CODUL DE PRACTICI ȘI PROCEDURI ALFATRUST CERTIFICATION

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Cuprins

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

1. Introducere

Acest document constituie Codul de Practici şi Proceduri (numit în continuare prescurtat şi CPP) al S.C. AlfaTrust Certification S.A.

Acest CPP descrie practicile si procedurile de lucru pe care Furnizorul de Servicii de Certificare AlfaTrust Certification ("FSC") le utilizează în furnizarea serviciilor de certificare, care emite, administrează, revocă şi reînnoieşte certificatele în conformitate cu prevederile reglementărilor legale în materie, şi anume:

- Legea nr. 455/2001 privind semnătura electronică,
- Hotărârea Guvernului nr. 1259/2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, cu modificările ulterioare şi
- Directiva 1999/93/EC a Parlamentului European şi al Consiliului European şi încheiată la 13 Decembrie 1999 privind stabilirea cadrului comunitar pentru semnătură electronică, cu modificările şi completările ulterioare.

Acest cod de practici şi proceduri se aplică companiei S.C. AlfaTrust Certification S.A., ca Autoritate de Certificare (AC), Autoritate de Înregistrare (AÎ) și Autoritate de Validare a certificatelor emise (AV), precum şi oricăror AC-uri, AÎ-uri sau AV-uri aflate în relaţie de subordonate sau aflate în relaţie contractuală cu S.C. AlfaTrust Certification S.A.

1.1. Rolul Codului de Practici și Proceduri

Acest CPP prezintă şi explică practicile şi procedurile de lucru ale companiei AlfaTrust Certification S.A., conţinând printre altele:

- Îndatoririle autorităţii de certificare, ale autorităţii de înregistrare precum şi ale utilizatorilor de certificate digitale, în special în cazul certificatelor calificate;
- Problemele legale referitoare la serviciile de certificare oferite de compania AlfaTrust Certification S.A.;
- Revizuirea practicilor de securitate şi audit la care se supune compania AlfaTrust Certification S.A.;
- Metodele folosite pentru a confirma identitatea solicitanţilor certificatului;
- Procedurile operaţionale pentru serviciile de certificare, realizate de S.C. AlfaTrust Certification S.A; solicitări cu privire la emiterea, aprobarea, revocarea şi reînnoirea certificatelor;
- Procedurile de securitate operaţională pentru înregistrările de verificare, reţinerea rapoartelor şi recuperarea după dezastru utilizate în cadrul S.C. AlfaTrust Certification S.A;
- Practicile de securitate fizică, de personal, de management al cheilor şi de securitate logică ale S.C. AlfaTrust Certification S.A.;
- Lista de certificate emise, precum si lista de certificate revocate deţinute de S.C. AlfaTrust Certification S.A,
- Administrarea CPP-ului, inclusiv metode de îmbunătăţire.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

1.1.1. Rezumatul politicii de certificare

S.C. AlfaTrust Certification S.A. oferă certificate (simple și/sau calificate) AlfaTrust Certification™ pentru orice tip de utilizator, în limita legilor în vigoare.

Certificatele simple (necalificate) AlfaTrust Certification™ pot fi utilizate pentru autentificarea utilizatorului, semnătură electronică (***neopozabilă în justiție***) și criptare (schimbul de chei simetrice).

Certificatele calificate AlfaTrust Certification™ pot fi utilizate pentru autentificare, semnătură electronică extinsă (bazată pe certificat calificat – ***opozabilă în justiție***), criptare, autentificare servere Web, semnare de cod, pentru gateway-uri VPN, toate împreună sau separat (în funcţie de serviciul ales de beneficiar) ca dovadă a identităţii în orice tip de tranzacţii electronice.

Certificatele furnizează siguranţa identităţii utilizatorului pe baza prezenţei fizice a acestuia în faţa unei persoane care îi confirmă identitatea, folosind cel puţin o formă de identificare recunoscută de autorităţi.

