



Certification and electronic seals policy of AlfaTrust Certification S.A.

TABLE OF CONTENTS

1. Introduction.....	3
2. Types of certificates and uses.....	4
3. Types of seals and uses	4
4. Procedures for identifying the user for the issuance of certificates	5
4.1. Physical identification	5
4.2. Remote identification by video means.....	5
4.3. Protection of personal data.....	6
5. PKI architecture	6
6. Services of AlfaTrust Certification S.A.	7
7. Responsibilities of the parties involved in the use of AlfaTrust Certification S.A. services	14
8. Information Security Policy.....	17
9. Personnel policy	17
10. Pricing Policy	18
11. Internal audit and compliance control.....	19
12. Associated documents.....	19
13. Certification Policy Update	20

1. Introduction

This Certification and Electronic Seals Policy (hereinafter referred to as the "CESP") is issued by AlfaTrust Certification S.A., as a qualified trust service provider, registered in the Trusted List of Romania and notified to the Authority for the Digitalization of Romania (ADR), in accordance with Regulation (EU) no. 910/2014 (eIDAS) on electronic identification and trust services, Law no. 214/2024 on electronic identification and trust services, Order no. 564/2021 issued by the Authority for Digitalization of Romania on the regulation, recognition, approval or acceptance of the procedure for remote identification of the person using video means, as well as the applicable complementary national legislation.

PCSE establishes the general principles applicable to the provision of certification services (electronic signature and electronic seals – simple, advanced and qualified – issued, managed, renewed and revoked by AlfaTrust Certification S.A. Users can choose the type of certificate according to the desired purpose – authentication, signing, encryption, identification, validation.

This policy applies to AlfaTrust Certification S.A., as a provider, Registration Authority (RA) and Validation Authority (VA), as well as to any other entity in a subordination relationship or in a contractual relationship with AlfaTrust Certification S.A. in the exercise of the CA, RA or VA attributions.

AlfaTrust Certification S.A. provides simple, advanced and qualified electronic certificates and seals, under the AlfaTrust Certification™ brand, for any category of users, within the limits established by law.

Object and scope of the Certification and Electronic Seals Policy

This Policy defines: establishes the operational, legal and procedural framework applicable to the provision of certification services and electronic seals by AlfaTrust Certification S.A., including:

- entities involved in the process of providing trust services (Certification Authority, Registration Authority, Validation Authority), as well as their responsibilities and obligations;
- the categories of digital certificates and electronic seals issued by AlfaTrust Certification S.A.;
- the types of evidence, information and confirmations used in the identification, registration and validation processes;
- procedures for verifying the identity of users;

- scope and limits of the services provided under this Policy.

The detailed description of these rules, together with the applicable technical and procedural measures, is included in the Statement of Trust Services Practices provided by AlfaTrust Certification S.A. (abbreviated "STSP"), a document associated with this Policy.

Knowledge and compliance with the provisions of the CESP and STSP is essential for end users, contracting entities and partners of AlfaTrust Certification S.A.

2. Types of certificates and uses

a) Simple (non-qualified) AlfaTrust Certification™ certificates - can be used for user authentication, electronic signature and encryption (symmetric key exchange).

b) AlfaTrust Certification Advanced Certificates™ - can be used for authentication, electronic signature, web server authentication, encryption, code signing, VPN gateways, separately or cumulatively, depending on the service purchased or requested by the user. They can be used as proof of identity in electronic transactions, to the extent that the legislation does not require the use of a qualified certificate. The advanced electronic signature does not benefit from the legal presumption of validity provided by Article 25 of Regulation (EU) no. 910/2014 (eIDAS), but only to the extent that it is explicitly accepted by the parties involved.

c) AlfaTrust Certification Qualified Certificates™ - can be used for qualified electronic signature, authentication, encryption, web server authentication, code signing, and VPN connection, separately or in combination, depending on the service chosen. They have full legal value and are recognised in all EU Member States in accordance with Art. 25 para. of the eIDAS Regulation.

