Time-Stamping Policy of AlfaTrust Certification S.A.

Table of contents

1. Introduction

This document represents the Time-Stamping Policy (TSP) applicable to the timestamping services provided by AlfaTrust Certification S.A., as a qualified trust service provider, officially notified to the Romanian Authority for Digitalization (ADR) and listed in the European Union Trusted List, in accordance with Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market ("eIDAS Regulation") and with Law No. 214/2024 on the use of electronic signatures, timestamps, and the provision of trust services.

The purpose of this document is to establish, in a formal framework, the general rules, operational principles, and requirements applicable to the timestamping services provided by AlfaTrust Certification S.A., in order to ensure compliance with legal requirements and applicable international standards (including ETSI EN 319 421, ETSI EN 319 401, and ETSI EN 319 422).

Timestamping services provide evidence that certain data existed at a specific moment in time, by generating qualified timestamps, based on robust cryptographic technologies (including public key cryptography) and on the use of time sources synchronized with UTC (Coordinated Universal Time), in compliance with the accuracy requirements provided by law.

This document complements and is applied together with the Declaration of Trust Service Practices (DPSI), as well as other operational reference documents.

In accordance with applicable legal obligations, AlfaTrust Certification S.A. provides:

- qualified timestamp generation services, as the operator of one or more Time Stamping Authorities (TSA);
- related services of monitoring, control, audit, and record-keeping, to maintain a high level of security, reliability, and integrity of the service provided.

Each Time Stamping Authority (TSA) operated by AlfaTrust Certification S.A. uses a distinct private key, protected in a qualified cryptographic module (HSM), associated with a qualified digital certificate issued by AlfaTrust Certification S.A., as a qualified trust service provider, in accordance with the requirements established by the eIDAS Regulation and Law No. 214/2024.

2. Reference documents for the timestamping service

The Time-Stamping Policy (TSP) sets the regulatory framework and the general requirements applicable to the qualified timestamping service provided by AlfaTrust Certification S.A., including the mandatory rules to be followed by the Time Stamping Authorities (TSA) operated by the provider.

The concrete application of these rules is detailed in the Declaration of Trust Service Practices (DPSI), which systematically describes:

- the technical processes used in generating timestamps;
- the measures ensuring synchronization accuracy with UTC (Coordinated Universal Time);
- the security controls and organizational requirements applicable to the personnel, infrastructure, and systems involved.

The DPSI is the operational and procedural document that complements the TSP and details the implementation of the requirements set out by Regulation (EU) No. 910/2014 (eIDAS), Law No. 214/2024, the applicable standards (including ETSI EN 319 421, ETSI EN 319 401), and the requirements established by the Romanian Authority for Digitalization.

3. Timestamping Service Policy

AlfaTrust Certification S.A., as a qualified trust service provider, delivers qualified timestamping services in accordance with Regulation (EU) No. 910/2014 (eIDAS), Law No. 214/2024 on the use of electronic signatures, timestamps, and the provision of trust services, and the relevant standards ETSI EN 319 421 and ETSI EN 319 401.

The accepted algorithms for document hashing, for which timestamps are requested, are SHA-256, SHA-384, and SHA-512. The private key used to sign timestamps is either 2048-bit or 4096-bit, and the signing algorithm is SHA256WithRSAEncryption.

The issued timestamps contain time synchronized with UTC, with an accuracy of ±1 second. This synchronization system, implemented via the Internet, enables real-time synchronization of a time server (STRATUM 2 – located at MCTI – URL: timp.mcsi.ro) with the time information provided by the Romanian national time and frequency standard.

If this server is not functional, the following STRATUM 1 or STRATUM 2 servers will be used: ptbtime1.ptb.de, ntp.obspm.fr. The information transmitted by these servers allows the synchronization of other time servers or any computer connected to the Internet.

The Time-Stamping Policy does not impose limitations on the applicability of the issued timestamps, which are valid in any technical or legal context where proof of the existence of certain data at a specific moment in time is required, provided that the requirements set out in this Policy and in the associated documents are met.

3.1. Certificate profile of the Time Stamping Authorities (TSA)

The digital certificates used by the **Time Stamping Authorities (TSAs)** operated by AlfaTrust Certification S.A. comply with the requirements of Regulation (EU) No. 910/2014 (eIDAS), Law No. 214/2024, ETSI EN 319 412-2 (Certificate profile for trust service providers), ETSI EN 319 421 (Policy and security requirements for TSPs issuing time-stamps), and RFC 5280, which replaces RFC 2459.