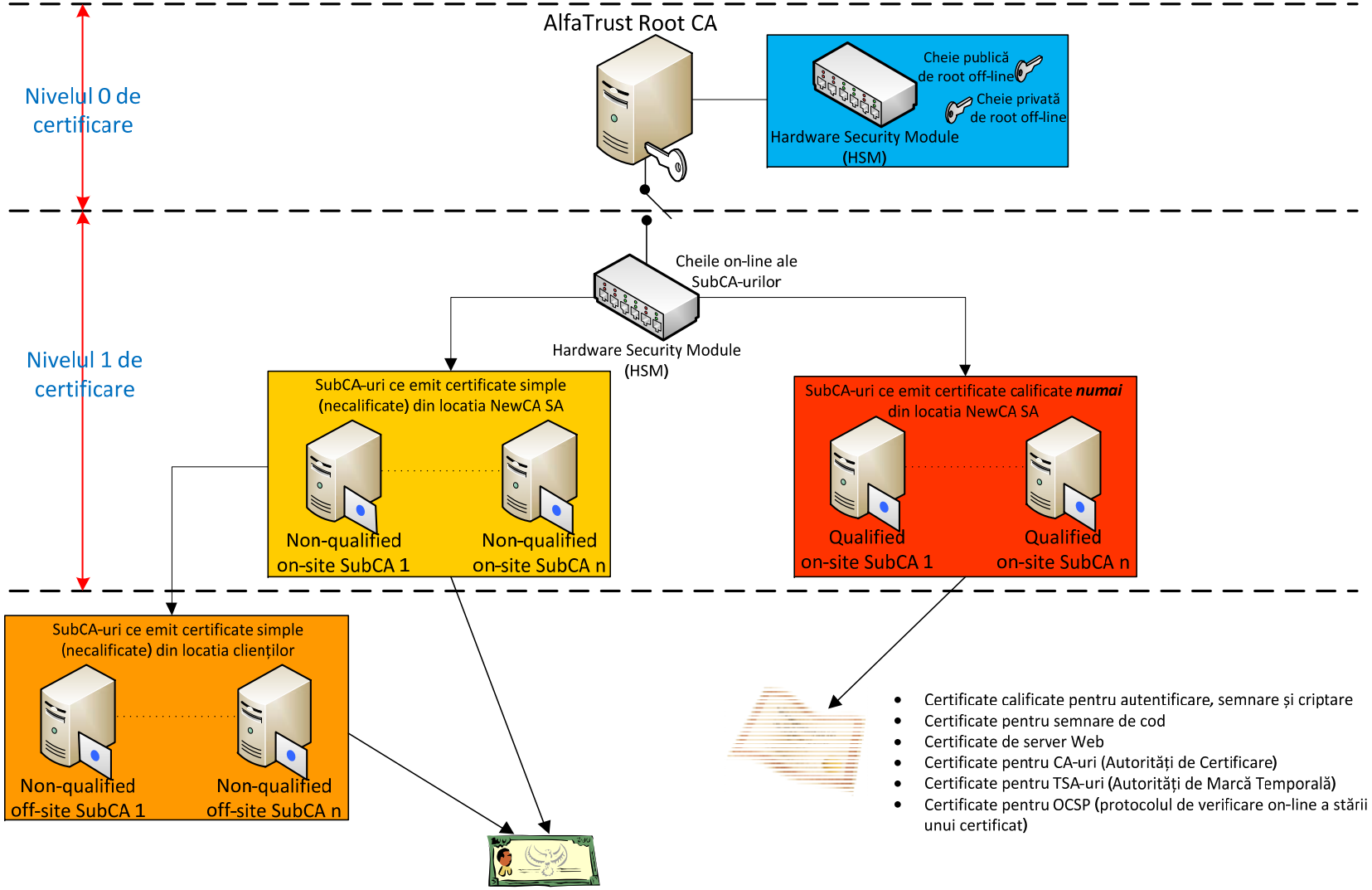
1.2. Privire de ansamblu asupra infrastructurii de certificare

Arhitectura Infrastructurii de Chei Publice (PKI) a AlfaTrust Certification este împărţită pe trei niveluri (vezi figura).

Nivelul 0 este format din AlfaTrust Certification ROOT CA. Autorităţile de certificare de pe nivelul 1 (on-site SubCA) sunt direct semnate de către AlfaTrust Certification ROOT CA. Autoritățile de pe nivelul 2 (off-site SubCA – toate necalificate, ce emit doar certificate simple) sunt semnate de SubCA-uri necalificate on-site, și se află plasate în locația clienților.

AlfaTrust Certification ROOT CA operează numai în mod off-line. În cazul compromiterii SubCA-urilor on-site, AlfaTrust Certification ROOT CA va fi folosită pentru a revoca certificatele acestora şi pentru a emite noi certificate. În cazul compromiterii SubCA-urilor off-site, unul din SubCA-urile necalificat on-site va fi folosit pentru a revoca certificatele acestora și pentru a emite noi certificate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195



- Certificate calificate pentru autentificare, semnare și criptare
- Certificate pentru semnare de cod
- Certificate de server Web
- Certificate pentru CA-uri (Autorități de Certificare)
- Certificate pentru TSA-uri (Autorități de Marcă Temporală)
- Certificate pentru OCSP (protocolul de verificare on-line a stării unui certificat)

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

1.3. Sfera de aplicabilitate

1.3.1. Sfera de aplicabilitate a prezentului CPP

Acest CPP se adresează tuturor participanţilor, incluzând AlfaTrust Certification S.A., distribuitori, utilizatori finali persoane fizice sau juridice, entităţi partenere şi alte părţi contractante. Acest CPP descrie practicile care guvernează utilizarea certificatelor calificate AlfaTrust Certification™. Utilizatorilor de servicii AlfaTrust Certification™ li se permite să folosească certificate emise pentru aplicaţii de mare securitate care sunt descrise în prezentul CPP.

Certificatele calificate AlfaTrust Certification™ destinate utilizatorilor permit terţilor (entităţilor partenere), participanţi în procesul de comunicare electronică să verifice semnăturile digitale bazate pe certificatele emise de AlfaTrust Certification.

Supusă legilor în vigoare, o semnătură digitală sau o tranzacţie interacţionând cu certificatul calificat AlfaTrust Certification™ va fi valid indiferent de locul în care certificatul calificat AlfaTrust Certification™ este emis sau de locul unde semnătura digitală a fost creată sau utilizată şi indiferent de locul unde AC-ul sau utilizatorul îşi desfăşoară activitatea.

În mod implicit (serviciul uzual pus la dispoziție), certificatele calificate AlfaTrust Certification™ au scopuri generale. Cerificatele calificate AlfaTrust Certification™ pot fi folosite la nivel global. Utilizarea certificatelor calificate AlfaTrust Certification™ nu este limitată la un anumit mediu de afaceri, cum ar fi un program pilot, un sistem de servicii financiare sau un mediu de piaţa virtuală.

S.C. AlfaTrust Certification S.A. sau ceilalţi participanţi nu sunt responsabili pentru monitorizarea sau impunerea vreunei restricţii în aceste medii.

Cu toate acestea, anumite certificate calificate AlfaTrust Certification™ au funcţii limitate. De exemplu, certificatele ACP (Autoritățile de Certificare Primare) nu pot fi utilizate pentru alte funcţii decât cele de ACP. Mai mult, certificatele pentru client se supun aplicaţiilor clientului şi nu pot fi folosite ca certificate de server.

