certSIGN Time Stamping Authority 2
Disclosure Statement

Version 3.2

Date: 22 June 2026

Important
Notice

Address: 29 A Tudor Vladimirescu Avenue,

AFI Tech Park 1, Bucharest, Romania

Phone: 004-021-31.19.901

Web: www.certsign.ro

Important Notice about this Document

This document is the CERTSIGN Time Stamping Authority 2 (CERTSIGN TSA 2) Disclosure Statement hereinafter referred to as the TSA Disclosure Statement. This document does not substitute or replace the CERTSIGN Time-Stamping Authority 2 Policy and Practice Statement (TSPS). You must read the TSPS at http://www.certsign.ro/repository before you apply for the CERTSIGN Time Stamping Authority 2 Service.

The purpose of this document is to provide a set of statements about the policies and procedures of the TSA that require particular emphasis or disclosure to subscribers and relying parties. This document is not intended to create contractual relationships between CERTSIGN SA ("CERTSIGN") and any other person. This document is intended for use only in connection with CERTSIGN and its business. This version of the TSA Disclosure Statement has been approved for use by the CERTSIGN Policies and Procedures Management Body and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the CERTSIGN Policies and Procedures Management Body. The date on which this version of the TSA Disclosure Statement becomes effective is indicated on this document.

Document History

Version	Effective Date[1]	Reason	The person who made the change
1.0	February 2017	First version publishing	Information Security Officer
2.0	March 2017	Second version, after interim audit	Information Security Officer
2.1	April 2017	Third version minor update	Information Security Officer
2.2	November 2018	Update change headquarters	PKI Policies Manager
2.3	January 2019	Annual review	PKI Policies Manager
2.4	January 2020	Annual review	PKI Policies Manager
2.5	January 2021	Annual review	PKI Policies Manager
2.6	January 2022	Annual review	PKI Policies Manager
2.7	January 2023	Annual review	PKI Policies Manager
2.8	January 2024	Annual review	PKI Policies Manager
2.9	15 January 2025	Annual review	PKI Policies Manager
3.0	15 January 2026	Annual review	PKI Policies Manager
3.1	31 March 2026	Updates for eIDAS2 compliance	PKI Policies Manager
3.2	22 June 2026	Add SHA 512/384	PKI Policies Manager

This document5 created and is the property of:

Owner	Author	Date created
Information Security Officer	Information Security Officer	December 2016

Distribution List

Destination	Date distributed
Public-Internet	February 2017
Public-Internet	March 2017
Public-Internet	April 2017
Public-Internet	November 2018
Public-Internet	January 2019
Public-Internet	January 2020
Public-Internet	January 2021
Public-Internet	January 2022
Public-Internet	January 2023
Public-Internet	January 2024
Public-Internet	January 2025
Public-Internet	January 2026
Public-Internet	March 2026
Public-Internet	June 2026

This document was approved by:

Public-Internet

Version	Name	Date
1.0	Policies and Procedures Management Body	February 2017
2.0	Policies and Procedures Management Body	March 2017
2.1	Policies and Procedures Management Body	April 2017

[1] *Effective Date is on the last day of the month*

2.2	Policies and Procedures Management Body	November 2018
2.3	Policies and Procedures Management Body	January 2019
2.4	Policies and Procedures Management Body	January 2020
2.5	Policies and Procedures Management Body	January 2021
2.6	Policies and Procedures Management Body	January 2022
2.7	Policies and Procedures Management Body	January 2023
2.8	Policies and Procedures Management Body	January 2024
2.9	Policies and Procedures Management Body	January 2025
3.0	Policies and Procedures Management Body	January 2026
3.1	Policies and Procedures Management Body	March 2026
3.2	Policies and Procedures Management Body	June 2026

Contents

1 Entire agreement

This TSA Disclosure Statement provides high level disclosures regarding the CERTSIGN Time-Stamp Authority 2 (CERTSIGN TSA 2). It does not replace or override the definitive TSPS documents available at http://www.certsign.ro/repository.

2 CERTSIGN contact info

Contact Data:

S.C. CERTSIGN S.A.

Office: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania

Trade Register Number: J2006000484402

VAT Code: RO 18288250

Site

www.certsign.ro

Sales

Phone: (+4031)1011870

E-mail: office@certsign.ro

HR CERTSIGN

Phone: (+4031)4133063 Int. 163

Technical support

Phone: (+4031)1011870

E-mail: suport@certsign.ro

Contact:

Phone: (+4021)3119901

E-mail: office@certsign.ro

3 Time-stamp token types and usage

The CERTSIGN TSA 2 aims to deliver time-stamping services used in compliance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

The identifier of the time-stamp policy is OID:

1.3.6.1.4.1.25017.2.2.1

{iso(1) identified-organization(3) dod(6) internet (1) private(4) enterprise(1)

CERTSIGN (25017) TSA(2) CPS-PC-EU Regulation 910/2014(2)}
- 1 is the number of the TS Unit

By including this object identifier in the generated time-stamps, CERTSIGN TSA 2 claims conformance with this time-stamp policy.

Time-stamps may include also the OID **0.4.0.2023.1.1**[2]**,** if this is specified in the time-stamp request content.

Supported signing algorithm is sha256WithRSAEncryption (2048/4096[3] bit key length). SHA512 and SHA384 are also supported.