The TSA certificates comply with the following essential characteristics:

Field name	Value or limit of value
Version	Version 3
Serial number	A unique value for the certificate

Signature algorithm	sha256WithRSAEncryption	
Issuer (Distinguished Name)		
	Name (CN) =	AlfaTrust Certification S.A.
	Organization (O) =	AlfaTrust Certification S.A.
	Country (C) =	EN
Not before (start date of validity period)	Based on Universal Time Coordintated	
Not after (expiry date)	Based on Universal Time Coordintated	
Subject (Distinguished Name)	The distinctive name complies with X.501 requirements	
Subject public key information	In the format that complies with RFC 5280, it contains information about RSA public keys. The size of the key is 2048 bits.or 4096.	
Signature	The signature of the certificate, generated in the format that complies with the requirements described in RFC 5280.	

3.2. Identification of the Time-Stamping Service Policy

The AlfaTrust Certification timestamp contains the following policy identifier (in accordance with ETSI TS 102 023 V1.2.2 (2008-10)):

1.3.6.1.4.1.{AlfaTrustCertification}.4.2023.1.1 = iso(1).identified-organization(3).dod(6).internet(1).private(4).enterprise(1).{AlfaTrustCertification}.identified-organization(4).time-stamp-policy(2023).policy-identifiers(1).baseline-ts-policy(1)
where {AlfaTrustCertification} represents the unique number assigned by IANA to AlfaTrust Certification S.A. (36915), available at http://www.iana.org/assignments/enterprise-numbers .

3.3. Service compliance with policy

AlfaTrust Certification S.A. indicates the policy under which a timestamp is issued through the identifier described in section 3.2. Conformity with the policy can be demonstrated either by providing evidence of compliance at the request of subscribers or partner entities, or through audits carried out by independent entities.

3.4. Timestamping process

Each timestamp issued by the **Time Stamping Authorities (TSAs)** operated by AlfaTrust Certification S.A. is generated in accordance with the requirements of Regulation (EU) No. 910/2014 (eIDAS), Law No. 214/2024 on the use of electronic signatures, timestamps, and the provision of trust services; European standard ETSI EN 319 421 applicable to qualified timestamping services; and, where compatible, SR ETSI TS 101 861 V1.2.1:2005 Time-stamping profile, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP): IETF RFC 3161; and, where applicable, the technical rules issued by the Romanian Authority for Digitalization.

The structure of the issued timestamp includes at least the following mandatory elements:

- a unique identifier of the time-stamping policy under which the timestamp is issued;
- a unique identifier of the timestamp (serial number);
- the exact date and time (UTC) when the timestamp was applied, provided by the IT system synchronized with the official national time of Romania;
- UTC time synchronized with STRATUM 1/2 time sources, within the regulated accuracy limits (±1 second);
- the document hash for which the timestamp is issued;
- the country identifier where the **Time Stamping Authority (TSA)** operated by AlfaTrust Certification S.A. is established.

3.5. Synchronization of the time base

The AlfaTrust timestamping platform includes a time server synchronized with UTC through a permanent and secure connection to the IT system providing the official national time of

Romania. If this server is unavailable, the following STRATUM 1 or STRATUM 2 servers will be used: **ptbtime1.ptb.de, ntp.obspm.fr.**

The synchronization accuracy of the time server used by the **Time Stamping Authorities (TSAs)** with UTC shall not exceed one second.

AlfaTrust Certification S.A. has designed and implemented all necessary measures to ensure that the accuracy of the time used in the issued timestamps remains within the parameters set forth in this Policy.

3.6. Operational Electronic Register (REOp) of issued timestamps

AlfaTrust Certification S.A. has established and maintains an **Operational Electronic Register** of all issued timestamps, permanently available for online consultation.

The REOp is continuously available and ensures complete traceability of the qualified timestamping service, in compliance with Regulation (EU) No. 910/2014 (eIDAS); Law No. 214/2024 on the use of electronic signatures and the provision of trust services; and ETSI EN 319 421 on security and auditability requirements applicable to qualified timestamping service providers.

Specifically, the Operational Electronic Register contains:

- all issued timestamps, related data, and the certificate used;
- event records from the IT system used for timestamp generation;
- cryptographic key changes;
- system shutdowns;
- security incidents.

The records of the above-mentioned events may be communicated, upon request, to the competent authority (including the **Romanian Authority for Digitalization – ADR**) or to any other authority legally entitled to access such information, in the event of disputes concerning the issued timestamps or the timestamping process itself.

All information in the **Operational Electronic Register (REOp)** and the related documentation on algorithms and procedures for generating issued timestamps are retained for 10 years. The retention process is detailed in the DPSI.

4. Responsibilities of the parties involved

4.1. Responsibilities of AlfaTrust Certification S.A. as a Timestamping Service Provider

AlfaTrust Certification S.A., as a qualified trust service provider, is obliged to fully comply with this Policy, without allowing derogations or exceptions from the assumed procedural and technical framework.

