



Politica de certificare și sigilii electronice a AlfaTrust Certification S.A.

CUPRINS

1. Introducere.....	3
2. Tipuri de certificate și utilizări	4
3. Tipuri de sigilii și utilizări	5
4. Proceduri de identificare a utilizatorului în vederea emiterii certificatelor	5
4.1. Identificare fizică	6
4.2. Identificare la distanță prin mijloace video	6
4.3. Protecția datelor cu caracter personal	7
5. Arhitectura PKI	7

1. Introducere

Această Politică de Certificare și Sigilii Electronice (denumită în continuare „PCSE”) este emisă de S.C. AlfaTrust Certification S.A., în calitate de prestator de servicii de încredere calificat, înscris în Lista Trusted List a României și notificat la Autoritatea pentru Digitalizarea României (ADR), în conformitate cu Regulamentul (UE) nr. 910/2014 (eIDAS) privind identificarea electronică și serviciile de încredere, Legea nr. 214/2024 privind identificarea electronică și serviciile de încredere, Ordinul nr. 564/2021 emis de Autoritatea pentru Digitalizarea României privind reglementarea, recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanță utilizând mijloace video, precum și legislația națională complementară aplicabilă.

PCSE stabilește principiile generale aplicabile prestării de servicii de certificare (semnătură electronică și sigilii electronice – simple, avansate și calificate – emise, administrate, reînnoite și revocate de către AlfaTrust Certification S.A. Utilizatorii pot alege tipul de certificat în funcție de scopul dorit – autentificare, semnare, criptare, identificare, validare.

Această politică se aplică AlfaTrust Certification S.A., în calitate de prestator, Autoritate de Înregistrare (AI) și Autoritate de Validare (AV), precum și oricărei alte entități aflate în relație de subordonare sau în relație contractuală cu AlfaTrust Certification S.A. în exercitarea atribuțiilor AC, AI sau AV.

S.C. AlfaTrust Certification S.A. furnizează certificate și sigilii electronice simple, avansate și calificate, sub marca AlfaTrust Certification™, pentru orice categorie de utilizatori, în limitele stabilite de lege.

Obiectul și domeniul de aplicare al Politicii de Certificare și Sigilii Electronice

Prezenta Politică definește: stabilește cadrul operațional, juridic și procedural aplicabil furnizării de servicii de certificare și sigilii electronice de către AlfaTrust Certification S.A., incluzând:

- entitățile implicate în procesul de furnizare a serviciilor de încredere (Autoritatea de Certificare, Autoritatea de Înregistrare, Autoritatea de Validare), precum și responsabilitățile și obligațiile acestora;
- categoriile de certificate digitale și sigilii electronice emise de AlfaTrust Certification S.A.;
- tipurile de dovezi, informații și confirmări utilizate în procesele de identificare, înregistrare și validare;
- procedurile de verificare a identității utilizatorilor;
- domeniul de aplicare și limitele serviciilor furnizate în baza prezentei Politici.

Descrierea detaliată a acestor reguli, împreună cu măsurile tehnice și procedurale aplicabile, este inclusă în Declarația Practicilor privind Serviciile de Încredere furnizate de AlfaTrust Certification S.A. (prescurtat „DPSI”), document asociat prezentei Politici.

Cunoașterea și respectarea prevederilor PCSE și DPSI este esențială pentru utilizatorii finali, entitățile contractante și partenerii AlfaTrust Certification S.A.

2. Tipuri de certificate și utilizări

- a) **Certificate simple (necalificate) AlfaTrust Certification™** - pot fi utilizate pentru autentificarea utilizatorului, semnătură electronică și criptare (schimbul de chei simetrice).
- b) **Certificate avansate AlfaTrust Certification™** - pot fi utilizate pentru autentificare, semnătură electronică, autentificare servere web, criptare, semnare de cod, gateway-uri VPN, separat sau cumulativ, în funcție de serviciul în funcție de serviciul achiziționat sau solicitat de utilizator. Acestea pot fi utilizate ca dovadă a identității în cadrul tranzacțiilor electronice, în măsura în care legislația nu impune utilizarea unui certificat calificat. Semnătura electronică avansată nu beneficiază de prezumția legală de validitate prevăzută de art. 25 din Regulamentul (UE) nr. 910/2014 (eIDAS), ci doar în măsura în care este acceptată explicit de părțile implicate.
- c) **Certificate calificate AlfaTrust Certification™** - pot fi utilizate pentru semnătură electronică calificată, autentificare, criptare, autentificare servere web, semnare de cod și conectare la rețele VPN, separat sau în combinație, în funcție de serviciul ales. Acestea au

valoare juridică deplină și sunt recunoscute în toate statele membre ale UE, în conformitate cu art. 25 alin. din Regulamentul eIDAS.

