.	Verwaltung der Zertifikatsrichtlinie.....	3
1.4.1.	Kontaktinformationen.....	3
1.4.2.	Pflege der Richtlinie.....	3
2.	Gesamtkonzept	3
2.1	Allgemein.....	3
2.2	Beteiligte der SIGN8 Zertifikatshierarchie	3
2.2.1	Certificate Authorities (CA)	3
2.2.2	Zeitstempelanbieter (TSA).....	4
2.2.3	Zeitstempeldienst Nutzer	4
2.2.4	Zeitstempeldienst Vertrauende Dritter	4
2.3	Nutzung der Zertifikate.....	4
3.	Veröffentlichungen und Verantwortung für den Verzeichnisdienst.....	5
4.	Verpflichtungen, Richtlinien und Verfahren	5
4.1	Unzulässige Verwendung des Dienstes	5
4.1	Verpflichtungen der Timestamping Authority (TSA).....	5
4.2	Verpflichtung der Nutzer.....	6
4.3	Verpflichtungen der Vertrauenden Dritter.....	6
4.4	Anwendbares Recht.....	6
4.5	Verfügbarkeit des Zeitstempeldienstes.....	6
5.	Verfahren zur Verwaltung und Betrieb des Zeitstempeldienstes.....	7
5.1	Kryptografische Algorithmen und Schlüssellängen.....	7
5.2	Unterstützte Hash-Algorithmen.....	7
5.3	Zugriff und Authentisierung.....	7

5.4	Schlüsselmanagement.....	7
5.5	Zeitstempel	8
5.5.1	Genauigkeit.....	8
5.6	TSA-Management und Betrieb.....	9
5.6.1	Sicherheitsmanagement	9
5.6.2	Klassifizierung und Betrieb der Systeme	9
5.6.3	Personelle Sicherheitsmaßnahmen.....	9
5.6.4	Infrastrukturelle Sicherheitsmaßnahmen.....	9
5.6.5	Betrieb.....	9
5.6.6	Zutrittskontrolle.....	9
5.6.7	Vertrauenswürdiger Einsatz und Unterhalt der Systeme.....	10
5.6.8	Kompromittierung des Zeitstempel Dienstes.....	10
5.6.9	Beendigung des Zeitstempel Dienstes.....	10
5.6.10	Einhaltung der gesetzlichen Vorschriften.....	10
5.6.11	Logging	11
6.	Organisation.....	12
7.	Profile von Zertifikaten	12
7.1	CA-Zertifikat	12
7.2	TSU-Zertifikate für Zeitstempel.....	15
8.	Konformitätsprüfung (Compliance Audits).....	17
9.	Rahmenvorschriften	18

1. Einleitung

Die SIGN8 GmbH ist qualifizierter Vertrauensdiensteanbieter (VDA), gemäß der Verordnung (EU) Nr. 2024/1183 des Europäischen Parlaments und des Rates vom 23. Juli 2014. Der VDA bietet die folgenden qualifizierten Vertrauensdienste an:

- Erstellung und Verwaltung von qualifizierten Zertifikaten für elektronische Signaturen, gemäß Anhang 1 der Verordnung (EU) Nr. 2024/1183.
- Erstellung und Verwaltung von qualifizierten Zertifikaten für elektronische Siegel, gemäß Anhang 3 der Verordnung (EU) Nr. 2024/1183.
- Erstellung und Verwaltung von qualifizierten Zertifikaten für elektronische Zeitstempel, gemäß Anhang 42 der Verordnung (EU) Nr. 2024/1183.

Maßgeblich ist allein die deutsche Fassung dieser Timestamping Policy (TSP).

Soweit nicht ausdrücklich anders vermerkt, beinhaltet das TSA Disclosure Statement keine Zusicherungen, Garantien oder Gewährleistungen.

1.1. Überblick

Der Zeitstempelanbieter (Timestamping Authority, im Folgenden die TSA genannt) ist die SIGN8 GmbH

Fürstenrieder Str. 5

80687 München.

Die SIGN8 GmbH ist qualifizierter Vertrauensdiensteanbieter gemäß der VO (EU) Nr. 2024/1183.