AlfaTrust Certification S.A. guarantees that all requirements imposed on the Time Stamping Authorities (TSAs), including procedures and practices related to timestamp issuance, system verification, and security audit, are consistent with this Policy.

AlfaTrust Certification S.A. ensures round-the-clock (24/7/365) availability of the TSA services.

The timestamps issued include time information with an accuracy of ±1 second. The TSAs operated by AlfaTrust Certification S.A. fulfill all obligations towards subscribers, as set out in this Time-Stamping Policy (TSP), including service availability and accuracy.

AlfaTrust Certification S.A. assumes responsibility and guarantees that it takes the necessary measures to:

- properly verify the identification of the algorithm used to generate the document hash;
- ensuring time accuracy as required under this Policy;
- ensuring the security of the private key used to sign timestamps (the private key cannot be derived from the corresponding public key;
- the certificate associated with the private key has not expired; the private key cannot be accessed or used by any unauthorized person;
- the private key shall only be used for issuing timestamps).

All these measures are intended to ensure trust and security for subscribers and partner entities relying on timestamps issued by AlfaTrust Certification S.A.

In accordance with Article 13 of the eIDAS Regulation and Article 20 of Law No. 214/2024, AlfaTrust Certification S.A. is liable for damages caused to any person who reasonably relies on a timestamp issued by it, if:

- the timestamp contains inaccurate information at the time of issuance;
- the service does not meet the applicable requirements;
- the obligations laid down in this Policy, law or regulation are breached.

Liability is limited to the RON equivalent of EUR 10,000 per insured event, pursuant to the insurance policy concluded by AlfaTrust. An "insured event" means each distinct damage caused, regardless of whether multiple damages occur simultaneously or sequentially from the same cause.

AlfaTrust Certification S.A. shall not be liable in the following situations, to the extent permitted by law:

- where it demonstrates that it has taken all necessary and reasonable measures to prevent the damage, but the damage could not be avoided;
- for damages caused by force majeure or unforeseen events, within the meaning of the Civil Code.

For the purposes of this Policy:

– *force majeure* is any external, unforeseeable, absolutely invincible and unavoidable event occurring after the entry into force of the contract, such as: earthquakes, fires, natural disasters, armed attacks, acts of terrorism, war, major external cyber attacks, massive unforeseen interruptions of the national infrastructure;

– *the fortuitous event* represents an unforeseeable circumstance, without extraordinary character, such as: strikes, legal restrictions, unexpected technological unavailability or institutional blockages.

• **for damages caused to subscribers or third parties** as a result of:

– incorrect or non-compliant use of the timestamping service;

– failure to comply with our obligations under this policy and the Statement of Trust Services Practices (SIPD);

– the negligent use, by subscribers or partner entities, of the information included in the timestamp, without prior verification of its validity.

The provisions of this section are supplemented by the contractual clauses in force established by the contract concluded between AlfaTrust Certification S.A. and the subscriber.

4.2. Responsibilities of the subscribers

The use of the timestamping service provided by AlfaTrust Certification S.A. implies the express and prior acceptance by the subscriber of all the provisions set out in the following documents:

- Time-Stamping Policy (TSP);
- Trust Service Practice Statement (TSPS / DPSI);
- he service agreement concluded between AlfaTrust Certification S.A. and the subscriber.

If the subscriber is a legal entity, it bears full responsibility for the actions or omissions of its authorized users, including compliance with the obligations laid down in this Policy.

In all cases, the subscriber shall:

- verify, upon receipt of a timestamp, the electronic signature of the issuing Time Stamping Authority (TSA);

- ensure, by consulting the publicly available information at www.alfasign.ro, that the TSA certificate is valid, active, and issued by a qualified trust service provider;
- use the timestamp in accordance with its intended technical and legal purpose, without alteration, reuse, or interpretation outside the applicable contractual and legal framework.

4.3. Responsibilities of partner entities

Partner entities that use or rely on timestamps issued by AlfaTrust Certification S.A. shall:

- verify the integrity of the timestamp and the electronic signature applied by the issuing Time Stamping Authority (TSA);
- check, at the time of using the timestamp, the status of the certificate associated with the TSA (validity, expiration, revocation), using the official channels made available at www.alfasign.ro;
- retain, where applicable, the timestamp and all associated elements in their original format, for audit, traceability, and evidentiary purposes, in accordance with regulatory requirements.

5. Key Lifecycle Management

5.1. Generation and protection of Timestamp Authority keys

The keys of the **Time Stamping Authorities (TSAs)** operated by AlfaTrust Certification S.A. are generated within a Hardware Security Module (HSM) compliant with NIST FIPS 140-2 Level 3, by trusted personnel acting in defined trusted roles.