3. Tipuri de sigilii și utilizări

a) **Sigiliile electronice calificate AlfaTrust Certification™** sunt utilizate exclusiv de persoane juridice și pot fi aplicate: pentru garantarea originii și integrității documentelor electronice; pentru autentificarea automată a entității juridice în sisteme informatice; în cadrul tranzacțiilor electronice, în conformitate cu Regulamentul (UE) nr. 910/2014 (eIDAS) și Legea nr. 214/2024. Aceste sigilii sunt opozabile terților, în condițiile prevăzute de lege, și pot produce efecte juridice echivalente semnăturii electronice calificate, însă exclusiv în numele persoanei juridice și fără implicarea unei voințe individuale. Ele asigură integritatea documentului, dar nu implică voință umană sau consimțământ personal.

b) **Sigiliile electronice avansate AlfaTrust Certification™** pot fi utilizate de persoane juridice pentru garantarea originii și integrității documentelor electronice și autentificarea automată a entității în cadrul sistemelor informatice. Acestea nu oferă aceleași garanții legale ca sigiliile calificate și nu sunt opozabile terților în lipsa unui acord expres, însă pot fi utilizate în relații contractuale, unde nivelul de încredere este acceptat de părți.

4. Proceduri de identificare a utilizatorului în vederea emiterii certificatelor

În vederea emiterii certificatelor și sigiliilor electronice, AlfaTrust Certification S.A. aplică măsuri riguroase pentru identificarea utilizatorilor, în conformitate cu:

- a) Regulamentul (UE) nr. 910/2014 (eIDAS);
- b) Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere;
- c) Normele ADR privind procedura de identificare la distanță prin mijloace video din 11.11.2021;
- d) Regulamentul (UE) 2016/679 (GDPR) și Legea nr. 190/2018.

Identificarea utilizatorului este obligatorie pentru emiterea certificatelor calificate, a sigiliilor calificate, precum și – opțional – pentru certificatele avansate sau sigiliile avansate, la solicitarea expresă a clientului.

Identificarea poate fi realizată prin una dintre următoarele metode:

4.1. Identificare fizică

Identificarea fizică presupune prezența utilizatorului în fața unui operator autorizat al Autorității de Înregistrare (AI), pe baza unui document oficial de identitate valabil, emis de o autoritate competentă. Operatorul AI:

- verifică autenticitatea documentului și conformitatea cu identitatea declarată;
- înregistrează operațiunea în sistemul intern securizat, arhivând copia actului de identitate în dosarul electronic al solicitantului.

4.2. Identificare la distanță prin mijloace video

AlfaTrust Certification S.A. oferă servicii de identificare electronică la distanță, în colaborare cu un terț specializat (împuternicit), în conformitate cu Normele ADR din 11.11.2021 și Legea nr. 214/2024.

Procedura este următoarea:

1. Inițierea identificării: utilizatorul accesează platforma terțului de identificare video, pusă la dispoziție prin link securizat, generat de AlfaTrust;
2. Verificarea video: terțul autorizat:
 - colectează și compară datele actului de identitate prezentat cu imaginea video în timp real;
 - aplică măsuri tehnice de verificare a liveness (prezență reală);
 - validează corespondența dintre imagine și act;
3. Transmiterea datelor: după finalizarea sesiunii, terțul transmite către AlfaTrust:
 - o înregistrare video sau capturi conforme;
 - copia actului de identitate;
 - raportul de identificare;
 - metadata tehnice (adresă IP, ora, durata sesiunii etc.);

- Validarea de către AI: operatorul AI AlfaTrust analizează documentația primită și, dacă nu există neconcordanțe, validează identificarea și autorizează emiterea certificatului sau sigiliului solicitat.

4.3. Protecția datelor cu caracter personal

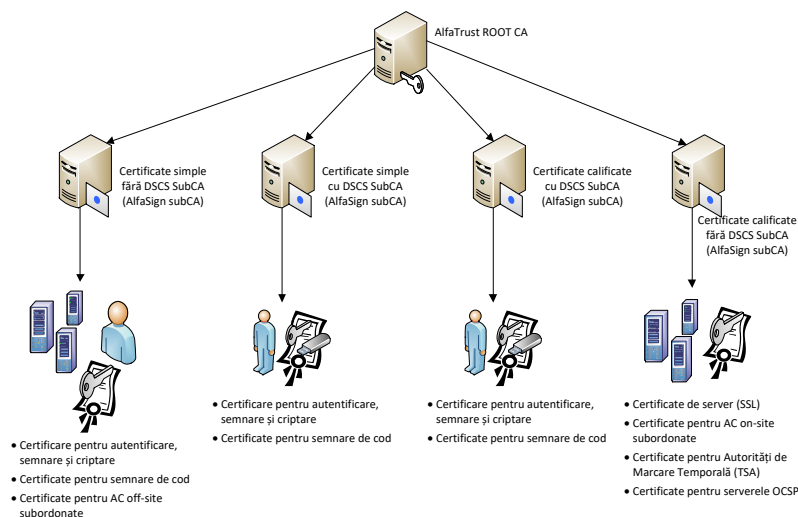
Datele colectate în cadrul ambelor forme de identificare (fizică și video) sunt prelucrate exclusiv în scopul emiterii de certificate sau sigilii electronice, în temeiul art. 6 alin. (1) lit. c) și e) din GDPR și Legea nr. 214/2024.