Acceptable Time Stamp Request Hashes include SHA512, SHA384 or SHA256. CERTSIGN digital signature on the Time-Stamp Token (TST) has a validity period of up to three years. Refer to section 6 below for information on how to verify a TST. CERTSIGN may charge fees for the services provided by the CERTSIGN TSA 2.

4 Reliance Limits

CERTSIGN does not set reliance limits for timestamp services, however reliance limits may be set by applicable law or by agreement. See Limitation of Liability below. The CERTSIGN TSA 2 assures time with ±1 second of a trusted UTC time source. If a trusted UTC time source cannot be acquired, the time stamp will not be issued. CERTSIGN maintains secure records concerning the operation of the CERTSIGN TSA 2 for a period of 10 years for the purpose of providing evidence in legal proceedings.

certSIGN TSA has implemented the following measures to ensure availability of the service:

- Redundant setup of IT Systems to avoid single point failures.
- Redundant high speed internet connections to avoid loss of service
- Use of uninterruptable power supplies and electric generator.

Although these measures ensure service availability of the certSIGN TSA, an annual availability of 100% cannot be guaranteed. certSIGN TSA aims to provide an availability of the service of 99% per year.

5 Obligations of the Subscribers

To use a method or software toolkit provided by CERTSIGN in order to request and receive time-stamps from CERTSIGN Time Stamping Authority 2, unless otherwise specified in the Subscriber agreement.

To verify the electronic signature of CERTSIGN Time Stamping Authority 2 when they receive the time stamp and also to check the status of the certificate of CERTSIGN Time Stamping Authority 2. Also, they need to check the Certificate Revocation List or OCSP Server, so that the certificate used for signing time stamp is trusted and valid.

[2] *{itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)}*
[3] *Current TSU, active this year, is with 2048 bits. From next TSU, active from Q4 2026, we will use 4096 bits for keys.*

6 Time-stamping unit (TSU) public key status checking obligations of relying parties

Before placing any reliance on a Time-Stamp, relying parties must verify that the TST has been correctly signed and that the associated TSU certificate has not been revoked. Revocation checking of the TSU certificate shall be done using OCSP service available at http://ocsp.certsign.ro or CRL available at http://crl.certsign.ro/certsign-qualifiedca2023rsa.crl

If this verification takes place after the end of the certificate validity period, the Relying Party should follow the guidance denoted in Annex D of ETSI EN 319 421, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

7 Retention of event logs

CERTSIGN TSA 2 event logs are retained for 10 years in accordance with the retention period for audit logs in the TSPS.

8 Limited warranty & disclaimer/ limitation of liability

Within the limit set by the Romania Law, in no event (except for fraud or willful misconduct) CERTSIGN will be liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of time stamping services;
- Any other damages.

9 Applicable agreements and practice statement

CERTSIGN publishes at the repository https://www.certsign.ro/repository the following documents:

- certSIGN TSA 2 – Policy and Practice Statement;
- certSIGN TSA 2 - Terms and Conditions
- certSIGN TSA 2 - Disclosure statement

10 Privacy policy

All information held by certSIGN was obtained, stored and processed in accordance with (EU) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of these data, with Law no. 190/2018 regarding the protection of individuals with regard to the processing of personal data and on the free movement of such data, and any generally binding rules adopted in relation to the protection of personal data. Relationships between the Subscriber, Relying Party and certSIGN are trust based.

11 Refund Policy

Refund policy is defined within the internal price policy. If a subscriber or a relying party is not satisfied with the services, they may request fee refund only if CERTSIGN does not fulfil

its obligations and duties specified in the subscriber agreement and the present document and according with Romanian Law.

12 Applicable law, complaints and dispute resolution

The law governing the time stamping services issued by CERTSIGN Time Stamping Authority 2 is: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

certSIGN complies with Romanian Law no.214/2024 on the use of electronic signatures, time-stamping and the provision of trust services based on them.

The Romanian laws shall govern the enforceability, construction, interpretation, and validity of the present document (without giving effect to any conflict of law provision that would cause the application of other laws).

13 TSA and Repository Licenses, Trust Marks and Audit

The CERTSIGN TSA 2 issues time stamps using CERTSIGN internal developed products that have been accredited by NATO (NATO Catalogue - NIAPC) and by Romanian National Security Agency (ORNISS) as being capable to protect CLASSIFIED information.

In the provision of trust services, CERTSIGN maintains several accreditations and certifications. These include:

- eIDAS certification for Timestaping Authorities – performed every two years, this certification ensures the potential relying parties that a qualified practitioner has evaluated certSIGN Certification Authority's business practices and control to determine whether they are in conformity with the ETSI standards, and has issued a report indicating that those principles are respected.
- ISO/IEC 20000-1, certifying that the Information Technology Service Management System operated by CERTSIGN is in compliance with this standard, for the provision of the following services: developing and maintenance of software and information systems; cybersecurity (e.g.: incident response and analysis, vulnerability assessment and penetration testing, Advanced Threat Intelligence & Correlation);
- ISO 9001 demonstrating the implementation of a quality management system, which is the ensuring mechanism that CERTSIGN meets the needs of customers and other stakeholders, also for training activities
- ISO 27001 demonstrating that the company is using a trusted Information security management system
- Clearance for personal data processing according to European Union (EU) and Romanian legislation
- ISO 14001 demonstrating that CERTSIGN has implemented and maintains an Environmental Management System according to this standard;
- ISO 18001 demonstrating that CERTSIGN has implemented and maintains a Health and Safety Management System according to this standard;