The key generation process is documented and audited in accordance with ETSI EN 319 401 and ETSI EN 319 421 requirements, as well as with the provisions of the **Trust Service Practice Statement (TSPS/DPSI).**

5.2. Distribution of public keys of the Timestamping Authorities

Timestamp Authority certificates are published in a secure, transparent and accessible manner through the official website www.alfasign.ro. The publication ensures the traceability and

independent validation of timestamps by third parties (relying parties), in accordance with Article 24(2)(d) of the eIDAS Regulation and the transparency requirements set by the ADR.

5.3. Key change of the Timestamping Authorities

The private signing keys of the TSAs operated by AlfaTrust Certification S.A. have a lifetime consistent with the strength of the cryptographic algorithm and the key length.

Expired private keys are not archived and are securely destroyed immediately upon expiration.

The public keys of the TSAs are retained for 10 years, in order to allow verification of previously issued timestamps.

5.4. Destruction of the Timestamp Authorities Key

The procedures for the destruction of keys that have expired are carried out in such a way as to ensure that they can no longer be restored.

5.5. Security Hardware Module (HSM) Management

AlfaTrust Certification S.A. ensures the security of security hardware modules (HSMs) throughout their life cycle, from the manufacturer to their removal from production.

6. Information Security Policy

AlfaTrust Certification S.A. ensures the security of certification services and electronic seals in accordance with the General Information Security Policy (PoG-SMSI – AlfaTrust Certification's General InfoSEC Policy) and the measures described in the DPSI.

7. Personnel policy

AlfaTrust Certification S.A. guarantees that, in order to occupy a position within Time Stamping Authorities (TSAs, each designated person meets the following cumulative conditions:

- is a Romanian citizen;

- has completed at least high school;
- signed a contract explicitly detailing the role, responsibilities and obligations of the position held;
- has benefited from advanced technical and operational training, corresponding to the duties and degree of confidence of the position held;
- has been trained on the protection of personal data as well as obligations regarding the confidentiality of sensitive information;
- has signed confidentiality commitments that include clauses regarding the protection of personal data of end users, as well as sensitive information from the perspective of the security of the infrastructure of AlfaTrust Certification S.A.;
- does not hold or exercise other functions or duties that may generate an actual or potential conflict of interest.

For personnel involved in positions of trust, AlfaTrust Certification S.A. requires the presentation of evidence of integrity, professional experience and training necessary for the exercise of specific duties. If the activity involves the execution of government contracts, the designated personnel must have all the official authorizations and approvals provided for by the applicable legislation.

Staff checks are carried out initially, before taking up the position, and are resumed periodically, at least once every 5 years, for all positions of trust.

Due diligence includes:

- confirmation of professional history (previous jobs);
- checking professional references;
- confirmation of the highest educational qualification obtained;
- requesting the criminal record certificate;

- requesting relevant extracts on the right to drive (if applicable);
- requesting any reports on the social benefits received (if they are relevant in the legal or contractual context).

8. Fees

The timestamping services provided by AlfaTrust Certification S.A. are offered on a commercial basis.

The applicable fees for these services vary depending on the type of service requested, the volume of timestamps, and the contractual specifications.

The price list is available upon request and may be provided in electronic or physical format to subscribers, partner entities, or competent authorities.

The fees **are subject to periodic review** and apply in accordance with the pricing policy published on www.alfasign.ro and included in the individual agreements.

9. Compliance with legal requirements

The Time Stamping Authorities (TSAs) operated by AlfaTrust Certification S.A. act with due diligence to ensure full compliance with applicable national and European legislation, as well as with any other normative acts that amend, supplement, or replace the provisions in force.

The reference legislative framework includes, but is not limited to:

- 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 (eIDAS Regulation);
- Law No. 214/2024 on the use of electronic signatures, electronic timestamps, and the provision of trust services based thereon;
- The 2020 technical rules issued by the Romanian Authority for Digitalization (ADR) for the application of Law No. 451/2004 (insofar as they remain applicable for transitional technical aspects);

- Any other applicable national or European regulations that supplement, amend, or replace the legislation in force in the field of trust services.

AlfaTrust Certification S.A. periodically reviews its procedural and documentation framework to reflect legislative changes and to ensure continuous alignment with the requirements of the Romanian Authority for Digitalization (ADR).

10. Policy updates

The Timestamp Policy may be subject to changes and updates, initiated by AlfaTrust Certification S.A., whenever necessary to reflect legislative, technological, organizational or good practice changes.

The changes are formalized through a separate document, entitled "Amendments to the Timestamping Policy", which will clearly highlight the nature and date of each change. Updated versions are archived and made available to the public through the document repository available at: http://www.alfasign.ro/depozit.