În cazul identificării video, terțul partener este desemnat împuternicit al operatorului (AlfaTrust Certification S.A.), în baza unui contract conform art. 28 din GDPR. Acesta are obligația de a respecta toate măsurile tehnice și organizatorice pentru asigurarea confidențialității, integrității și securității datelor.

Toate înregistrările sesiunilor video, actele de identitate și metadatele sunt păstrate conform politicilor interne și termenelor legale, iar accesul este permis doar persoanelor autorizate.

5. Arhitectura PKI

Structura infrastructurii cu chei publice (PKI) AlfaTrust Certification S.A. este prezentată în figura următoare:



6. Serviciile AlfaTrust Certification S.A.

În calitate de prestator de servicii de încredere calificate, notificat la Autoritatea pentru Digitalizarea României (ADR) și înscris în Lista Trusted List a României, AlfaTrust Certification S.A. oferă următoarele servicii:

- a) **Emiterea de certificate digitale** – simple, avansate sau calificate – către utilizatori finali (persoane fizice, persoane juridice, servere web, aplicații sau dispozitive hardware);
- b) **Furnizarea de servicii de sigilii electronice** – calificate sau avansate – destinate exclusiv entităților juridice;
- c) **oferirea de servicii de consultanță și/sau implementare a infrastructurilor de chei publice (PKI), precum și a unei game variate de soluții/servicii de securitate a informației** - aceste servicii de consultanță și securitate nu constituie servicii de încredere în sensul Regulamentului (UE) nr. 910/2014 (eIDAS), ci servicii conexe. Și nu sunt supuse supravegherii ADR.

6.1. Funcționalitatea certificatelor și interoperabilitatea

Certificatele digitale emise de AlfaTrust Certification™, destinate utilizatorilor, permit terților (inclusiv entităților partenere) să verifice semnăturile și sigiliile electronice digitale bazate pe certificatele sau sigiliile electronice emise de AlfaTrust Certification.

Conform art. 25 alin. (1)-(3) din Regulamentul (UE) nr. 910/2014 (eIDAS), o semnătură electronică calificată are același efect juridic ca o semnătură olografă și este recunoscută automat în toate statele membre UE, indiferent de statul în care a fost emis certificatul, locul în care a fost creată sau utilizată semnătura sau locul în care își desfășoară activitatea Autoritatea de Certificare sau utilizatorul.

6.2. Utilizarea certificatelor calificate

În mod implicit, certificatele calificate AlfaTrust Certification™ au scopuri generale și pot fi utilizate la nivel global. Utilizarea acestora nu este limitată la un anumit mediu de afaceri, cum ar fi un program pilot, un sistem de servicii financiare sau un mediu de piață virtuală.

S.C. AlfaTrust Certification S.A. sau ceilalți participanți nu sunt responsabili pentru monitorizarea sau impunerea vreunei restricții în aceste medii. Cu toate acestea, anumite certificate calificate AlfaTrust Certification™ au funcții limitate. De exemplu:

- certificatele ACP (Autoritățile de Certificare Primare) nu pot fi utilizate pentru alte funcții decât cele de ACP;
- certificatele de client nu pot fi folosite ca certificate de server și invers, cu excepția cazului în care extensiile permit explicit acest lucru;
- certificatele de utilizator final nu pot fi utilizate decât în limita extensiilor prezente în certificat.

Certificatele pot fi utilizate doar în scopul exprimat explicit în cererea de certificat și pentru care au fost create extensiile folosite la generarea lor. Tipurile de utilizare includ:

- a) **autentificare, semnare și criptare** (atât pentru certificatele simple cât și pentru cele calificate);
- b) **certificate de server, semnare de cod, Autoritate de Certificare** – ca serviciu suplimentar, la cererea expresă a clientului (valabil doar pentru SubCA-urile ce emit certificate calificate);
- c) **sigilii electronice.**

Fiecare utilizator care solicită un anumit tip de certificat sau serviciu trebuie să accepte condițiile contractuale asociate, în mod expres, printr-un acord scris formal care atestă acceptarea certificatelor AlfaTrust.

Semnăturile electronice avansate nu beneficiază de prezumția legală de validitate juridică prevăzută de art. 25 eIDAS, spre deosebire de semnăturile electronice calificate. Acest aspect este important pentru informarea clară a utilizatorilor în vederea evaluării gradului de protecție juridică oferit.