Certificatele de utilizator final nu pot fi utilizate decât în limita extensiilor prezente în certificat, iar acestea sunt:

- **autentificare, semnare și criptare** (atât pentru certificatele simple cât și pentru cele calificate)
- **certificate de server, de semnare de cod, de AC, TSA și OCSP –** ca serviciu suplimentar, la cererea expresă a clientului (valabil doar pentru SubCA-urile ce emit certificate calificate).

În general, certificatele pot fi utilizate doar în scopul exprimat explicit în cererea de certificat și pentru care au fost create extensiile folosite la generarea lor.

1.3.2. Sfera de aplicabilitate a certificatelor emise de AlfaTrust Certification

Sfera de aplicabilitate a certificatelor stabileşte scopul în care poate fi folosit un certificat. Acest scop este definit de două elemente:

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- primul defineşte aplicabilitatea certificatului (de exemplu, semnatura electronica, autentificare, criptare),
- celălalt este o listă sau o descriere a aplicaţiilor permise sau interzise.

Certificatele emise de AlfaTrust Certification pot fi folosite preponderent pentru autentificare (utilizator sau mașină), semnătură electronică și criptare, sau la cererea clientului se pot customiza extensiile astfel încât cerfificatele să poată fi folosite și pentru semnare de cod, autentificare server Web, autentificare gateway-uri VPN având două nivele diferite de încredere.

Nivelul de sensibilitate al informațiilor ce se dorește a fi protejate trebuie evaluate de către utilizatorul final, aceasta stând la baza deciziei de a folosi unul din tipurile de certificate furnizate de AlfaTrust Certification.

În prezentul Cod de Practici şi Proceduri sunt definite două nivele de încredere a certificatelor:

- **Certificate simple (necalificate)** = Pot fi folosite pentru autentificarea utilizatorului, semnătură electronică (dar nu semnătură electronică extinsă, în întelesul dat de Legea 455/2001) și criptare. Acest nivel oferă o securitate de bază pentru informaţii în medii cu grad scăzut sau mediu de risc (risc fără consecinţe majore). Dintre acestea, menţionăm accesul la informaţii private acolo unde probabilitatea de apariţie a unui acces neautorizat nu este foarte mare. Aceste certificate pot fi folosite pentru a autentifica şi controla integritatea informaţiei care a fost semnată şi pentru a asigura confidenţialitatea informaţiei, mai ales în cazul poştei electronice.
- **Certificate calificate** = Certificatul calificat reprezintă un certificat care satisface condiţiile prevăzute la art. 18 din Legea 455/2001 şi care este eliberat de un furnizor de servicii de certificare ce satisface condiţiile prevăzute la art. 20 din aceeași lege. Aceste certificate pot fi utilizate pentru autentificare, creare de semnături electronice extinse, criptare, autentificare servere Web, semnare de cod, autentificare gateway-uri VPN. Semnătură electronică extinsă (care este bazată doar pe un certificat ***calificat***) reprezintă acea semnătură electronică care îndeplineşte cumulativ următoarele condiţii:

  a) este legată în mod unic de semnatar;

  b) asigură identificarea semnatarului;

  c) este creată prin mijloace controlate exclusiv de semnatar;

  d) este legată de datele în formă electronică, la care se raportează în aşa fel încât orice modificare ulterioară a acestora este identificabilă.

  Acest nivel se recomandă pentru asigurarea securităţii informaţiei în medii unde există riscul apariţiei de breşe de securitate iar consecinţele acestor breşe sunt moderate sau mari. Certificatele pot fi folosite pentru protecţia tranzacţiilor financiare sau a tranzacţiilor în care există şanse de apariţie a fraudelor. Aceste certificate pot fi folosite pentru protecţia tranzacţiilor de valoare nelimitată (dacă nu se specifică altceva în certificat), a tranzacţiilor în care există mari şanse de apariţie a fraudelor.

AlfaTrust Certification emite șapte tipuri de bază de certificate având arii diferite de aplicabilitate. Aceste sunt:

1. **certificate simple pentru autentificare, semnare și criptare** – permit semnarea emailurilor şi fişierelor, sau autentificarea unui utilizator (de exemplu prin protocolul SSL);

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

2. **certificate calificate** – permit autentificarea utilizatorului, criptarea mesajelor și semnarea documentelor cu valoare juridică;
3. **certificate pentru autentificarea serverelor și schimb de chei simetrice** – sunt folosite de serviciile care operează pe baza protocoalelor SSL/TLS/WTLS;
4. **certificate pentru semnarea codului** – folosite de programatori pentru a proteja software-ul împotriva falsificării;
5. **certificate pentru Autorităţile de Certificare** – folosirea lor nu este restricţionată la aria definită; aria de aplicabilitate poate fi dată de extensia din certificate ce stabileşte modul în care poate fi folosită cheia privată (vezi câmpul *KeyUsage*, Capitolul 6), sau de rolul acesteia (de exemplu, utilizator final, Autoritate de Certificare sau altă autoritate care furnizează servicii PKI); acest tip conţine de asemenea şi certificatele operaţionale ale Autorităţilor de Certificare;
6. **certificate pentru confirmarea stării unui certificat** – sunt emise pentru serverele care funcţionează conform protocolului OCSP şi care furnizează informaţii despre starea certificatelor;
7. **certificate pentru Autorităţi de Marcare Temporala** – sunt emise serverelor care, ca răspuns la cererea unui utilizator al serviciului de time-stamping, emit mărci temporale prin care asociază unor date (documente, mesaje, semnaturi electronice etc.) un moment de timp pe baza căruia se poate determina secvenţialitatea în timp a datelor.