3. Types of seals and uses

a) AlfaTrust Certification™ qualified electronic seals are used exclusively by legal entities and can be applied: to guarantee the origin and integrity of electronic documents; for automatic authentication of the legal entity in IT systems; in electronic transactions, in accordance with Regulation (EU) No. 910/2014 (eIDAS) and Law no. 214/2024. These seals are enforceable against third parties, under the conditions provided by law, and may produce legal effects equivalent to the qualified electronic signature, but exclusively in the name of the legal person and without the involvement of an individual will. They ensure the integrity of the document, but do not imply human will or personal consent.

b) AlfaTrust Certification™ advanced electronic seals can be used by legal entities to guarantee the origin and integrity of electronic documents and automatic authentication of the entity within information systems. They do not offer the same legal guarantees as qualified seals and are not enforceable against third parties in the absence of an express

agreement, but they can be used in contractual relationships, where the level of trust is accepted by the parties.

4. Procedures for identifying the user for the issuance of certificates

In order to issue electronic certificates and seals, AlfaTrust Certification S.A. applies rigorous measures for the identification of users, in accordance with:

- a) Regulation (EU) no. 910/2014 (eIDAS);
- b) Law no. 214/2024 on the use of electronic signatures, timestamps and the provision of trust services;
- c) ADR Rules on the procedure of remote identification by video means of 11.11.2021;
- d) Regulation (EU) 2016/679 (GDPR) and Law no. 190/2018.

User identification is mandatory for the issuance of qualified certificates, qualified seals, as well as – optionally – for advanced certificates or advanced seals, at the express request of the customer.

Identification can be done by one of the following methods:

4.1. Physical identification

Physical identification implies the presence of the user in front of an authorized operator of the Registration Authority (RA), based on a valid official identity document, issued by a competent authority.

RA Operator:

- verifies the authenticity of the document and compliance with the declared identity;
- registers the operation in the secure internal system, archiving the copy of the identity document in the applicant's electronic file.

4.2. Remote identification by video means

AlfaTrust Certification S.A. offers remote electronic identification services, in collaboration with a specialized third party (authorized), in accordance with the ADR Rules of 11.11.2021 and Law no. 214/2024.

The procedure is as follows:

1. Initiation of identification: the user accesses the third-party video identification platform, made available through a secure link, generated by AlfaTrust;
2. Video verification: Authorized third party:
 - collects and compares the ID data presented with the video image in real time;

- applies technical measures to verify liveness;
 - validates the correspondence between image and act;
3. Data transmission: after the session is completed, the third party transmits to AlfaTrust:
- a video recording or compliant captures;
 - a copy of the identity document;
 - the identification report;
 - technical metadata (IP address, time, session duration, etc.);
4. RA validation: the AlfaTrust RA operator analyzes the documentation received and, if there are no inconsistencies, validates the identification and authorizes the issuance of the requested certificate or seal.