Die TSA verfügt über die Konformitätsbewertung durch eine anerkannte Konformitätsbewertungsstelle, welche die Einhaltung der in der VO (EU) Nr. 2024/1183 sowie den Normen ETSI EN 319 401, ETSI EN 319 421 und ETSI EN 319 422 festgelegten Anforderungen bestätigt.

Zertifikate, die von der TSA ausgegeben werden, unterliegen immer der Zertifizierung im Sinne der eIDAS-VO, VDG, VDV, ETSI EN 319 401, ETSI EN 319 421 und ETSI EN 319 422. Die Bereitstellung des Zeitstempeldienstes steht im Einklang mit der ETSI Best practices time stamp policy (BTSP - OID: 0.4.0.2023.1.1) gemäß ETSI EN 319 421.

Der TSA kann Teilaufgaben an Partner oder externe Anbieter auslagern.

Das CPS umfasst allgemeine Regelungen, Maßnahmen und Konzepte des VDA, die auch für den Zeitstempeldienst gelten. Die aktuelle Fassung des CPS können Sie über <https://sign8.eu/trust> abrufen.

1.2. Name und Kennung des Dokumentes

Dokumentenname: Timestamping Policy der SIGN8 GmbH

Kennzeichnung (OID): 1.3.6.1.4.1.58197.1.10.0

Version: 1.0

Der angebotene Dienst entspricht dem folgenden Service-Identifizier:

- URI: <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

1.3. Abkürzungen

CA	Certificate Authority
CPS	Zertifikats-Richtlinien (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
TSP	Timestamping Policy
TSA	Timestamping Authority
TSS	Timestamping Service
TSU	Timestamping Unit
EUTL	European Trust List
UTC	Universal Coordinated Time (ehemals GMT)

1.4. Verwaltung der Zertifikatsrichtlinie

1.4.1. Kontaktinformationen

Eine Kontaktaufnahme kann über folgende Adressen erfolgen:

SIGN8 GmbH

Fürstenrieder Str. 5

80687 München

E-Mail: info@sign8.eu

1.4.2. Pflege der Richtlinie

Diese Policy behält Gültigkeit, solange sie nicht von der zuständigen Instanz widerrufen wird. Sie wird bei Bedarf fortgeschrieben und erhält dann jeweils eine neue aufsteigende Versionsnummer.

2. Gesamtkonzept

2.1 Allgemein

Die SIGN8 TSA stellt ausschließlich qualifizierte elektronische Zeitstempel aus. Die Zeitstempel sind konform zu den Profilanforderungen der ETSI EN 319 422 [5].

2.2 Beteiligte der SIGN8 Zertifikatshierarchie

2.2.1 Certificate Authorities (CA)

Root CA

Die SIGN8 Root CA ist durch verteilte Smart Cards geschützt und wird nur bei Bedarf aktiviert. Sie stellt ausschließlich Zertifikate für direkt untergeordnete Certificate Authorities (CA) der SIGN8 GmbH aus. Unter der SIGN8 Root CA werden die folgenden CAs betrieben:

Time-stamping Service CA

Dient zum Ausstellen und Signieren der Zertifikate der TimeStamping Units (TSUs). Sie entspricht den Anforderungen für qualifizierte elektronische Zeitstempel gemäß Artikel 42 der eIDAS-VO sowie ETSI EN 319 421.

Weitere nicht für den Zeitstempeldienst relevanten CAs und deren Profile für die Zertifikate sind im CPS beschrieben.

Timestamping Unit (TSU)

Es werden mehrere TSUs, die die Timestamping Token signieren, betrieben. Der Betrieb der TSUs und die Trennung der Funktionen erfolgen gemäß den Vorgaben der ETSI EN 319 401.

2.2.2 Zeitstempelanbieter (TSA)

Der Zeitstempelanbieter (TSA) ist die SIGN8 GmbH, die für die Tätigkeiten ihrer Mitarbeiter verantwortlich ist. Daher wird erwartet, dass sie ihre Mitarbeiter über die korrekte Nutzung von Zeitstempeln informiert. Bei der Verwendung automatisierter Verfahren zur Anbringung von Zeitstempeln werden technische Kontrollen eingesetzt, um die Zeitstempel zu überprüfen.