Certificatele emise în concordanţă cu politicile de certificare AlfaTrust Certification pot fi folosite în aplicaţii ce satisfac cel puţin următoarele condiţii:

- gestionează corespunzător cheile publice şi private,
- certificatele şi cheile publice asociate acestora sunt folosite în concordanţă cu scopul declarat al acestora, confirmat de către AlfaTrust Certification,
- dispun de mecanisme interne de verificare a stării certificatelor, de creare a căilor de certificare şi controlul validităţii (validitatea semnaturii, data expirării etc.),
- oferă utilizatorului informaţii corespunzătoare despre certificate şi starea acestora.

Lista aplicaţiilor recomandate este publicata pe site la adresa: http://www.AlfaSign.ro .

Aplicaţiile sunt incluse în lista aplicaţiilor recomandate pe baza unor declaraţii scrise ale producătorilor şi/sau pe baza testelor făcute de AlfaTrust Certification. AlfaTrust Certification permite fiecărui utilizator final să-şi genereze singur cheile criptografice folosite în procesul de certificare prin intermediul dispozitivelor recomandate. Autoritatea de Certificare poate de asemenea să genereze cheile pe un dispozitiv criptografic şi apoi să livreze utilizatorului final dispozitivul împreună cu cheile. În acest caz, AlfaTrust Certification foloseşte dispozitive criptografice ce satisfac cel puţin cerinţele standardului FIPS PUB 140-2.

1.3.3. Autorități de certificare (AC)

Termenul autoritate de certificare cuprinde toate entităţile care emit certificate respectând propriul CPP, care poate fi acelaşi pentru fiecare ACP, sau poate diferi de la un ACP la altul, în funcţie de scopul ACP-ului. Termenul “ACP” se referă la o subcategorie de emitenţi numite autorităţi de certificare primare (ACP), care se comportă ca rădăcini (eng. root). Fiecare ACP este o entitate AlfaTrust Certification™. Subordonate ACP-ului sunt autorităţile de certificare, care emit certificate abonaţilor-utilizatori finali sau

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

altor AC-uri. Toate ACP-urile AlfaTrust Certification™ ce emit certificate calificate sunt găzduite de centrul de procesare propriu, aflat pe teritoriul României, în locaţiile strict securizate.

Autoritatea de Certificare AlfaTrust Certification ROOT CA este o Autoritate de Certificare Primară pentru domeniul AlfaTrust Certification. Toate celelalte Autorităţi de Certificare din cadrul acestui domeniu sunt subordonate AlfaTrust Certification ROOT CA.

Autoritatea de Certificare Primară AlfaTrust Certification ROOT CA poate înregistra în depozitul de la nivelul Autorității de Validare şi emite certificate numai Autorităţilor de Certificare Subordonate (numite de acum încolo SubCA-uri și care vor avea în nume AlfaSign).

Înainte de a începe activitatea, fiecare autoritate de certificare subordonată (SubCA) trebuie să trimită o cerere către Autoritatea de Certificare Principală AlfaTrust Certification ROOT CA pentru înregistrare şi emitere de certificat de cheie publică (a se vedea şi procedurile descrise în subcapitolul 5.1.1.1). Autoritatea AlfaTrust Certification ROOT CA funcţionează pe baza unui certificat autosemnat, emis de ea însăşi. Într-un astfel de certificat, extensia **certificatePolicies** lipseşte (vezi subcapitolul 6.1.1), ceea ce semnifică faptul că nu există limitări ale setului de căi de certificare la care certificatul AlfaTrust Certification ROOT CA poate fi ataşat.

Autoritatea de Certificare AlfaTrust Certification ROOT CA reprezintă punctul de încredere pentru clienţii AlfaTrust Certification. Prin urmare, fiecare cale de certificare trebuie să înceapă cu certificatul autorităţii AlfaTrust Certification ROOT CA.

Autoritatea de Certificare AlfaTrust Certification ROOT CA furnizează servicii de certificare pentru:

- sine (emite şi reînnoieşte certificate proprii),
- Autorităţile de Certificare înregistrate în domeniul de certificare AlfaTrust Certification,
- entităţi ce furnizează servicii de verificare on-line a stării certificatelor şi ale entităţilor ce oferă servicii de non-repudiere (de exemplu, servicii de marcare temporală).

Autorităţile de Certificare Subordonate (SubCA-urile AlfaSign) sunt configurate pentru a emite certificate către:

* utilizatori care vor să-şi asigure securitatea şi credibilitatea poştei electronice şi a altor servicii (de exemplu, comerţ electronic, semnarea codului software) prin intermediul certificatelor,
* entităţi care oferă servicii de marcare temporală,
* furnizori de servicii din domeniul telecomunicaţiilor mobile,
* dispozitive de reţea care realizează conexiuni criptate prin VPN,
* utilizatori în vederea oferirii de servicii pe bază de certificate de chei publice cum ar fi serviciul de verificare on-line a stării certificatelor (OCSP),
* alte Autorităţi de Certificare.

Orice entitate externa care doreste incheierea unui contract pentru operarea unui CA subordonat AlfaTrust Certification va incheia cu AlfaTrust Certification un contract prin care se obliga sa respecte versiunile curente ale CPP și să se supună unui audit pentru verificarea conformitatii cu legislația în vigoare și cu politicile și procedurile AlfaTrust Certification.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

1.3.4. Autorități de înregistrare (AÎ)

AI-ul asistă un AC prin îndeplinirea funcţiilor de confirmare a identităţii, de aprobare sau respingere a cererilor pentru certificat, de cerere a revocării certificatelor şi de aprobare sau respingere a cererilor de reînnoire.

Nivelul de precizie al procesului de determinare a identităţii clientului este dat de nevoile utilizatorului final şi este impus de nivelul certificatului pe care îl solicită.

În cazul celei mai simple identificări, Autoritatea de Înregistrare verifică doar corectitudinea adresei de e-mail trimisă. Cea mai precisă identificare presupune prezenţa în persoană a solicitantului la Autoritatea de Înregistrare şi furnizarea de dovezi cu privire la identitatea sa.

