SIGN8 GmbH
Fürstenrieder Str. 5
80687 München

T: +49 (0)89 / 2153 7472 000
info@sign8.eu
www.sign8.eu

Timestamping Policy der SIGN8 GmbH

Version: 1.2
Datum: 22.01.2026

Unterschrift: Christian Eling

Digitally signed by Christian Eling
Date: 2026.01.26 18:47:49 +01'00'

(Geschäftsführer SIGN8 GmbH)

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
1.2	Kapitel 5. 5. Verfahren zur Verwaltung und Betrieb des Zeitstempeldienstes überarbeitet sowie redaktionelle Anpassungen vorgenommen	22.01.2026

Inhalt

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

1.2 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.

1.3 Name und Kennung des Dokumentes

Dokumentenname:	Timestamping Policy der SIGN8 GmbH
Kennzeichnung (OID):	1.3.6.1.4.1.58197.1.10.0
Version:	1.2

Der angebotene Dienst entspricht dem folgenden Service-Identifier:

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

1.4 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)

1.5 Verwaltung der Zertifikatsrichtlinie

1.5.1 Kontaktinformationen

Eine Kontaktaufnahme kann über folgende Adressen erfolgen:

SIGN8 GmbH
Fürstenrieder Str. 5
80687 München
E-Mail: info@sign8.eu

1.5.2 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:

Timestamping 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 Timestamp-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 für Endanwender an.

2.2.4 Zeitstempeldienst Vertrauende Dritter

Vertrauende Dritte sind Timestamp-Token-Empfänger. Der Timestamp-Token-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 Timestamp-Token
- Überprüfen, ob die Zertifikats-Kette bis zum Vertrauensanker 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.

4.2 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 Timestamp-Token sowie der Systemüberprüfungen und Sicherheits-Audits, gemäß den Prozessen in Kapitel 5 eingehalten werden.

4.3 Verpflichtung der Nutzer

Die Nutzer müssen bei Nutzung des Zeitstempeldienstes 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.

4.4 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 CA-Zertifikat verifiziert werden, das in der EUTL (European Trusted List) aufgeführt ist.
- Alle weiteren Vereinbarungen und sonstigen Vorsichtsmaßnahmen wurden eingehalten.

4.5 Anwendbares Recht

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

4.6 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 SHA-512
- Für die CAs und die TSS CA: RSA 4096 mit SHA-512
- Für Zertifikate der TSUs: RSA 4096 mit SHA-512 oder ECDSA P-521 mit SHA-512

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

5.2 Unterstützte Hash-Algorithmen

Unterstützt werden die Hash-Algorithmen SHA-256, SHA-384 und SHA-512. Sollte ein Zeitstempel-Antrag einen anderen Hash-Algorithmus enthalten, wird der Antrag abgelehnt und im resultierenden Timestamp-Token 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. Die TSS CA verwendet einen eigenen privaten Signaturschlüssel, der redundant in mindestens zwei HSMs gespeichert ist, die jedoch denselben öffentlichen Schlüssel verwenden. Der TSS 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 das Zertifikat hinsichtlich seiner Integrität und Authentizität 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 mindestens acht verschiedenen externen UTC(k)-Zeitservern von mindestens drei 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 Timestamp-Token generiert, bis die Referenzuhr wieder kalibriert ist.

5.5.2 Erweiterungen

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

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, das 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 Timestamp-Token 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.

7.1 CA-Zertifikat

CA-Zertifikate erhalten die folgenden Erweiterungen:

Feld	Kritisch	Wert
Signature Algorithm		sha512RSA (1.2.840.113549.1.1.13)
Signature Hash Algorithm		sha512 (2.16.840.1.101.3.4.2.3)
Algorithm Identifier		RSA (1.2.840.113549.1.1.1)
Key Size		4096 Bits
		Aussteller
countryName **(2.5.4.6)**		DE
State **(2.5.4.8)**		Bavaria
organizationName **(2.5.4.10)**		SIGN8 GmbH
OrganizationalUnitName **(2.5.4.11)**		SIGN8 GmbH ROOT CA 01
organizationIdentifier **(2.5.4.97)**		DE349977882
commonName **(2.5.4.3)**		SIGN8 GmbH ROOT CA 01
		Gültigkeit
NotBefore		*SIGN8 TIMESTAMP CA 01:* Donnerstag, 14. November 2024 14:24:19