4.3. Protection of personal data

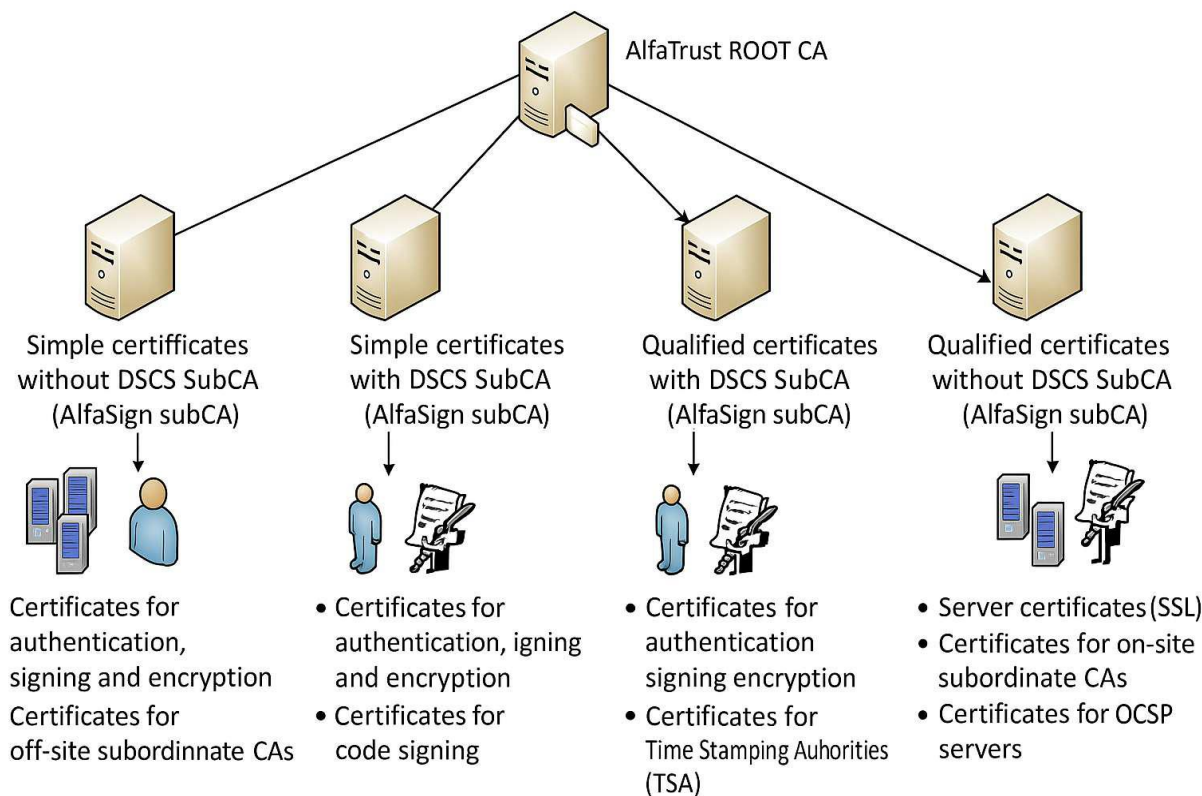
The data collected within both forms of identification (physical and video) are processed exclusively for the purpose of issuing certificates or electronic seals, pursuant to art. 6 para. (1) letters c) and e) of the GDPR and Law no. 214/2024.

In the case of video identification, the third-party partner is designated as the processor of the operator (AlfaTrust Certification S.A.), based on a contract in accordance with art. 28 of the GDPR. It has the obligation to comply with all technical and organizational measures to ensure the confidentiality, integrity and security of the data.

All video session recordings, IDs, and metadata are retained in accordance with internal policies and legal deadlines, and access is allowed only to authorized persons.

5. PKI architecture

The structure of the public key infrastructure (PKI) AlfaTrust Certification S.A. is shown in the following figure:



6. Services of AlfaTrust Certification S.A.

As a qualified trust service provider, notified to the Authority for the Digitalization of Romania (ADR) and registered in the Trusted List of Romania, AlfaTrust Certification S.A. offers the following services:

- a) **Issuance of digital certificates** – simple, advanced or qualified – to end users (individuals, legal entities, web servers, applications or hardware devices);
- b) **Provision of electronic seal services** – qualified or advanced – intended exclusively for legal entities;
- c) **the provision of consultancy and/or implementation services of public key infrastructures (PKIs), as well as a wide range of information security solutions/services** – these consultancy and security services do not constitute trust services within the meaning of Regulation (EU) No 910/2014 (eIDAS), but related services. And they are not subject to ADR supervision.

6.1. Certificate functionality and interoperability

The digital certificates issued by AlfaTrust Certification™, intended for users, allow third parties (including partner entities) to verify digital electronic signatures and seals based on the certificates or electronic seals issued by AlfaTrust Certification.

According to art. 25 para. (1)-(3) of Regulation (EU) no. 910/2014 (eIDAS), a qualified electronic signature has the same legal effect as a handwritten signature and is automatically recognized in all EU Member States, regardless of the state where the certificate was issued, the place where the signature was created or used, or the place where the Certification Authority or user operates.

6.2. Use of qualified certificates

By default, AlfaTrust Certification™ qualified certificates are for general purposes and can be used globally. Their use is not limited to a specific business environment, such as a pilot program, a financial services system, or a virtual marketplace environment.