6.3. Tipuri de certificate emise

AlfaTrust Certification S.A. emite mai multe tipuri de certificate digitale, corespunzătoare unor arii diferite de aplicabilitate. Acestea includ:

1. **Certificate simple** – utilizate pentru autentificare, semnare electronică și criptare. Permit, de exemplu, semnarea e-mailurilor sau fișierelor și autentificarea utilizatorilor prin protocoale precum SSL.
2. **Certificate și sigilii electronice avansate** - utilizate pentru semnare, criptare și autentificare, fără a beneficia de efectele juridice ale celor calificate.
3. **Certificate și sigilii electronice calificate** – utilizate pentru semnarea documentelor cu valoare juridică, criptare și autentificare, având efecte juridice opozabile terților.
4. **Certificate pentru autentificarea serverelor și schimb de chei simetrice** – folosite de serviciile bazate pe protocoalele SSL/TLS/WTLS.
5. **Certificate pentru semnarea codului** – utilizate de dezvoltatori pentru protejarea integrității și autenticității software-ului.
6. **Certificate pentru Autorități de Certificare (AC)** - utilizate de entitățile care emit certificate digitale. Aria lor de aplicabilitate este determinată de extensiile certificate și de rolul desemnat (ex. utilizator final, AC, autoritate PKI). Acestea includ și certificatele operaționale ale AC.
7. **Certificate pentru validarea stării certificatelor - OCSP (Online Certificate Status Protocol)** – emise pentru serverele care furnizează răspunsuri privind validitatea certificatelor conform protocolului OCSP.
8. **Certificate pentru Autorități de Marcare Temporară (TSA)** – utilizate pentru generarea de mărci temporale electronice care asociază datele (documente, semnături, mesaje) cu un moment temporal verificabil.
9. **Certificate pentru sigilii electronice** – emise exclusiv persoanelor juridice, în scopul semnării automate și al garantării integrității datelor.

Formatul certificatului emis respectă standardul internațional X.509, elaborat de ITU-T, care stabilește structura tehnică a certificatelor digitale utilizate în infrastructurile PKI. Acest format permite interoperabilitatea globală, integrarea extensiilor obligatorii (cum ar fi OID-urile politicilor de certificare) și este cerut de standardele ETSI și Regulamentul (UE) nr. 910/2014 (eIDAS) pentru recunoașterea automată a certificatelor în Uniunea Europeană.

6.4. Condiții generale de utilizare

Certificatele emise de AlfaTrust Certification S.A. pot fi utilizate doar în următoarele condiții:

- sistemele utilizatorului gestionează în mod corespunzător cheile publice și private;
- certificatul este utilizat exclusiv în scopul declarat în cererea de emisie. Scopul utilizării certificatului este determinat de cererea inițială a utilizatorului și de extensiile incluse în certificatul emis (conform standardului X.509);
- dispun de mecanisme interne de verificare a stării certificatelor, de creare a cailor de certificare și controlul validității (validitatea semnăturii, data expirării etc.);
- utilizatorul are acces la informații clare despre certificatul emis, perioada de valabilitate, starea acestuia și responsabilitățile asociate.

6.4.1. Certificatele simple (necalificate)

Certificatele simple oferite de AlfaTrust Certification S.A. sunt disponibile în două configurații principale: fără DSCS și cu DSCS (DSCS – Dispozitiv de Securitate cu Cheie Stocată).

a) Certificatele simple fără DSCS pot fi utilizate în următoarele scopuri:

- pe servere web (certIFICATE SSL), pentru realizarea unui schimb securizat de chei simetrice, reducând riscul atacurilor de tip “*man-in-the-middle*” (în special în contextul utilizării schemei Diffie-Hellman);
- emiterea de certificate interne de către Autorități de Certificare aflate în infrastructura clientului, în baza politicii de certificare aplicabile în mediul respectiv. În cazul în care autoritatea de certificare funcționează în infrastructura clientului, aplicabilitatea și politicile de certificare pot fi definite de client, cu condiția acceptării prealabile de către AlfaTrust Certification S.A.

Aceste certificate respectă standardul ETSI TS 102 042 V2.1.1 (2009-05) și sunt asociate cu următorul identificator de politică (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),*

unde {AlfaTrustCertification} = 36915 reprezintă numărul de identificare atribuit de IANA pentru AlfaTrust Certification S.A., disponibil la www.iana.org/assignments/enterprise-numbers.

b) Certificate simple cu DSCS (Dovada Suportului pentru Controlul Securității)

Aceste certificate sunt destinate: autentificării utilizatorilor; semnării electronice; criptării datelor; semnării de cod informatic.

Acest tip de certificat este recomandat pentru medii cu nivel scăzut sau mediu de risc (ex: e-mailuri personale, acces la conturi private, aplicații interne), unde probabilitatea de acces neautorizat este redusă, iar eventualele breșe de securitate nu produc consecințe semnificative.

Certificatele cu DSCS permit autentificarea și verificarea integrității informației semnate, precum și protejarea confidențialității acesteia – în special în cadrul comunicațiilor prin poștă electronică.