Identificarea poate fi realizată fie automat (în cazul certificării identității persoanei de către o autoritate cu competențe în acest sens conform legilor din România), fie manual de către un operator al Autorităţii de Înregistrare (în cazul prezentării viitorului utilizator final la sediul AlfaTrust Certification).

Toate AI-urile AlfaTrust Certification™ care asista ACP-urile AlfaTrust Certification™ la emiterea de certificate abonaţilor-utilizatori finali sunt găzduite în propriile locaţii securizate.

1.3.5. Autoritatea de Validare (AV)

Autoritatea de Validare este punctul în care Autoritatea de Certificare depozitează certificatele generate și lista de certificate revocate (urmare a cererilor primite prin intermediul Autorității de Înregistrare). Tot Autoritatea de Validare este responsabilă de generarea răspunsului la interogările primite prin OCSP (protocolul de verificare online a stării certificatelor).

Autoritatea de Validare AlfaTrust Certification se află în locația securizată a AlfaTrust Certification S.A.

1.3.6. Utilizatorii finali și entitățile partenere

Un utilizator final este o entitate al cărei identificator este plasat în câmpul Subject al unui certificat şi care nu emite certificate altor entităţi.

O Entitate Parteneră este o entitate care foloseşte certificatul unui utilizator final pentru a verifica semnatura electronica a acestuia sau pentru a asigura confidenţialitatea informaţiilor transmise.

Orice persoană fizică sau juridică, precum şi dispozitivele hardware pe care acestea le deţin pot fi utilizatori finali ai serviciilor oferite de AlfaTrust Certification, în condiţiile respectării legii. În particular, operatorii Autorităţii de Înregistrare, ceilalţi angajaţi AlfaTrust Certification şi echipamentele indispensabile pentru asigurarea securităţii infrastructurii AlfaTrust Certification (firewall-uri, routere, servere de autentificare) reprezintă, de asemenea, utilizatori finali.

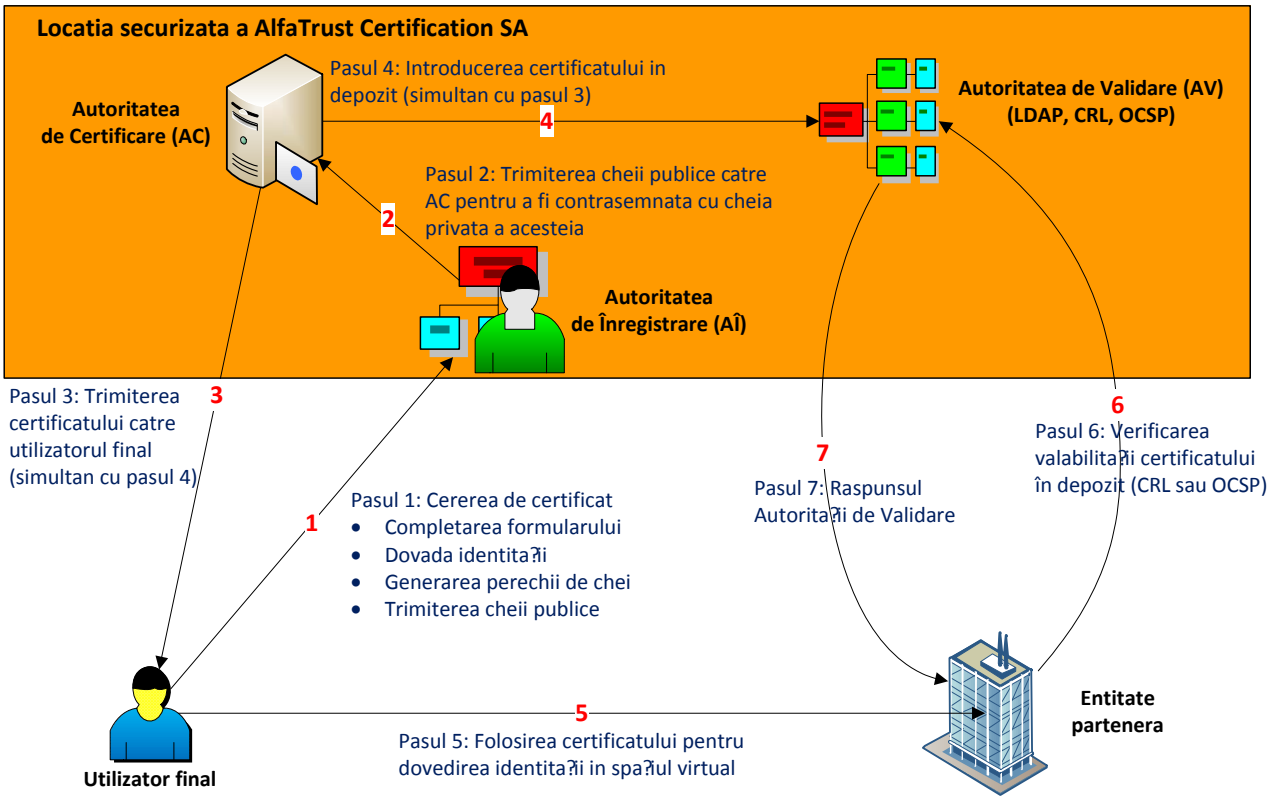
Organizaţiile (utilizatorii finali persoane juridice) care doresc să obţină certificate emise de AlfaTrust Certification S.A. pentru angajaţii lor, pot să o facă prin intermediul reprezentanţilor lor, pe când utilizatorii finali persoane fizice trebuie să ceară personal un certificat.