AlfaTrust Certification S.A. or the other participants are not responsible for monitoring or imposing any restrictions in these environments. However, certain AlfaTrust Certification™ qualified certificates have limited functions. For example:

- PCA (Primary Certification Authority) certificates cannot be used for functions other than PCA;
- client certificates cannot be used as server certificates and vice versa, unless extensions explicitly allow it;
- End-user certificates can only be used within the limits of the extensions present in the certificate.

Certificates can only be used for the purpose explicitly stated in the certificate request and for which the extensions used to generate them were created. Types of use include:

- a) **authentication, signing and encryption** (for both simple and qualified certificates);
- b) **server certificates, code signing, Certification Authority** – as an additional service, at the express request of the client (valid only for SubCAs that issue qualified certificates);
- c) **electronic seals.**

Each user who requests a particular type of certificate or service must accept the contractual conditions associated, expressly, through a formal written agreement attesting to the acceptance of AlfaTrust certificates.

Advanced electronic signatures do not benefit from the legal presumption of legal validity provided by art. 25 eIDAS, unlike qualified electronic signatures. This is important for clearly informing users in order to assess the degree of legal protection offered.

6.3. Types of certificates issued

AlfaTrust Certification S.A. issues several types of digital certificates, corresponding to different areas of applicability. These include:

1. **Simple certificates** – used for authentication, electronic signature and encryption. They allow, for example, signing emails or files and authenticating users through protocols such as SSL.
2. **Advanced electronic certificates and seals** – used for signing, encryption, and authentication, without benefiting from the legal effects of qualified ones.
3. **Qualified electronic certificates and seals** – used for signing legally binding documents, encryption and authentication, having legal effects enforceable against third parties.
4. **Certificates for server authentication and symmetric key exchange** – used by services based on SSL/TLS/WTLS protocols.
5. **Code Signing Certificates** – used by developers to protect the integrity and authenticity of software.
6. **Certification Authority (CA) certificates** - used by entities that issue digital certificates. Their scope of applicability is determined by the certified extensions and the designated role (e.g. end user, CA, PKI authority). These also include the operational certificates of the CA.
7. **Certificates for validating the status of certificates - OCSP (Online Certificate Status Protocol)** - issued for servers that provide answers regarding the validity of certificates according to the OCSP protocol.
8. **Timestamp Authority (TSA) Certificates** – used to generate electronic timestamps that associate data (documents, signatures, messages) with a verifiable time point.
9. **Electronic seal certificates** – issued exclusively to legal entities, for the purpose of automatic signing and guaranteeing data integrity.

The format of the issued certificate complies with the international standard X.509, developed by ITU-T, which establishes the technical structure of digital certificates used in PKI infrastructures. This format allows the global interoperability, the integration of mandatory extensions (such as certification policy OIDs) and is required by ETSI standards and Regulation (EU) no. 910/2014 (eIDAS) for the automatic recognition of certificates in the European Union.

6.4. General terms and conditions of use

The certificates issued by AlfaTrust Certification S.A. can be used only under the following conditions:

- the user's systems properly manage public and private keys;
- The certificate is used exclusively for the purpose stated in the application for issuance. The purpose of using the certificate is determined by the user's initial request and the extensions included in the issued certificate (according to the X.509 standard);
- have internal mechanisms for verifying the status of certificates, creating certification paths and checking validity (signature validity, expiry date, etc.);
- The user has access to clear information about the issued certificate, its validity period, its status and associated responsibilities.

6.4.1. Simple (non-qualified) certificates

The simple certificates offered by AlfaTrust Certification S.A. are available in two main configurations: without SDSK and with SDSK (SDSK – Stored Key Security Device).

a) Simple certificates without SDSK may be used for the following purposes:

- on web servers (SSL certificates), for performing secure symmetric key exchange, reducing the risk of *man-in-the-middle attacks* (especially in the context of the use of the Diffie-Hellman scheme);
- issuance of internal certificates by Certification Authorities located in the customer's infrastructure, based on the certification policy applicable in the respective environment. If the certification authority operates in the customer's infrastructure, the applicability and certification policies may be defined by the customer, subject to AlfaTrust Certification S.A.'s prior acceptance.