Aceste certificate respectă standardul ETSI TS 102 042 V2.1.1 (2009-05) și sunt asociate cu următorul identificator de politică (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),*

unde {AlfaTrustCertification} = 36915 reprezintă numărul desemnat de IANA pentru AlfaTrust Certification S.A. (poate fi consultat la adresa www.iana.org/assignments/enterprise-numbers).

6.4.2. Certificatele și sigiliile calificate sau avansate

a) Certificatele și sigiliile calificate

Certificatele și sigiliile calificate emise de AlfaTrust Certification S.A. sunt acele certificate care respectă condițiile prevăzute de legislația în vigoare, fiind eliberate de un prestator de servicii de încredere calificat, în conformitate cu Regulamentul (UE) nr. 910/2014 (eIDAS) și cu dispozițiile Legii nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere.

Aceste certificate pot fi utilizate pentru:

- a) **autentificare, semnătură electronică calificată sau avansată, criptare** – cu DSCS (Dispozitiv de Securitate cu Cheie Stocată) sau prin certificate remote *AlfaCloud* emise și stocate pe module criptografice hardware securizate (HSM);
- b) **autentificarea serverelor web și certificate pentru Autorități de Certificare (AC)** – fără DSCS.

Semnătura electronică calificată, bazată exclusiv pe un certificat calificat, îndeplinește cumulativ următoarele condiții (cf. eIDAS):

- este legată în mod unic de semnatar;
- permite identificarea semnatarului;
- este creată printr-un dispozitiv calificat pentru crearea semnăturii electronice (QSCD), aflat exclusiv sub controlul semnatarului;
- este legată de datele semnate în așa fel încât orice modificare ulterioară a acestora este detectabilă.

CertIFICATELE CALIFICATE CU DSCS POT FI EMISE LOCAL SAU REMOTE (AlfaCloud) ȘI SUNT STOCATE PE MODULE HSM CONFORME, ÎN CONDIȚII CARE ASIGURĂ NIVELUL DE SECURITATE CERUT DE eIDAS ȘI DE NORMELE ADR PRIVIND IDENTIFICAREA VIDEO ȘI LIVRAREA QSCD.

b) Certificatele și sigiliile avansate

Un **certificat avansat** este emis pentru utilizarea unei **semnături electronice avansate**, care respectă următoarele cerințe:

- este legată exclusiv de semnatar;
- permite identificarea semnatarului;
- este creată utilizând date de creare a semnăturii aflate sub controlul exclusiv al semnatarului;
- este legată de datele semnate în așa fel încât orice modificare ulterioară este detectabilă.

Acest nivel este recomandat pentru: tranzacții electronice cu risc moderat sau ridicat; procese în care există probabilitatea de fraudă; semnarea unor documente cu valoare economică ridicată (în lipsa unei obligații legale de utilizare a unui certificat calificat, semnătura avansată nebeneficiind de prezumția legală de validitate prevăzută la art. 25 din Regulamentul (UE) nr. 910/2014 (eIDAS), doar în măsura în care părțile implicate acceptă în mod expres nivelul de încredere al semnăturii avansate.

6.4.3. Identificatori de politici (OID-uri ETSI)

CertIFICATELE ȘI SIGILIILE CALIFICATE EMISE DE ALFATRUST CERTIFICATION SUNT CONFORME CU STANDARDELE ETSI TS 101 456 V1.4.3 (2007-05) ASTFEL:

a) Certificate calificate cu DSCS

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),

Notă: {AlfaTrustCertification} = 36915 este identificatorul unic IANA atribuit AlfaTrust Certification S.A., disponibil public la: www.iana.org/assignments/enterprise-numbers.

0.4.0.194112.1.2 – QCP-n-qcsd - Certificate calificate emise către persoane fizice pe dispozitive criptografice QSCD, conform Regulamentului (UE) nr. 910/2014;

0.4.0.194112.1.3 – QCP-l-qcsd - Sigilii electronice calificate emise către persoane juridice pe dispozitive criptografice QSCD, conform Regulamentului (UE) nr. 910/2014.

b) Certificatele calificate fără DSCS

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),

Notă: {AlfaTrustCertification} = 36915 este identificatorul unic IANA atribuit AlfaTrust Certification S.A., disponibil public la: www.iana.org/assignments/enterprise-numbers.

Alegerea tipului de certificat

Abonatul AlfaTrust Certification poate alege tipul de certificat dorit în funcție de scopul utilizării. Detalii complete privind fiecare tip de certificat sunt disponibile în Declarația Practicilor privind Serviciile de Încredere (DPSI), accesibilă pe site-ul oficial www.alfatrust.ro. Informații suplimentare pot fi solicitate prin e-mail la: office@alfasign.ro.

6.5. Includerea de atribute suplimentare în certificatele digitale

AlfaTrust Certification S.A. poate, la cererea expresă a utilizatorului sau a entității contractante, să includă în certificatele digitale anumite **atribute suplimentare** (ex. profesii – „avocat”, „inginer”, „doctor”, coduri identificatoare – NIF, CNP, ID instituțional etc.).