Der TSA obliegt die Verantwortung für den Betrieb einer oder mehrerer TSUs, die im Auftrag der TSA, Zeitstempel erstellen und signieren.

Der TSA kann Dritte für die Erbringung von Teilen des Zeitstempeldiensts heranziehen. Der TSA obliegt jedoch stets die Gesamtverantwortung und er stellt sicher, dass die in diesem Dokument genannten Anforderungen und Richtlinien erfüllt werden

2.2.3 Zeitstempeldienst Nutzer

Die TSA bietet qualifizierte elektronische Zeitstempel nicht direkt Endanwendern an.

2.2.4 Zeitstempeldienst Vertrauende Dritter

Vertrauende Dritte sind Zeitstempel-Objekt Empfänger. Der Zeitstempel-Objekt Empfänger 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 DSS Demonstration WebApp

<https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation> gemacht werden.

2.3 Nutzung der Zertifikate

Die in dieser TSP definierte ausstellende CA, ihre privaten Schlüssel und die ausgestellten Zertifikate werden ausschließlich zum Signieren der Zertifikate der TSUs verwendet. Die privaten Schlüssel und Zertifikate der TSUs dürfen nur zur Erstellung von Zeitstempel-

Signaturen genutzt werden. Ein Zeitstempel beweist, dass Daten zu einem bestimmten Zeitpunkt existierten und seither unverändert geblieben sind.

3. Veröffentlichungen und Verantwortung für den Verzeichnisdienst

Die Angaben sind dem CPS, Kapitel 2 zu entnehmen.

4. Verpflichtungen, Richtlinien und Verfahren

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

- Timestamping Authority (TSA),
- Zeitstempelersteller und
- Zeitstempeldienst Nutzer

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

4.1 Unzulässige Verwendung des Dienstes

Die Verwendung von Zeitstempeln für Dienste und Systeme, die bei Störungen oder Ausfällen zu großen materiellen oder immateriellen Schäden führen sowie Schäden an Leib oder Leben verursachen können, ist nicht gestattet. Hierzu zählen Atomkraftwerke, Chemieproduktionsanlagen oder Luftfahrtsysteme. Hiervon abweichende Regelungen können im Einzelnen mit dem TSA schriftlich vereinbart werden.

4.1 Verpflichtungen der Timestamping Authority (TSA)

SIGN8 verpflichtet sich, alle in dieser Policy und dem zugehörigen CPS beschriebenen Aufgaben zur Umsetzung der Vorgaben der eIDAS-VO und der relevanten technischen Standards ETSI EN 319 401 und ETSI EN 319 421 zu erfüllen. SIGN8 garantiert, dass alle Anforderungen an die TSA, einschließlich der Abläufe und Verfahren zur Ausgabe der Zeitstempel-Objekte sowie der Systemüberprüfungen und Sicherheits-Audits, gemäß den Prozessen in Kapitel 5 eingehalten werden.

4.2 Verpflichtung der Nutzer

Die SIGN8 GmbH stellt seinen Zeitstempeldienst nicht unmittelbar Endnutzern zur Verfügung.

4.3 Verpflichtungen der Vertrauenden Dritter

Es gelten die mit dem TSA geschlossenen einzelvertraglichen Vereinbarungen.

Die Zertifikatnehmer und Dritte dürfen dem Zeitstempel nur vertrauen, wenn folgende Bedingungen erfüllt sind:

- Der Zeitstempel wurde korrekt signiert und der private Schlüssel, der zur Signatur verwendet wurde, war bis zum Zeitpunkt der Verifizierung nicht widerrufen.
- Die Gültigkeit des Zertifikats, das zur Erstellung des Zeitstempels verwendet wurde, wird durch den Statusabfragedienst (OCSP) bestätigt.
- Der Zeitstempel wird gemäß den zulässigen Nutzungsarten verwendet und eventuelle Einschränkungen in der Zeitstempel-Policy wurden beachtet.
- Die Zertifikatskette kann erfolgreich bis zu einem vertrauenswürdigen Root-Zertifikat verifiziert werden, das in der EUTL (European Trusted List) aufgeführt ist.
- Alle weiteren Vereinbarungen und sonstigen Vorsichtsmaßnahmen wurden eingehalten.