These certificates comply with the ETSI TS 102 042 V2.1.1 (2009-05) standard and are associated with the following policy identifier (OID):

1.3.6.1.4.1.{AlfaTrustCertification}.0.4.0.2042.1.1 = *iso(1).identified-organization(3).dod(6).internet(1).private(4).enterprise(1).{AlfaTrustCertification}.itu-t(0).identified-organization(4).etsi(0).other-certificate-policies(2042).policy-identifiers(1).ncp(1),*

where {AlfaTrustCertification} = 36915 is the identification number assigned by the IANA for AlfaTrust Certification S.A., available at www.iana.org/assignments/enterprise-numbers.

b) Simple certificates with SDSK (Proof of Security Control Support)

These certificates are intended for: user authentication; electronic signature; data encryption; computer code signing.

This type of certificate is recommended for low or medium risk environments (e.g. personal emails, access to private accounts, internal applications), where the probability of unauthorized access is low, and any security breaches do not produce significant consequences.

SDSK certificates allow authentication and verification of the integrity of the signed information, as well as protecting its confidentiality – especially in the context of e-mail communications.

These certificates comply with the ETSI TS 102 042 V2.1.1 (2009-05) standard and are associated with the following policy identifier (OID):

1.3.6.1.4.1.{AlfaTrustCertification}.0.4.0.2042.1.2 = *iso(1).identified-organization(3).dod(6).internet(1).private(4).enterprise(1).{AlfaTrustCertification}.itu-t(0).identified-organization(4).etsi(0).other-certificate-policies(2042).policy-identifiers(1).ncplusplus(2),*

where {AlfaTrustCertification} = 36915 is the number designated by IANA for AlfaTrust Certification S.A. (can be found at www.iana.org/assignments/enterprise-numbers).

6.4.2. Qualified or advanced certificates and seals

a) Qualified certificates and seals

The qualified certificates and seals issued by AlfaTrust Certification S.A. are those certificates that comply with the conditions set forth by the legislation in force, being issued by a qualified trust service provider, in accordance with Regulation (EU) no. 910/2014 (eIDAS) and with the provisions of Law no. 214/2024 on the use of electronic signatures, timestamps and the provision of trust services.

These certificates may be used for:

- a) authentication, qualified or advanced electronic signature, encryption** – with SDK (Secure Device with Stored Key) or through AlfaCloud remote certificates issued and stored on secure hardware cryptographic modules (HSMs);
- b) web server authentication and Certification Authority (CA) certificates** – without SDK.

The qualified electronic signature, based exclusively on a qualified certificate, cumulatively meets the following conditions (pursuant to eIDAS):

- it is uniquely linked to the signatory;
- it allows the identification of the signatory;
- it is created through a qualified electronic signature creation device (QSCD), under the sole control of the signatory;

- it is linked to the signed data in such a way that any subsequent changes to them are detectable.

Qualified certificates with SDSK can be issued either locally or remotely (via AlfaCloud) and are stored on HSM-compliant modules, under conditions ensuring the level of security required by eIDAS and by ADR regulations regarding remote video identification and QSCD deliver

b) Advanced certificates and seals

An **advanced certificate** is issued for the use of an **advanced electronic signature**, which complies with the following requirements:

- it is linked exclusively to the signatory;
- it allows the identification of the signatory;
- it is created using signature creation data under the sole control of the signer;
- it is linked to the signed data in such a way that any subsequent changes are detectable.

This level is recommended for: electronic transactions with moderate or high risk; processes where there is a likelihood of fraud; signing documents with high economic value (in the absence of a legal obligation to use a qualified certificate, since the advanced signature does not benefit from the legal presumption of validity provided under Article 25 of Regulation (EU) No. 910/2014 (eIDAS), except to the extent that the parties involved expressly accept the level of trust of the advanced signature).

6.4.3. Policy identifiers (ETSI OIDs)

The qualified certificates and seals issued by AlfaTrust Certification comply with ETSI TS 101 456 V1.4.3 (2007-05) standards as follows:

a) Qualified certificates with SDSK

1.3.6.1.4.1.{AlfaTrustCertification}.0.4.0.1456.1.1 = iso(1).identified-organization(3).dod(6).internet(1).private(4).enterprise(1). {AlfaTrustCertification}.itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1).qcp-public-with-sscd(1),

Note: {AlfaTrustCertification} = 36915 is the unique IANA identifier assigned to AlfaTrust Certification S.A., publicly available at: www.iana.org/assignments/enterprise-numbers.