Condiții și procedură:

a) **Justificare documentară** – Solicitantul trebuie să furnizeze documente doveditoare care atestă calitatea sau atribuția solicitată, precum:

- Decizia de admitere/numire în profesie sau certificatul de atestare a dreptului de exercitare a profesiei, emis de autoritatea competentă (ex. Baroul pentru avocați, CECCAR pentru experți contabili, UNNPR pentru notari). Nu este suficientă doar copia legitimației sau a cardului profesional;
- Adeverințe sau extrase din registre oficiale;
- În cazul NIF (Număr de Identificare Fiscală) sau alte identificatoare: dovada atribuirii de la autoritatea fiscală sau instituția emitentă.

b) **Validare de către Autoritatea de Înregistrare** – Personalul AlfaTrust Certification S.A. va analiza documentele și va confirma veridicitatea acestora, păstrând o copie conformă arhivată electronic, în sistemul intern de evidență.

c) **Inserarea atributului**

d) **Trasabilitate și responsabilitate** – Toate solicitările de inserare a atributelor sunt înregistrate în registrul AI (Autoritate de Înregistrare), cu:

- Data solicitării și aprobării;
- Numele operatorului responsabil;
- Documentele justificative arhivate.

e) **Actualizare sau revocare** – În cazul în care atributele devin nevalabile (ex: expirarea calității profesionale), utilizatorul are obligația de a solicita:

- actualizarea certificatului, sau
- revocarea acestuia.

6.6. Revocarea și suspendarea certificatelor

Orice certificat emis de AlfaTrust Certification S.A. poate fi revocat în următoarele cazuri:

- pierderea sau compromiterea datelor de creare a semnăturii/sigiliului (cheii private);
- schimbarea statutului juridic al utilizatorului (ex: dizolvarea persoanei juridice, încetarea mandatului);
- constatarea furnizării unor informații false sau inexacte în cererea de emitere;
- la solicitarea expresă a titularului;
- prin decizia prestatorului, în cazuri justificate (ex: activitate frauduloasă, solicitare din partea unei autorități competente).

Revocarea sau suspendarea se face fără întârziere, în maximum 24 de ore de la confirmarea motivului, și se reflectă imediat în registrul de certificate revocate (CRL) și prin serviciul OCSP.

7. Responsabilitățile părților implicate în utilizarea serviciilor AlfaTrust Certification S.A.

7.1.1. Responsabilitatea prestatorului de servicii de încredere calificat

AlfaTrust Certification S.A., în calitate de prestator de servicii de încredere calificate (inclusiv servicii de certificare, sigilii electronice și marcarea temporală), este responsabilă, în temeiul Regulamentului (UE) nr. 910/2014 (eIDAS), pentru prejudiciul adus oricărei persoane care își întemeiază conduita pe efectele juridice ale certificatelor, și anume:

- a) în ceea ce privește exactitatea, în momentul eliberării certificatului, a tuturor informațiilor pe care le conține;

- b) în ceea ce privește asigurarea că, în momentul eliberării certificatului, semnatarul identificat în cuprinsul acestuia deține datele de generare a semnăturii corespunzătoare datelor de verificare a semnăturii menționate în respectivul certificat;
- c) în ceea ce privește asigurarea că datele de generare a semnăturii corespund datelor de verificare a semnăturii, în cazul în care furnizorul de servicii de certificare le generează pe amândouă;
- d) în ceea ce privește revocarea certificatului, în cazurile și cu respectarea condițiilor prevăzute în legislație.

De asemenea, AlfaTrust Certification S.A., ca prestator de servicii de încredere calificate, poate să indice în cuprinsul unui certificat calificat restricții ale utilizării acestuia, precum și limite ale valorii operațiunilor pentru care acesta poate fi utilizat, cu condiția ca respectivele restricții să fie vizibile și ușor de recunoscut de către terți, conform art. 13 alin. (2) eIDAS.

AlfaTrust Certification S.A., ca furnizor de servicii de certificare, nu poate fi ținută responsabilă pentru prejudiciile rezultate din utilizarea unui certificat calificat cu încălcarea restricțiilor prevăzute în cuprinsul acestuia.

Utilizatorii care folosesc certificatele cu nerespectarea restricțiilor contractuale și tehnice asumă întreaga răspundere juridică pentru consecințele utilizării abuzive.

Garanțiile și limitele responsabilității dintre o Autoritate de Înregistrare și Autoritatea de Certificare care asistă emiterea certificatelor, pe de o parte, și utilizatorul respectiv, pe de altă parte, se supun și sunt guvernate de acordurile dintre aceștia, cu respectarea legislației în vigoare.