4.4 Anwendbares Recht

Es gilt deutsches Recht sowie das Recht der europäischen Union. Der Gerichtsstand des TSA ist München.

4.5 Verfügbarkeit des Zeitstempeldienstes

Der Zeitstempeldienst wird von der TSA in Rechenzentren hochverfügbar betrieben und ist 24/7 erreichbar. Im Falle eines Ausfalls wird dieser schnellstmöglich wieder zur Verfügung gestellt.

5. Verfahren zur Verwaltung und Betrieb des Zeitstempeldienstes

5.1 Kryptografische Algorithmen und Schlüssellängen

Die verwendeten kryptografischen Algorithmen und deren Schlüssellängen werden gemäß den Veröffentlichungen der ETSI (siehe ETSI TS 119 312) ausgewählt und sind wie folgt festgelegt:

- Für den CA Root-Key: RSA 4096 mit SHA512RSA
- Für die CAs und die TSS CA: RSA 4096 mit SHA512RSA
- Für Endbenutzerzertifikate und die Zertifikate der TSUs: RSA 4096 mit SHA512RSA oder ECDSA mit SHA512

Weitere Einzelheiten, wie z. B. Padding-Algorithmen, sind im Profil der Zertifikate und Online-Statusabfragedienst festgelegt.

5.2 Unterstützte Hash-Algorithmen

Unterstützt wird ausschließlich der Hash-Algorithmus SHA-512. Sollte ein Zeitstempel-Antrag einen anderen Hash-Algorithmus enthalten, wird der Antrag abgelehnt und im resultierenden Zeitstempel-Objekt durch den entsprechenden Status markiert.

5.3 Zugriff und Authentisierung

Zur Sicherstellung der Nachvollziehbarkeit gewährt SIGN8 nur authentisierten Benutzern Zugriff auf den Zeitstempel-Dienst.

5.4 Schlüsselmanagement

Die Gültigkeitszeiträume der Zertifikate, die von der SIGN8 GmbH ausgestellt werden, werden gemäß den Veröffentlichungen der ETSI (siehe ETSI TS 119 312) definiert und sind wie folgt festgelegt:

- Das Zertifikat der Root-CA hat eine maximale Gültigkeitsdauer von 15 Jahren.
- Die Zertifikate der Ausstellungs-CAs einschließlich der TSS CA haben eine maximale Gültigkeitsdauer von 15 Jahren.
- Die Zertifikate der Zeitstempelunterzeichner (TSUs) haben eine maximale Gültigkeitsdauer von 5 Jahren.

Die TSU-Schlüssel erhalten ein Ablaufdatum. Der öffentliche TSU-Schlüssel hat die Gültigkeitsdauer des TSU-Zertifikats und der private TSU-Schlüssel hat eine 365 Tage kürzere Gültigkeit. Diese Vorgabe wird bei der Erstellung der TSU-Zertifikats berücksichtigt. Es wird sichergestellt, dass vor Ablauf eines privaten TSU-Schlüssels ein neuer privater TSU-Schlüssel zur Verfügung steht. Eine Verwendung der Schlüssel außerhalb ihrer Gültigkeit ist ausgeschlossen.

Die Verfahren und Kontrollen für den Lebenszyklus und die Sicherung der verwendeten Hardware-Sicherheitsmodule (HSM) und der privaten Schlüssel der TSS CA und TSUs entsprechen den im CPS und Sicherheitskonzept beschriebenen Standards.

Jede TSS CA oder TSU hat jeweils nur einen aktiven Signaturschlüssel, welcher exklusiv zum Signieren von Zeitstempel verwendet wird. Die TSS CA verwendet einen eigenen privaten Signaturschlüssel, der redundant in zwei HSMs gespeichert ist, die jedoch denselben öffentlichen Schlüssel verwenden. Der TSU CA Signaturschlüssel wird nicht in weitere HSMs importiert. Jede TSU verwendet ihr eigenes Zertifikat und Schlüsselpaar für Signatur und Verifizierung. Die Zertifikate der TSS CA und der TSUs werden wie im CPS beschrieben veröffentlicht.