0.4.0.194112.1.2 – QCP-n-qcsd – Qualified certificates issued to individual persons on QSCD cryptographic devices, according to Regulation (EU) No. 910/2014;

0.4.0.194112.1.3 – QCP-l-qcsd - Qualified electronic seals issued to legal entities on QSCD cryptographic devices, according to Regulation (EU) no. 910/2014.

b) Qualified certificates without SDSK

1.3.6.1.4.1.{AlfaTrustCertification}.0.4.0.1456.1.2 = iso(1).identified-organization(3).dod(6).internet(1).private(4).enterprise(1).{AlfaTrustCertification}.itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1).qcp-public(2),

Note: {AlfaTrustCertification} = 36915 is the unique IANA identifier assigned to AlfaTrust Certification S.A., publicly available at: www.iana.org/assignments/enterprise-numbers.

Choosing the type of certificate

The AlfaTrust Certification subscriber may choose the desired type of certificate depending on the purpose of use. Full details regarding each type of certificate are available in the Statement of Trust Services Practices (STSP), accessible on the official website www.alfatrust.ro. Further information can be requested by e-mail at: office@alfasign.ro.

6.5. Inclusion of additional attributes in digital certificates

AlfaTrust Certification S.A. may, at the express request of the user or the contracting entity, include in the digital certificates certain **additional attributes** (e.g. professions – "lawyer", "engineer", "doctor", identification codes – TIN, NIN, INSTITUTIONAL ID, etc.).

Conditions and procedure:

a) **Documentary justification** – The applicant must provide supporting documents attesting to the requested quality or attribution, such as:

- The decision of admission/appointment to the profession or the certificate attesting the right to practice the profession, issued by the competent authority (e.g. Bar Association for lawyers, CECCAR for expert accountants, UNNPR for notaries). A copy of the ID card or professional card is not enough;
- Certificates or extracts from official registers;
- In the case of TIN(Tax Identification Number) or other identifiers: proof of issuance by the tax authority or the issuing institution.

b) **Validation by the Registration Authority** – The staff of AlfaTrust Certification S.A. will review the documents and confirm their authenticity, keeping a compliant copy electronically archived in the internal record system.

c) **Attribute insertion**

d) **Traceability and accountability** – All requests for attribute insertion are recorded in the RA (Registration Authority) log, including:

- Date of application and approval;
 - The name of the responsible operator;
 - Archived supporting documents.
- e) **Update or revocation** – If the attributes become invalid (e.g. expiration of the professional status), the user is required to request either:
- the update of the certificate, or
 - its revocation.

6.6. Revocation and suspension of certificates

Any certificate issued by AlfaTrust Certification S.A. may be revoked in the following cases:

- loss or compromise of the signature/seal creation data (private key); - change of the legal status of the user (e.g. dissolution of the legal entity, termination of the mandate);
- discovery of false or inaccurate information provided in the issuance request;
- at the express request of the holder;
- by the provider's decision, in justified cases (e.g. fraudulent activity, request from a competent authority).

Revocation or suspension is carried out without delay, within a maximum of 24 hours from the confirmation of the reason, and is immediately reflected in the Certificate Revocation List (CRL) and through the OCSP service.

7. Responsibilities of the parties involved in the use of AlfaTrust Certification S.A. services

7.1.1. Responsibility of the qualified trust service provider

AlfaTrust Certification S.A., as a qualified trust service provider (including certification services, electronic seals and time-stamping), is responsible, under Regulation (EU) no. 910/2014 (eIDAS), for the damage brought to any person who bases his conduct on the legal effects of the certificates, namely:

- a) as regards the accuracy, at the time of issuing the certificate, of all the information it contains;

- b) as regards ensuring that, at the time of issuing the certificate, the signatory identified therein held the signature generation data corresponding to the signature verification data mentioned in that certificate;
- c) as regards ensuring that the signature generation data corresponds to the signature verification data, where the certification service provider generates both;
- d) regarding the revocation of the certificate, in the cases and in compliance with the conditions provided by the legislation.