		SIGN8 TIMESTAMP CA 02: Donnerstag, 14. November 2024 14:27:45
NotAfter		*SIGN8 TIMESTAMP CA 01:* Freitag, 11. November 2039 14:24:19
		SIGN8 TIMESTAMP CA 02: Freitag, 11. November 2039 14:27:45
Inhaber		
countryName **(2.5.4.6)**		DE
State **(2.5.4.8)**		Bavaria
organizationName **(2.5.4.10)**		SIGN8 GmbH
OrganizationalUnitName **(2.5.4.11)**		Trust Services
OrganizationIdentifier **(2.5.4.97)**		NTRDE-DED2601V.HRB271573
commonName **(2.5.4.3)**		SIGN8 TIMESTAMP CA 01
		SIGN8 TIMESTAMP CA 02
Extensions		
KeyUsage **(2.5.29.15)**	✓	keyCertSign, cRLSign
ExtendedKeyUsage **(2.5.29.37)**		NICHT GESETZT
basicConstraints **(2.5.29.19)**	✓	CA: True Path Length Constraint: 0
authorityKeyIdentifier **(2.5.29.35)**		63F07B0C0BB72741E887715176EE3D62E0FD9D94

subjectKeyIdentifier (2.5.29.14)		*SIGN8 TIMESTAMP CA 01:* CCF02344B03EE11973A8E4812669F854DA884860
		SIGN8 TIMESTAMP CA 02: 823932ECFB412238EEF4C3ACF2367CBF0FDD0ECF
Certificate Policies (2.5.29.32)		[0] Certificate Policy: • Policy Identifier: 1.3.6.1.4.1.58197.1.10.0 • PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1): ○ https://sign8.eu/trust

7.2 TSU-Zertifikate für Zeitstempel

Feld	**Kritisch**	**Wert**	
Signature Algorithm		sha512RSA (1.2.840.113549.1.1.13)	
Signature Hash Algorithm		sha512 (2.16.840.1.101.3.4.2.3)	
Algorithm Identifier (Public Key)		ECC (1.2.840.10045.2.1)	RSA (1.2.840.113549.1.1.1)
Key Size		*ECC P521:* 521 Bits	*RSA:* 4096 Bits
Aussteller			
countryName (2.5.4.6)		DE	
State (2.5.4.8)		Bavaria	
organizationName (2.5.4.10)		SIGN8 GmbH	
organizationalUnitName (2.5.4.11)		Trust Services	
commonName (2.5.4.3)		SIGN8 TIMESTAMP CA 01	

		SIGN8 TIMESTAMP CA 02
Gültigkeit		
NotBefore		[Zeit der Ausstellung]
NotAfter		Maximal 1.825 Tage ab Beginn der Gültigkeit
Inhaber		
commonName (2.5.4.3)		SIGN8 TSU [XX]
organizationName (2.5.4.10)		SIGN8 GmbH
countryName (2.5.4.6)		DE
Extensions		
keyUsage (2.5.29.15)	✓	nonRepudiation
Private Key Usage Period (2.5.29.16)		NotBefore: None NotAfter: [365 Tage weniger als das Ende der Gültigkeit des Zertifikats]
ExtendedKeyUsage (2.5.29.37)	✓	timestamping (1.3.6.1.5.5.7.3.8)
basicConstraints (2.5.29.19)		CA: False Path Length Constraint: None
authorityKeyIdentifier (2.5.29.35)		*SIGN8 TIMESTAMP CA 01:* CCF02344B03EE11973A8E4812669F854DA884860
		SIGN8 TIMESTAMP CA 02: 823932ECFB412238EEF4C3ACF2367CBF0FDD0ECF
subjectKeyIdentifier (2.5.29.14)		[AUTOMATISCH]
qcStatements (1.3.6.1.5.5.7.1.3)		QcCompliance: 0.4.0.1862.1.1 QcPDS: 0.4.0.1862.1.5
Certificate Policies (2.5.29.32)		[0] Certificate Policy: • Policy Identifier: 1.3.6.1.4.1.58197.1.10.0

		• PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1): ○ https://sign8.eu/trust
AuthorityInfoAccess		[0]: • Access Method: Ca Issuers (1.3.6.1.5.5.7.48.2) • Access Location: ○ URI: https://aia.object.sign8.eu/[...] [1]: • Access Method: OCSP (1.3.6.1.5.5.7.48.1) • Access Location: ○ URI: http://ocsp-q.sign8.eu

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.