

TSA Disclosure Statement der SIGN8 GmbH



Version: 1.0
Datum: 09.09.2024

Dokumentationshistorie

Version	Anmerkung	Datum
1.0	Erstellung 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 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (eIDAS-Verordnung).	09.09.2024

Inhaltsverzeichnis

1	Einleitung.....	3
2	Kontaktinformationen.....	3
3	Token-Typen und Nutzung der Zeitstempel.....	3
3.1	Zeitstempel-Algorithmen	3
3.2	Gültigkeit der Zeitstempel.....	4
3.3	Nutzungseinschränkungen	4
3.4	Prüfung der Gültigkeit von Zeitstempeln.....	4
4	Genauigkeit der Zeitstempel.....	4
5	Verpflichtungen der Nutzer.....	4
6	Verpflichtungen der Vertrauenden Dritter.....	5
7	Verpflichtungen der TSA.....	5
7.1	Zusicherungen, Garantien und Gewährleistungen.....	5
7.2	Anwendbares Recht.....	5
7.3	Streitschlichtungsverfahren	6
7.4	SIGN8-Repository, Trust Marks und Audit.....	6
7.5	Datenschutzerklärung.....	6
7.6	Wichtige Dokumente	6

1 Einleitung

Die SIGN8 GmbH ist qualifizierter Vertrauensdiensteanbieter (VDA), gemäß der Verordnung (EU) Nr. 2024/1183 des europäischen Parlamentes und des Rates vom 11. April 2024.

Dieses Dokument ist das TSA Disclosure Statement der SIGN8 GmbH, welches die Bedingungen der von SIGN8 angebotenen Zeitstempeldienste in einem lesbaren und verständlichen Format für unsere Abonnenten und Vertrauende Dritte zusammenfasst. Dieses Statement ist kein Ersatz für das TSA Policy und das Certificate Practice Statement (CPS) von SIGN8. Die zugrundeliegende TSA Policy (OID 1.3.6.1.4.1.58197.1.2) ist unter <https://sign8.eu/trust/> öffentlich zugänglich.

Die Zeitstempel-Server der SIGN8 GmbH sind nicht öffentlich.

2 Kontaktinformationen

SIGN8 GmbH
Fürstenrieder Str. 5
80687 München
Tel.: +49 (0)89 2153 7472 000
E-Mail: info@sign8.eu
Website: <https://sign8.eu/>

3 Token-Typen und Nutzung der Zeitstempel

Die SIGN8 TSA stellt ausschließlich qualifizierte elektronische Zeitstempel gemäß der Verordnung (EU) Nr. 2024/1183 aus. Die Bereitstellung des Zeitstempeldienstes seitens der SIGN8 GmbH 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 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.

Der angebotene Dienst entspricht dem folgenden Service-Identifizier:

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

3.1 Zeitstempel-Algorithmen

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 die Zertifikate der TSUs: RSA 4096 mit SHA512RSA oder ECDSA mit SHA512

Unterstützt wird ausschließlich der Hash-Algorithmus SHA-512.

3.2 Gültigkeit der Zeitstempel

Die Zertifikate der Zeitstempelunterzeichner (TSUs) haben eine maximale Gültigkeitsdauer von 15 Jahren.

3.3 Nutzungseinschränkungen

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. Die TSA legt keine weiteren Einschränkungen für die Verwendung ihrer Zeitstempel fest.

3.4 Prüfung der Gültigkeit von Zeitstempeln

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.

4 Genauigkeit der Zeitstempel

Die Zeitstempel enthalten die korrekte Zeit. Die Zeitkalibrierung erfolgt automatisch und in solch einer Weise, dass die TSU-Zeiten innerhalb der maximalen Zeitabweichung bleiben. 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.

5 Verpflichtungen der Nutzer

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

6 Verpflichtungen der Vertrauenden Dritter

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. OCSP-URI: <http://ocspq.sign8.eu>
- 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.

7 Verpflichtungen der TSA

SIGN8 verpflichtet sich, alle in der time stamp policy (BTSP - OID: 0.4.0.2023.1.1) 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 der time stamp policy eingehalten werden.

7.1 Zusicherungen, Garantien und Gewährleistungen

Weder dieses Dokument noch die jeweilige CPS enthalten Zusicherungen, Garantien oder Gewährleistungen des TSA. Im Verhältnis zu Zertifikatsinhabern, Vertrauenden Dritten sowie allen anderen natürlichen und juristischen Personen sind ausschließlich die entsprechenden Regelungen in den AGB bzw. der jeweiligen einzelvertraglichen Vereinbarung sowie die gesetzlichen Bestimmungen maßgeblich. Der VDA ist außerdem für keine Schäden, die durch eine andere als der vorgeschriebenen Nutzung der Zertifikate entstanden ist, verantwortlich.

Allgemeine Geschäftsbedingungen: <https://sign8.eu/agb/>

7.2 Anwendbares Recht

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

7.3 Streitschlichtungsverfahren

Beschwerden können schriftlich bei der SIGN8 GmbH, Fürstenrieder Str. 5, 80687 München oder via E-Mail (info@sign8.eu) eingereicht werden.

7.4 SIGN8-Repository, Trust Marks und Audit

SIGN8 und seine qualifizierten Dienste werden regelmäßig auditiert. Im Falle der TSA erfolgt dies gemäß den Anforderungen der EN 319 421 durch eine akkreditierte Stelle nach EN 319 403 für Vertrauensdienste gemäß der Verordnung (EU) Nr. 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität.

7.5 Datenschutzerklärung

Die Datenschutzerklärung ist abrufbar unter <https://sign8.eu/impressum-datenschutzerklaerung/>.

7.6 Wichtige Dokumente

Alle relevanten Dokumente lassen sich unter der folgenden Adresse herunterladen: <https://sign8.eu/trust>.