AlfaTrust Certification emite certificate de tipuri diferite şi de niveluri de încredere diferite. Utilizatorii finali trebuie să decidă ce tip de certificat este cel mai potrivit pentru nevoile lor.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

O Entitate Parteneră poate fi orice entitate ce utilizează serviciile AlfaTrust Certification şi care ia decizii bazându-se pe corectitudinea legăturii dintre identitatea unui utilizator final şi cheia sa publică (legătură confirmată de una din Autorităţile de Validare AlfaTrust Certification).

În principiu, furnizarea serviciului de certificare al AlfaTrust Certification urmează paşii din figura de mai jos:



1.4. Detalii de contact

Întrebări despre prezentul Cod de Practici şi Proceduri (CPP) pot fi adresate la următoarea adresă:

S.C. AlfaTrust Certification S.A.

Calea Victoriei 155, bl. D1, tr. 8, etj. 7, sect. 1, Bucureşti

E-mail: cpp@AlfaSign.ro

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

2. Dispoziții generale

2.1. Obligații

2.1.1. Obligațiile Autorității de Certificare (AC)

S.C. AlfaTrust Certification S.A. face eforturi continue ca să asigure buna legătura dintre serviciile oferite utilizatorilor finali şi entităților partenere, ambii constituindu-se în părţi contractante, obligaţiile ambelor părţi fiind stipulate clar şi fără echivoc în cadrul contractului dintre părţi în spiritul prezentului CPP.

O Autoritate de Certificare (AC) care emite certificate, asumându-şi politica de certificare aflată în mod public la dispoziţia utilizatorului final în vederea consultării, are următoarele obligaţii principale:

1. Crearea unui document care să reflecte clar modalităţile de lucru, procedurile aplicabile şi aplicate, politica generală a firmei, obligaţiile şi drepturile părţilor contractante, etc. - CPP (Codul de Practici şi Proceduri) şi afişarea lui în mod public (pe Internet) după ce a fost aprobat de persoanele responsabile din cadrul AC-ului;
2. Modul de desfăşurare a activităţii AC-ului să se conformeze strict cu prevederile CPP-ului aprobat;
3. Modalitatea de punere în practică a CPP-ului şi a Politicilor de Certificare ale AC-ului să se bazeze pe o infrastructura (de comunicaţii, software şi hardware) fiabilă, capabilă în orice moment de a garanta buna desfăşurare a activităţii AC-ului conform cu politica de funcţionare 24x7 impusă nu numai de legile româneşti în vigoare privind Autorităţile de Certificare ce emit certificate calificate, dar şi de realităţile lumii contemporane în ceea ce priveşte afacerile desfăşurate pe Internet;
4. Garantarea faptului că cererile de emitere de certificate sunt procesate (în sensul identificării persoanei numai pe baza modalităţilor puse la dispoziţie de legile române în vigoare) numai de o AI aflată în legătură contractuală cu AC-ul emitent de certificate (şi căruia i se subordonează), şi care la rândul ei se conformează cadrului general stabilit de prezentul CPP, în strânsă legătură şi cu documentul ce statutează Politica de Certificare a AC-ului;
5. Garantarea faptului că activitatea AI-ului pe linia identificării persoanelor ce se înregistrează în vederea obţinerii unui certificat digital calificat se desfăşoară în litera şi spiritul Legii nr. 677/ 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
6. Garantarea faptului că informaţiile incluse în certificate sunt valide şi conform realităţii la momentul aprobării certificatului, precum şi garantarea menţinerii conform Legii 455/2001 a actelor ce fac dovada identităţii persoanelor înregistrate în vederea eliberării certificatului calificat;
7. Garantarea aducerii la cunoştinţa utilizatorilor a obligaţiilor pe care le au în concordanţă cu acest CPP, prin prisma faptului că sunt posesori şi virtuali utilizatori ai certificatelor digitale calificate, precum şi informarea acestora asupra riscului la care se supun prin nerespectarea acestor obligaţii;
8. Revocarea certificatelor acelor utilizatori despre care s-a stabilit (sau există dubii) că au acţionat contrar obligaţiilor ce revin utilizatorilor, aşa cum se desprind ele din acest CPP, cu obligativitatea AC-ului de a anunţa utilizatorul despre măsura luată;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

9. Serviciile de înregistrare în vederea emiterii de certificate şi de ridicare a certificatelor în urma aprobării acestora, servicii ce sunt destinate utilizatorului final trebuie să fie furnizate exclusiv prin mijloace electronice, bazate pe o infrastructură care să permită rularea acestora pe Internet (iar în cazuri particulare pe Intranet), cu obligativitatea AC-ului de a menţine un registru de evidentă a certificatelor emise de către toate ACP-urile subordonate, registru ce trebuie actualizat dinamic astfel încât el să reflecte situaţia la zi a certificatelor emise către abonaţi;

2.1.2. Obligațiile Autorității de Înregistrare (AÎ)

AI constă într-un centru de procesare unde se garantează îndeplinirea funcţiilor de validare, de aprobare sau respingere a cererilor pentru certificat prin cererea revocării certificatelor şi prin aprobarea cererilor de reînnoire. În prevederile CPP-ului sunt specificate obligaţiile AI AlfaTrust Certification S.A.