Eine TSU erstellt keine Zeitstempel, bis das TSU-Zertifikat vollständig geladen wurde. Vor der Verwendung eines TSU-Zertifikats wird die Zertifikatskette hinsichtlich ihrer Vertraulichkeit überprüft.

5.5 Zeitstempel

Die Zeitstempel werden auf eine sichere Weise ausgestellt und verknüpft die zu signierenden Daten mit der Zeit, sodass die Möglichkeit einer unbemerkten Änderung der Daten vernünftigerweise ausgeschlossen ist. Sie werden nur dann ausgestellt, wenn das Zertifikat der zuständigen TSU im Hardware-Sicherheitsmodule (HSM) hinterlegt ist. Darüber hinaus werden Zeitstempel nur während der Gültigkeitsdauer des Zertifikats und des privaten Schlüssels der ausstellenden TSU ausgestellt und jeglicher Ausstellungsversuch wird nach Ablauf der Gültigkeit abgelehnt von der ausstellenden TSU.

5.5.1 Genauigkeit

Die Zeitstempel enthalten die korrekte Zeit. Die Zeitkalibrierung erfolgt automatisch und in solch einer Weise, dass die TSU-Zeiten innerhalb der maximalen Zeitabweichung bleiben. Hierzu werden Zeitsignale von acht verschiedenen externen UTC(k)-Zeitservern von 3 UTC(k)-

Laboren abgerufen, um sicherzustellen, dass die interne Zeit mit der koordinierten Weltzeit (UTC) synchronisiert ist. Schaltsekunden werden korrekt erkannt, protokolliert und bei der Ausstellung der Zeitstempel berücksichtigt. Die Anpassungen für Schaltsekunden werden standardmäßig in der letzten Minute am Tag der Änderung ausgeführt.

Die Zeitgenauigkeit des Zeitstempels liegt innerhalb einer maximalen Abweichung von 1 Sekunde von der UTC (Universal Time Coordinated). Zeitabweichungen werden erkannt. Sollte die Abweichung mehr als 1 Sekunde betragen oder die Referenzuhr ihre zuverlässige Zeitquelle verlieren, stellt der Zeitstempeldienst automatisch die Ausstellung neuer Zeitstempel ein und benachrichtigt die betroffenen Stellen unverzüglich. In einem solchen Fall kann die TSA die Zeitgenauigkeit nicht mehr garantieren, und es werden keine weiteren Zeitstempel-Objekte generiert, bis die Referenzuhr wieder kalibriert ist.

5.6 TSA-Management und Betrieb

5.6.1 Sicherheitsmanagement

Alle Angelegenheiten, die das Sicherheitsmanagement der TSA betreffen, sind im CPS und im Sicherheitskonzept beschrieben.

5.6.2 Klassifizierung und Betrieb der Systeme

Die Methoden und Maßnahmen zur Sicherstellung der Verfügbarkeit und Stabilität der SIGN8 Trust Services sind im Kapitel 5 "Nicht-bauliche Sicherheitsmaßnahmen" des CPS beschrieben.

5.6.3 Personelle Sicherheitsmaßnahmen

Anforderungen an das Personal sowie die Rollen, die das Personal einnehmen wird, sind im CPS in Kapitel 5.2 „Verfahrensvorschriften“ beschrieben.

5.6.4 Infrastrukturelle Sicherheitsmaßnahmen

Die Beschreibung der infrastrukturellen Sicherheitsmaßnahmen sind in CPS in Kapitel 6 „Technische Sicherheitsmaßnahmen“ beschrieben.

5.6.5 Betrieb

Der Zeitstempel-Dienst von SIGN8 verfügt über betriebliche Kontrollen gemäß ETSI EN 319 401. Die betrieblichen Kontrollen werden im CPS und in eigenständigen Dokumenten, die nicht veröffentlicht werden, geregelt. Die TSU-Einheiten werden vor Gefahren geschützt, welche ihre Zeitgenauigkeit unbemerkt beeinflussen könnten.