In addition, AlfaTrust Certification S.A., as a qualified trust service provider, may indicate within a qualified certificate restrictions on its use, as well as limitations on the value of the transactions for which it may be used, provided that such restrictions are visible and easily recognizable by third parties, in accordance with Article 13(2) eIDAS.

AlfaTrust Certification S.A., as a certification service provider, cannot be held liable for damages resulting from the use of a qualified certificate in breach of the restrictions specified therein.

Users who use the certificates in violation of contractual and technical restrictions assume full legal responsibility for the consequences of misuse.

The guarantees and limits of liability between a Registration Authority and the Certification Authority assisting in the issuance of certificates, on the one hand, and the respective user, on the other hand, are subject to and governed by the agreements between them, in compliance with the applicable legislation.

7.1.2. Guarantees of the certification service provider (CSP)

AlfaTrust Certification S.A., as a qualified trust service provider, has the financial resources to cover any damages it may cause in the course of activities related to the certification of electronic signatures and electronic seals. To this end, insurance coverage has been secured by subscribing to a professional civil liability policy for damages caused by negligence, errors in identification, or errors in the issuance of certificates, with a recognized insurance company.

The insured amount complies with the requirements stipulated by the Authority for the Digitalization of Romania, acting as the regulatory and supervisory authority in this field.

The services of AlfaTrust Certification S.A. also include a guarantee for certificate holders, as follows:

- There are no misinterpretations of the entities that approve the applications for the certificate or that issue the certificate;
- There are no errors regarding the information regarding the certificate, made by the entities responsible for approving the application for the certificate, the same ones that are also responsible for issuing the certificate;

- User certificates satisfy all requirements of this Policy as well as of the STSP;
- Revocation services and use of the repository (or registry) are in compliance with this Policy and the STSP in all material respects.

The contractual agreements include a guarantee for parties relying on a certificate, to the effect that:

- All information contained in or incorporated into such a certificate, except for unverified information about the user, is accurate;
- For certificates listed in the AlfaTrust Certification S.A. register, the certificate has been issued to a natural person or a company, and the user has accepted the certificate in accordance with the specifications of this Policy and the STSP;
- The entities approving certificate applications and issuing certificates will comply with this Policy and the DPSI when issuing certificates;
- Users who accept the certificates undertake to use them in accordance with the stated purpose and limitations, based on informed consent.

The detailed responsibilities of the Registration Authorities and intermediary entities are regulated in the internal agreements, in accordance with the STSP and the applicable ADR rules.

7.2. Responsibilities of end-users

End-users of AlfaTrust Certification S.A. certificates are required to:

- use the signature/seal personally, provided that the certificate is valid (not expired or not revoked);
- ensure that no unauthorised person has access to the private key;
- guarantee the accuracy of all the information provided in the certificate application;
- use the certificate exclusively for the declared purpose and in accordance with the CESP and STSP;
- not use the certificate as a Certification Authority (CA), including for signing other certificates or revocation lists;
- request immediate revocation if:
 - the signature/seal creation data has been lost;
 - there is suspicion that such data have been compromised;

- the essential information in the certificate no longer corresponds to reality.

7.3. Responsibilities of partner entities

Partner entities are required to verify each electronic signature on the documents received, including the validity of the associated certificates. For this purpose, they must use the verification tools provided by AlfaTrust Certification S.A., such as the Certificate Revocation List (CRL), the OCSP services, as well as the supplied trust chains. The verification procedures are detailed in the STSP.

If the verification of the signature fails, the document must be rejected, and validation must be performed through other methods in compliance with the applicable legislation and the STSP.

7.4. Financial responsibilities

Within the limits of the law, AlfaTrust Certification S.A. may claim damages from users in the following cases:

- a) Providing false or misleading information in the certificate application;
- b) Omitting essential information, whether negligently or with fraudulent intent;
- c) Failure to comply with the obligation to protect the private key / failure to comply with the related security measures;
- d) Use of a name (including common name, domain, or email address) that infringes the intellectual property rights of a third party.