O AI care realizează funcţii de înregistrare se va conforma prevederilor acestui CPP aprobat. AC-urile sunt responsabile pentru asigurarea faptului că certificatele sunt generate şi administrate în conformitate cu acest CPP şi cu Politica de Certificare a AC-ului, şi că funcţiile de generare, administrare şi retragere a certificatelor sunt realizate numai de cei care înţeleg cerinţele politicii de certificare asociate şi care sunt de acord să le respecte. Cerinţele de securitate impuse AC-urilor sunt asemănătoare celor impuse oricăror AI-uri datorită faptului că AI-urile sunt responsabile pentru informaţia colectată. AI este responsabila cu:

1. Autentificarea entităților care solicită certificate digitale;
2. Validarea informațiilor furnizate de entitățile finale;
3. Validarea drepturilor entităților finale de a obține certificate de un anumit tip;
4. Verificarea faptului că entitatea finală deține într-adevăr cheia privată asociată cheii publice pentru care a solicitat un certificat digital. Acest proces este denumit în literatura de specialitate “dovada deținerii cheii private” (POP – Proof of Possession);
5. Distribuirea de chei si/sau certificate către abonaţi;
6. Trimiterea de cereri către AC pentru eliberarea, revocarea sau reînnoirea certificatelor;
7. Verificarea prealabila a datelor furnizate de abonaţi pentru aceste cereri, conform cerinţelor din CPP;
8. Asigurarea faptului ca PIN-ul si cheia privată ce urmează să se distribuie către abonat nu sunt interceptate de către terţe părţi;
9. Transmiterea unui contract („Acordul Părţilor”) ce urmează a fi semnat, către fiecare utilizator ce urmează a fi deţinătorul unui certificat.

2.1.3. Obligațiile Autorității de Validare (AV)

Autoritatea de Validare AlfaTrust Certification conține trei componente principale:

1. Depozitul (repository), ce este în principiu un server LDAP unde se țin toate certificatele împreună cu datele lor de validare,
2. Lista Certificatelor Revocate (CRL), ce conține certificatele revocate până la un moment bine stabilit de timp,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

3. Protocolul de verificare online a stării certificatelor (OCSP), ce poate specifica în timp real dacă un certificat este valabil sau nu.

Depozitul este gestionat şi controlat de Autoritatea de Validare, prin urmare AlfaTrust Certification se obligă:

* să depună toate eforturile pentru a se asigura că toate certificatele publicate în depozit aparţin utilizatorilor finali înscrişi în certificate, iar utilizatorii şi-au dat acordul asupra acestor certificate,
* să se asigure că certificatele Autorităţilor de Certificare aparţinând domeniului AlfaTrust Certification precum şi certificatele utilizatorilor (după aprobarea lor) sunt publicate şi arhivate la timp,
* să asigure publicarea şi arhivarea Politicii de Certificare, a Codului de Practici şi Proceduri, a listei aplicaţiilor şi dispozitivelor recomandate,
* să permită accesul la informaţiile despre starea certificatelor prin publicarea de Liste de Certificate Revocate (CRL), prin intermediul serverelor OCSP sau prin interogări HTTP,
* să asigure accesul permanent la informaţiile din depozit pentru Autorităţile de Certificare, Autoritatea de Înregistrare, utilizatori finali şi Entităţile Partenere,
* să publice CRL-urile sau alte informaţii în timp util şi în concordanţă cu termenele limită specificate în Politica de Certificare,
* să asigure accesul sigur şi controlat la informaţiile din depozit.

2.1.4. Obligaţiile utilizatorului final

Codul de Practici şi Proceduri şi Politica de Certificare sunt parte integrantă a fiecărui contract încheiat între un utilizator final şi AlfaTrust Certification. Prin aplicarea pentru înregistrare la Autoritatea de Înregistrare şi semnarea confirmării de înregistrare, utilizatorul este de acord să se integreze în sistemul de certificare în condiţiile statuate în documentele menţionate mai sus.

În funcţie de relaţiile dintre AlfaTrust Certification şi un abonat şi de nivelul de credibilitate al certificatului solicitat de utilizator, obligaţiile pot fi formulate sub forma unui contract între abonat şi AlfaTrust Certification.

Prin contract, utilizatorul final se angajează:

* să fie de acord cu termenii contractului;
* să aprobe fiecare certificat emis pentru el; garanţiile şi obligaţiile AlfaTrust Certification în legătură cu un anumit tip de certificat sunt valide din momentul aprobării certificatului de către utilizator;
* să ia măsurile necesare care să-i permită să genereze în mod corespunzător (de către el însuşi sau de către Autoritatea de Înregistrare) şi să stocheze în siguranţă cheia privată din cadrul unei perechi de chei (pentru a preveni pierderea, compromiterea, modificarea şi folosirea neautorizată a acesteia);
* să folosească dispozitivele şi aplicaţiile software recomandate de AlfaTrust Certification în cazul în care utilizatorul îşi generează singur cheile;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- să declare date corecte în aplicaţiile trimise Autorităţii de Înregistrare care apoi sunt stocate în baza de date a AlfaTrust Certification şi în certificate de chei publice emise; un utilizator trebuie să fie conştient de responsabilităţile ce îi revin pentru daunele directe şi indirecte provocate ca urmare a falsificării datelor;
- să accepte faptul că fiecare semnatură electronică creată prin intermediul unei chei private, aparţinând utilizatorului şi asociată unui certificat aprobat care conţine cheia publică corespunzătoare, reprezintă semnatura utilizatorului şi să recunoască faptul că certificatul nu a fost invalid (în afara datei de valabilitate) şi nici revocat sau suspendat atunci când a fost creată semnatura;
- să cunoască în general noţiunile referitoare la certificate, semnaturi electronice şi PKI.