5.6.6 Zutrittskontrolle

Die Zutrittskontrollen werden im CPS in Kapitel 5.4.1 "Überwachung des Zutritts" geregelt.

5.6.7 Vertrauenswürdiger Einsatz und Unterhalt der Systeme

Das Schlüsselmaterial des Zeitstempel-Dienstes von SIGN8 wird ausschließlich in vertrauenswürdiger Umgebung gemäß des CPS Kapitel 6 "Technische Sicherheitsmaßnahmen" generiert.

5.6.8 Kompromittierung des Zeitstempel Dienstes

Die TSA verfügt über ein Notfallkonzept, der allen beteiligten Rollen bekannt ist und bei Bedarf umgesetzt wird. Die Verantwortlichkeiten sind klar verteilt.

Im Falle einer kritischen Schwachstelle oder Kompromittierung muss die TSA unverzüglich handeln und entsprechende Maßnahmen ergreifen. In Absprache mit der Aufsichtsbehörde werden die Auswirkungen analysiert und gegebenenfalls weitere Schritte zur Behebung eingeleitet. Die TSA benachrichtigt innerhalb von 24 Stunden nach einem Vorfall die entsprechenden Parteien, wenn es sich um Sicherheitsverletzungen handelt, die erhebliche Auswirkungen auf den bereitgestellten Vertrauensdienst und die verarbeiteten personenbezogenen Daten haben. Dabei stellt die TSA Informationen zur Verfügung, die zur Identifizierung der möglicherweise betroffenen Zeitstempel verwendet werden können, sofern dies nicht die Privatsphäre der Nutzer der TSA oder die Sicherheit der TSA-Dienste verletzt.

Im Falle einer Kompromittierung, einer vermuteten Kompromittierung oder eines Verlustes der Kalibrierung bei der Ausgabe von Zeitstempeln stellt die TSA allen Parteien eine Beschreibung der aufgetretenen Kompromittierung zur Verfügung und unterbricht die TSU-Dienste. Die Beschreibung enthält unter anderem Informationen zur Identifizierung betroffener Zeitstempel.

Sollte der private Schlüssel der TSU kompromittiert sein, werden die entsprechenden Verfahren gemäß Kapitel 4.9 "Widerruf und Suspendierung von Zertifikaten" des CPS durchgeführt.

5.6.9 Beendigung des Zeitstempel Dienstes

Im Falle der Einstellung des Betriebes des Zeitstempel-Dienstes von SIGN8 werden die Verfahren beschrieben im CPS in Kapitel 4.11 „Beendigung des Zertifizierungsdienstes“ durchgeführt.

5.6.10 Einhaltung der gesetzlichen Vorschriften

Der Zeitstempel-Dienst der SIGN8 wird gemäß europäischer Gesetzgebung, insbesondere der eIDAS-VO betrieben.

5.6.11 Logging

Allgemeines

Der Zeitstempel-Dienst von SIGN8 nutzt ein zentrales Logging-System, das folgende Funktionen bietet:

- Alle Ereignisse im Zusammenhang mit Zeitstempeln, Schlüsselverwaltung und Zeitsynchronisation werden mit genauer Zeitangabe protokolliert.
- Die erfolgreiche Ausstellung von Zeitstempel-Objekten wird protokolliert.
- Die Vertraulichkeit und Integrität der Logdateien werden gemäß den festgelegten Prozessen im CPS sichergestellt.

Schlüssel Management

Folgende Ereignisse werden geloggt:

- Alle Ereignisse im Zusammenhang mit den Zertifikaten der TSS CA und der TSUs.
- Alle Ereignisse im Zusammenhang mit der TSS CA und dem TSU Signaturschlüssel, insbesondere Schlüsselerzeugung, Schlüsselerneuerung, Schlüsselbackup und Schlüsselvernichtung.

Zeitsynchronisierung

Folgende Ereignisse werden geloggt:

- Alle Ereignisse des Zeitstempel-Servers in Bezug auf die Kalibrierung, wozu auch die Berücksichtigung von Schaltsekunden zählen.
- alle Vorkommnisse im Zusammenhang mit dem Verlust der Synchronisierung der Zeit des Zeitservers mit der UTC-Zeit.