7.1.2. Garanțiile furnizorului de servicii de certificare (FSC)

AlfaTrust Certification S.A., ca prestator de servicii de încredere calificate, dispune de resurse financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfășurării activităților legate de certificarea semnăturilor electronice și a sigiliilor electronice. În acest sens, asigurarea s-a realizat prin subscrierea unei polițe de răspundere civilă profesională pentru prejudicii cauzate din neglijență, erori de identificare sau de emitere a certificatelor, la o societate de asigurări. Suma asigurată este conform celei stipulate de către Autoritatea pentru Digitalizarea României, în calitate de autoritate de reglementare și supraveghere specializată în domeniu.

Serviciile AlfaTrust Certification S.A. includ, de asemenea, o garanție pentru titulari, după cum urmează:

- Nu există interpretări greșite ale entităților care aprobă cererile pentru certificat sau care emit certificatul;
- Nu există erori privind informațiile referitoare la certificat, făcute de entitățile care răspund de aprobarea cererii pentru certificat, aceleași care răspund și de emiterea certificatului;
- Certificatele utilizatorilor satisfac toate cerințele acestei Politici precum și ale DPSI;
- Serviciile de revocare și utilizarea depozitului (sau registrului) sunt conforme cu această Politică și cu DPSI în toate aspectele importante.

Acordurile părților contractante conțin o garanție pentru părți care se bazează pe un certificat, în sensul că:

- Toate informațiile din sau încorporate într-un astfel de certificat, cu excepția informațiilor neverificate despre utilizator, sunt precise;
- În cazul certificatelor apărute în registrul AlfaTrust Certification S.A., certificatul a fost emis pentru o persoană fizică sau companie, iar utilizatorul a acceptat certificatul în concordanță cu specificațiile prezentei Politici și ale DPSI;
- Entitățile care aprobă cererile pentru certificat și emit certificatele vor respecta această Politică și DPSI atunci când emit certificatele;
- Utilizatorii care acceptă certificatele se obligă să le utilizeze în conformitate cu scopul și limitele declarate, pe baza unui consimțământ informat.

Responsabilitățile detaliate ale Autorităților de Înregistrare și ale entităților intermediare sunt reglementate în acordurile interne, în conformitate cu DPSI și cu normele ADR aplicabile.

7.2. Responsabilitățile utilizatorilor finali

Utilizatorii certificatelor AlfaTrust Certification S.A. au obligația să:

- utilizeze semnătura/sigiliul în mod propriu, în condițiile în care certificatul este valid (neexpirat sau nerevocat);
 - se asigure că nicio persoană neautorizată nu are acces la cheia privată;
 - garanteze veridicitatea tuturor informațiilor furnizate în cererea de emitere a certificatului;
 - utilizeze certificatul exclusiv în scopul declarat și conform PCSE și DPSI;
 - nu utilizeze certificatul în calitate de AC, inclusiv pentru semnarea altor certificate sau liste de revocare;
 - solicite revocarea imediat ce:
 - datele de creare a semnăturii/sigiliului au fost pierdute;
 - există suspiciuni că acestea au fost compromise;
 - informațiile esențiale din certificat nu mai corespund realității.

7.3. Responsabilitățile entităților partenere

Entitățile partenere au obligația de a verifica fiecare semnătură electronică de pe documentele recepționate, inclusiv validitatea certificatelor asociate. În acest scop, trebuie utilizate instrumentele de verificare puse la dispoziție de AlfaTrust Certification S.A., cum ar fi lista certificatelor revocate (CRL), serviciile OCSP, precum și lanțurile de încredere furnizate. Procedurile de verificare sunt detaliate în DPSI.

În cazul în care verificarea semnăturii nu reușește, documentul trebuie respins, iar validarea trebuie realizată prin alte metode conforme cu legislația aplicabilă și DPSI.

7.4. Responsabilități financiare

În limitele legii, AlfaTrust Certification S.A. poate solicita despăgubiri utilizatorilor, în următoarele cazuri:

- a) Furnizarea de informații false sau denaturate în cererea de emitere a certificatului;

- b) Omiterea unor informații esențiale, din neglijență sau cu intenție frauduloasă;
- c) Nerespectarea obligației de protecție a cheii private/ nerespectarea măsurilor de securitate aferente;
- d) Utilizarea unui nume (inclusiv nume comun, domeniu, e-mail) care încalcă drepturile de proprietate intelectuală ale unui terț.

AlfaTrust Certification S.A. va acoperi prejudiciile cauzate persoanelor care se bazează pe certificatele calificate emise, până la concurența sumei echivalente în lei a 10.000 EUR pentru fiecare risc asigurat, în conformitate cu cerințele legale și reglementările ADR. Riscul asigurat este fiecare prejudiciu distinct cauzat prin încălcarea obligațiilor legale ale furnizorului

8. Politica de Securitate a Informatiei

AlfaTrust Certification S.A. asigură securitatea serviciilor de certificare și sigilii electronice în conformitate cu Politica Generală a Securității Informației (PoG-SMSI – Politica Generală InfoSEC a AlfaTrust Certification S.A.) și măsurile descrise în DPSI.