AlfaTrust Certification S.A. will cover damages caused to persons relying on the qualified certificates issued, up to the amount equivalent in RON to **EUR 10,000** for each insured risk, in accordance with the legal requirements and the regulations of the Romanian Authority for Digitalization. The insured risk refers to each distinct damage caused by a breach of the provider's legal obligations.

8. 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.A.'s General InfoSEC Policy) and the measures described in the STSP.

9. Personnel policy

AlfaTrust Certification S.A. guarantees that every person who performs responsibilities within a Certification, Registration or Validation Authority:

- has completed at least secondary education;
- is a Romanian citizen;
- has signed a contract defining their role and responsibilities;
- has received advanced training relevant to the duties of the position
- has been trained on the protection of personal data and confidential information;
- has signed a contract that includes clauses on the protection of sensitive information and users' private data;
- does not perform tasks that generate conflicts of interest between the authorities involved.

Trusted personnel must demonstrate the qualifications, experience and background necessary to competently carry out their functions. Furthermore, where applicable, evidence of acceptance by the relevant governmental authorities must be provided.

Verification of personnel information is carried out initially and repeated at least once every five years, including:

- confirmation of previous jobs;
- verification of professional references;
- confirmation of completed studies;
- requesting the criminal record;
- Driving licence and social benefits assessments.

If the local law does not allow certain verifications, AlfaTrust Certification S.A. will use alternative methods allowed by law to ensure the same level of information.

10. Pricing Policy

The value of the certification services and the categories of services for which fees are charged are published in the price list available at <http://www.AlfaSign.ro>.

The services offered by AlfaTrust Certification S.A. are structured as follows:

- a) Individual certification services** – the fee is set for each certificate or a small number of certificates;
 - b) Service packages** – the tariff is calculated for a package of services provided to a single entity;
-

c) Subscription-based services – the fee is charged monthly and depends on the type and volume of services accessed;

d) Indirect services – the tariff is applied for services offered by AlfaTrust partners using the AlfaTrust infrastructure. For example, if a Certificate Authority is certified by AlfaTrust, a fee is charged per certificate issued by it.

Payment can be made in cash, by payment order or by bank card, based on an invoice, according to the applicable legal regulations.

Additional paid services may include:

- the sale of cryptographic devices;
- key generation for authorities or users
- application testing and inclusion in compatibility lists;
- sale of software licenses;
- design, installation and implementation services;
- information security consulting and auditing;
- training courses.

11. Internal audit and compliance control

AlfaTrust Certification S.A. periodically carries out internal audit and compliance control activities, in order to assess compliance with the provisions of Regulation (EU) no. 910/2014 (eIDAS), of Law no. 214/2024 and its own documentation (including STSP and this Policy).

The internal audit takes place at least once a year and includes checks on:

- the functioning of PKI infrastructure and HSM modules;
- compliance with the identification, issuance, revocation and archiving procedures;
- the activity of personnel holding critical roles in the chain of trust;
- records of security incidents and how to manage them;
- coherence between IT systems and publicly declared policies.

The results of the audit are documented and kept in an internal register, and the recommendations are implemented within a reasonable timeframe, with the follow-up of corrective actions.

12. Associated documents

This Certification and Electronic Seals Policy applies together with the following operational and legal documents of AlfaTrust Certification S.A.:

- Statement of Trust Services Practices (STSP);
- Timestamping policy;
- Business Continuity and Disaster Recovery Plan;
- General Terms and Conditions for the use of services;
- Code of Practices and Procedures (CPP).

These documents contain additional details regarding information security, the operation of trust services, contractual relationships, and risk scenarios. They may be consulted by competent authorities or partners, upon request or through the official website www.alfasign.ro.

13. Certification Policy Update

Amendments to the Certification Policy for Trust Services (CPS) will be periodically carried out by AlfaTrust Certification S.A. These will be published in the form of a separate document including the modifications or updates to this Policy and will be accessible in the official document repository at [http://www. AlfaSign.ro/](http://www.AlfaSign.ro/).