6. Organisation

Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen sind dem CPS Kapitel 5 zu entnehmen.

7. Profile von Zertifikaten

Die folgenden Kapitel beinhalten die Zertifikatsprofile des VDA.

Alle Zertifikate werden im Format X.509v3 ausgegeben.

Ergänzende Erweiterungen können aufgenommen werden, müssen dabei alle von ETSI EN 319 412-5 referenzierte RFCs entsprechen oder in einem referenzierten Dokument beschrieben sein.

Semantik Identifizierungsattribute können inkludiert werden, müssen den Spezifikationen in ETSI EN 319 412-1 und alle von ETSI EN 319 412-1 referenzierte Normen oder RFCs entsprechen.

7.1 CA-Zertifikat

CA-Zertifikate erhalten die folgenden Erweiterungen:

Feld	Beschreibung	Wert
Signature Algorithm	Signaturalgorithmus	sha512RSA (1.2.840.113549.1.1.13)
Signature Hash Algorithm	Signaturhashalgorithmus	sha512 (2.16.840.1.101.3.4.2.3)
Algorithm Identifier	Schlüsselalgorithmus	RSA (1.2.840.113549.1.1.1)
Key Size	Schlüssellänge	4096 Bits
Aussteller		
countryName (2.5.4.6)	Name Land	DE

State	Name Staat	Bavaria
organizationName (2.5.4.10)	Name Organisation	SIGN8 GmbH
OrganizationalUnitName (2.5.4.11)	Name Organisationseinheit	SIGN8 GmbH ROOT CA 01
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	DE349977882
commonName (2.5.4.3)	Name Inhaber	SIGN8 GmbH ROOT CA 01
Gültigkeit		
NotBefore	Beginn Gültigkeit	Donnerstag, 14. November 2024 14:24:19 (CA 01) Donnerstag, 14. November 2024 14:27:45 (CA 02)
NotAfter	Ende Gültigkeit	Freitag, 11. November 2039 14:24:19 (CA 01) Freitag, 11. November 2039 14:27:45 (CA 02)
Inhaber		
countryName (2.5.4.6)	Name Land	DE
State	Bundesland	Bavaria
organizationName (2.5.4.10)	Name der Organisation	SIGN8 GmbH

OrganizationalUnitName (2.5.4.11)	Name Organisationseinheit	Trust Services
OrganizationIdentifier (2.5.4.97)	Identifizierung Organisation	NTRDE-DED2601V.HRB271573
commonName (2.5.4.3)	Name Inhaber	SIGN8 TIMESTAMP CA 01 SIGN8 TIMESTAMP CA 02
Extensions		
KeyUsage (2.5.29.15)	Verwendungszweck	keyCertSign, cRLSign
ExtendedKeyUsage (2.5.29.37)	Erweiterte Schlüsselverwendung	NICHT GESETZT
basicConstraints (2.5.29.19)	Beschränkung Verwendung ausgestellter Zertifikate	Typ des Antragstellers= Zertifizierungsstelle Einschränkung der Pfadlänge=0
authorityKeyIdentifier (2.5.29.35)	Identifizierung des öffentlichen Schlüssels des Ausstellers	63F07B0C0BB72741E887715176EE3 D62E0FD9D94
subjectKeyIdentifier (2.5.29.14)	Identifizierung des öffentlichen Schlüssels des Inhabers	SIGN8 TIMESTAMP CA 01 CCF02344B03EE11973A8E4812669F 854DA884860 SIGN8 TIMESTAMP CA 02 823932ECFB412238EEF4C3ACF2367 CBF0FDD0ECF
Certificate Policies (2.5.29.32)	Verweis auf das für das jeweilige Zertifikat anwendbare Certificate Practice Statement	policyIdentifier= 1.3.6.1.4.1.58197.1.10.0 (TSA Policy) policyQualifier= https://sign8.eu/trust/