9. Politica de personal

AlfaTrust Certification S.A. garantează că fiecare persoană care îndeplinește responsabilități în cadrul unei Autorități de Certificare, Înregistrare sau Validare:

- a absolvit cel puțin învățământul liceal;
- este cetățean român;
- a semnat un contract care definește rolul și responsabilitățile sale;
- a beneficiat de pregătire avansată relevantă pentru atribuțiile postului;
- a fost instruită privind protecția datelor personale și a informațiilor confidențiale;
- a semnat un contract ce include clauze privind protejarea informațiilor sensibile și a datelor private ale utilizatorilor;
- nu îndeplinește sarcini care generează conflicte de interese între autorități implicate.

Personalul de încredere trebuie să demonstreze calificările, experiența și istoricul necesare pentru a exercita funcțiile în mod competent. De asemenea, dacă este cazul, trebuie prezentate dovezi ale acceptării de către autoritățile guvernamentale relevante.

Verificarea informațiilor privind personalul se realizează inițial și se repetă cel puțin o dată la 5 ani, incluzând:

- confirmarea locurilor de muncă anterioare;
- verificarea referințelor profesionale;
- confirmarea studiilor absolvite;
- solicitarea cazierului judiciar;
- evaluări privind permisul de conducere și beneficiile sociale.

Dacă legea locală nu permite anumite verificări, AlfaTrust Certification S.A. va utiliza metode alternative permise de lege care să asigure același nivel de informare.

10. Politica de prețuri

Valoarea serviciilor de certificare și categoriile de servicii pentru care sunt percepute taxe sunt publicate în lista de prețuri disponibilă la adresa <http://www.AlfaSign.ro>.

Serviciile oferite de AlfaTrust Certification S.A. sunt structurate astfel:

- a) Servicii de certificare individuale** – tariful este stabilit pentru fiecare certificat sau un număr redus de certificate;
- b) Pachete de servicii** – tariful este calculat pentru un pachet de servicii prestate unei singure entități;
- c) Servicii bazate pe abonament** – tariful este perceput lunar și depinde de tipul și volumul serviciilor accesate;
- d) Servicii indirecte** – tariful este aplicat pentru serviciile oferite de partenerii AlfaTrust care utilizează infrastructura AlfaTrust. De exemplu, în cazul în care o Autoritate de Certificare este certificată de AlfaTrust, se percepe un tarif per certificat emis de aceasta.

Plata se poate realiza în numerar, prin ordin de plată sau cu card bancar, pe bază de factură, conform reglementărilor legale aplicabile.

Servicii suplimentare contra cost pot include:

- vânzarea de dispozitive criptografice;
- generarea de chei pentru autorități sau utilizatori;
- testarea aplicațiilor și includerea lor în listele de compatibilitate;
- vânzarea de licențe software;
- servicii de proiectare, instalare și implementare;
- consultanță și audit în domeniul securității informației;
- cursuri de instruire.

11. Audit intern și controlul conformității

AlfaTrust Certification S.A. desfășoară periodic activități de audit intern și control al conformității, în scopul evaluării respectării prevederilor Regulamentului (UE) nr. 910/2014 (eIDAS), ale Legii nr. 214/2024 și ale documentației proprii (inclusiv DPSI și prezenta Politică).

Auditul intern are loc cel puțin o dată pe an și include verificări privind:

- funcționarea infrastructurii PKI și a modulelor HSM;
- respectarea procedurilor de identificare, emiteră, revocare și arhivare;
- activitatea personalului cu roluri critice în lanțul de încredere;
- evidențele privind incidentele de securitate și modul de gestionare a acestora;
- coerența dintre sistemele informatice și politicile declarate public.

Rezultatele auditului sunt documentate și păstrate într-un registru intern, iar recomandările se implementează în termen rezonabil, cu urmărirea acțiunilor corective.

12. Documente asociate

Prezenta Politică de certificare și sigilii electronice se aplică împreună cu următoarele documente operaționale și juridice ale AlfaTrust Certification S.A.:

- Declarația Practicilor privind Serviciile de Încredere (DPSI);
- Politica de marcare temporală;
- Planul de continuitate și recuperare în caz de dezastru;
- Termenii și Condițiile generale de utilizare a serviciilor;
- Codul de Practici și Proceduri (CPP).

Aceste documente conțin detalii suplimentare privind securitatea informației, funcționarea serviciilor de încredere, relațiile contractuale și scenariile de risc. Ele pot fi consultate de autoritățile competente sau de parteneri, la cerere sau prin intermediul site-ului oficial www.alfasign.ro.

13. Actualizarea politicii de certificare

Modificările aduse Politicii de certificare a serviciilor de încredere (PCSE) vor fi realizate periodic de AlfaTrust Certification S.A. Acestea vor fi publicate sub forma unui document separat care include modificările sau actualizările prezentei politici și vor putea fi accesate în depozitul oficial al documentelor la adresa <http://www.AlfaSign.ro/>.