7.2 TSU-Zertifikate für Zeitstempel

Feld	Beschreibung	Wert
Signature Algorithm	Signaturalgorithmus	ecdsa-with-SHA512 (1.2.840.10045.4.3.4) sha512RSA (1.2.840.113549.1.1.13)
Signature Hash Algorithm	Signaturhashalgorithmus	sha512 (2.16.840.1.101.3.4.2.3)
Algorithm Identifier	Schlüsselalgorithmus	ECC (1.2.840.10045.2.1) RSA (1.2.840.113549.1.1.1)
Key Size	Schlüssellänge	256 Bits (ECC) 4096 Bits (RSA)
Aussteller		
countryName (2.5.4.6)	Name Land	DE
State	Name Staat	Bavaria
organizationName (2.5.4.10)	Name Organisation	SIGN8 GmbH
OrganizationalUnitName (2.5.4.11)	Name Organisationseinheit	Trust Services
commonName (2.5.4.3)	Name Inhaber	ECC SIGN8 TIMESTAMP CA 02

		RSA SIGN8 TIMESTAMP CA 01
Gültigkeit		
NotBefore	Beginn Gültigkeit	
NotAfter	Ende Gültigkeit	Maximal 1.825 Tage ab Beginn der Gültigkeit
Inhaber		
commonName (2.5.4.3)	Name TSU Einheit	SIGN8 TSU XX
organizationName (2.5.4.10)	Name TSA Organisation	SIGN8 GmbH
countryName (2.5.4.6)	Land in dem die TSA betrieben wird	DE
Extensions		
keyUsage (2.5.29.15)	Verwendungszweck	digitalSignature, nonRepudiation
Private Key Usage Period NotAfter (2.5.29.16)	Ende Gültigkeit (Privater Schlüssel)	365 Tage weniger als das Ende der Gültigkeit des Zertifikats
ExtendedKeyUsage (2.5.29.37)	Erweiterte Schlüsselverwendung	timeStamping
basicConstraints (2.5.29.19)	Beschränkung Verwendung ausgestellt Zertifikate	Typ Antragsteller = Endeinheit Einschränkung Pfadlänge = keine
authorityKeyIdentifier (2.5.29.35)	Identifizierung des öffentlichen Schlüssels des Ausstellers	ECC 823932ECFB412238EEF4C3ACF2367 CBF0FDD0ECF

		RSA CCF02344B03EE11973A8E4812669F 854DA884860
subjectKeyIdentifier (2.5.29.14)	Identifizierung des öffentlichen Schlüssels des Inhabers	
qcStatements (1.3.6.1.5.5.7.1.3)	Kennzeichner (OID) eIDAS-Konformität qSig /qSeal -Qualifiziertes Zertifikat -Typ (elektr. Signatur/Siegel) -Erzeugung auf SSCD	QcCompliance= 0.4.0.1862.1.1 QcPDS = 0.4.0.1862.1.5
Certificate Policies (2.5.29.32)	Verweis auf das für das jeweilige Zertifikat anwendbare Certificate Practice Statement	policyIdentifier= 1.3.6.1.4.1.58197.1.10.0 (TSA Policy) policyQualifier= https://sign8.eu/trust/
AuthorityInfoAccess	Verweis auf Aussteller und Dienst zur Statusabfrage	OID: calssuers; URI: https://sign8.eu/trust (1.3.6.1.5.5.7.48.2) OID:OCSP; URI: http://ocsp-q.sign8.eu (1.3.6.1.5.5.7.48.1)

Die **qcStatements** enthalten eine Instanz des Statement "esi4-qtstStatement-1" definiert nach ETSI EN 319 422 Anhang B.

8. Konformitätsprüfung (Compliance Audits)

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

- die CPS der SIGN8 GmbH sowie zugehörige Dokumente wie Sicherheitskonzept, Rollenkonzept etc.
- diese Timestamping Policy

- Verordnung (EU) 2024/1183 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO), in der Fassung vom 11.04.2024
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers; ETSI EN 319 401 (2024-03)
- Policy and Security Requirements for Trust Service Providers issuing Time-Stamps; ETSI EN 319 421 (2023-05)
- Time-stamping protocol and time-stamp token profiles; ETSI EN 319 422 (2016-03) inklusive Anhängen

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

9. Rahmenvorschriften

Die Regelungen sind dem CPS Kapitel 9 zu entnehmen.