De asemenea, utilizatorul final se angajează:

- să se supună regulilor din prezentul Cod de Practici şi Proceduri şi Politica de Certificare,
- să genereze cheile criptografice, să gestioneze parolele, cheile publice şi private, să schimbe informaţii cu Autoritatea de Înregistrare şi Autorităţile de Validare numai prin intermediul aplicaţiilor software recomandate de către AlfaTrust Certification; accesul la acest software, mediile şi dispozitivele pe care sunt stocate cheile şi parolele trebuie să fie controlat în mod adecvat,
- să considere pierderea sau dezvăluirea parolei (dezvăluirea parolei către o persoană neautorizată) ca o pierdere sau dezvăluire a cheii private (dezvăluirea acesteia către o persoană neautorizată),
- să nu permită accesul la cheile sale private persoanelor neautorizate,
- să nu folosească ca utilizator final o cheie privată asociată unui certificat emis de AlfaTrust Certification, pentru semnarea de CRL-uri sau certificate,
- să facă dovada posesiei cheii private la Autoritatea de Înregistrare sau Validare sau să demonstreze posesia acesteia în alt mod,
- să nu dezvăluie parolele persoanelor neautorizate,
- să transmită Autorităţii de Înregistrare documentele cerute care să confirme informaţiile incluse în aplicaţia trimisă şi identitatea celui ce a transmis cererea sau a entităţii ce acţionează în numele utilizatorului,
- în cazul în care se constată încălcarea securităţii (sau există suspiciunea de încălcare a securităţii) cheilor private, să anunţe emitentul certificatului ,
- să folosească certificatele de chei publice şi cheile private corespunzătoare numai în scopurile declarate în certificat şi în concordanţă cu ariile de aplicabilitate şi restricţiile stabilite prin Codul de Practici şi Proceduri,
- să obţină certificate de chei publice ale Autorităţilor de Certificare şi Autorităţii de Înregistrare precum şi cele corespunzătoare altor servicii oferite de AlfaTrust Certification.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

2.1.5. Obligațiile entităților partenere

Codul de Practici şi Proceduri şi Politica de Certificare sunt parte integrantă a fiecărui contract încheiat între AlfaTrust Certification, o entitate parteneră şi / sau un utilizator. Obiectul unui astfel de contract poate fi:

* furnizarea de servicii tip depozit, servicii de marcă temporală şi servicii de verificare a stării certificatelor (OCSP) – în cazul încheierii de contracte cu AlfaTrust Certification;
* specificarea condiţiilor pe care trebuie să le îndeplinească o semnatură electronică pentru a fi considerată validă de către o entitate parteneră – în cazul încheierii de contracte cu un utilizator;

În funcţie de relaţiile dintre o entitate parteneră şi AlfaTrust Certification sau un abonat şi de nivelele certificatelor acceptate de o entitate parteneră, obligaţiile entităţilor partenere sunt stabilite în cadrul unui contract încheiat între AlfaTrust Certification şi entitatea parteneră.

Prin contract, Entitatea Parteneră se angajează:

* să fie de acord şi să respecte termenii şi condiţiile din contract. Drepturile şi obligaţiile părţilor încep să îşi producă efectele începând cu data încheierii contractului.
* să verifice cu atenţie fiecare semnatură electronică de pe un certificat sau document recepţionat. Pentru a verifica semnatura, entitatea parteneră trebuie:
    i. să specifice calea de certificare ce conţine toate certificatele Autorităţilor de Certificare care fac posibilă verificarea semnaturii de pe certificatul semnatarului,
    ii. să se asigure că, din perspectiva creării semnăturii calea de certificare aleasă este cea mai bună; în unele cazuri, este posibil să existe mai mult de o cale pornind de la un certificat dat (prin intermediul căruia a fost creată semnatura) şi până la o Autoritate de Certificare pe care se bazează verificarea semnaturii,
    iii. să verifice că nici unul din certificatele din calea de certificare, aparţinând AlfaTrust Certification, nu se află în listele de certificate revocate sau suspendate,
    iv. să verifice că toate certificatele din calea de certificare aparţin unor Autorităţi de Certificare şi că acestea sunt autorizate să semneze alte certificate,
    v. (opţional) să specifice data şi ora la care a fost semnat un document sau mesaj. Acest lucru este posibil numai dacă documentul sau mesajul a fost marcat (înainte de semnare) cu o marcă temporală emisă de o Autoritate de Marcare Temporală, sau semnaturii electronice i s-a asociat o marcă temporală imediat după semnarea documentului; o astfel de verificare permite implementarea de servicii de non-repudiere sau se poate folosi pentru rezolvarea disputelor,
    vi. să verifice, folosind o cale de certificare definită, credibilitatea certificatului semnatarului documentului sau mesajului şi autenticitatea semnăturii,
* să efectueze corect operaţiile criptografice, folosind aplicaţii software şi dispozitive având un nivel de securitate corespunzător nivelului de sensibilitate al certificatului procesat şi nivelului de credibilitate al certificatelor folosite,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- să considere o semnatură electronică ca fiind invalidă dacă prin mijloacele software sau dispozitivele folosite nu este posibil să se determine dacă semnatura electronică este validă sau dacă rezultatul verificării este negativ,
- verificarea semnăturii electronice îşi propune să stabilească dacă:
    1. semnătura electronică a fost creată prin intermediul unei chei private corespunzătoare unei chei publice dintr-un certificat emis de AlfaTrust Certification pentru un utilizator final şi
    2. mesajul (documentul) semnat nu a fost modificat după semnare.
- să aibă încredere numai în acele certificate de chei publice care:
    1. sunt folosite în concordanţă cu scopul declarat şi corespund ariilor de aplicabilitate specificate de entitatea parteneră, de exemplu, printr-o politică de semnatură,
    2. a căror stare a fost verificată pe baza Listelor de Certificate Revocate (CRL) corespunzătoare, sau prin intermediul serviciului OSCP al AlfaTrust Certification.
- să specifice condiţiile pe care un certificat de cheie publică şi o semnatură electronică trebuie să le îndeplinească pentru a fi considerate valide; aceste condiţii pot fi formulate, de exemplu, sub forma unor politici de certificare acceptate şi apoi publicate.

Orice document cu o semnatură electronică eronată, sau dubioasă trebuie să fie respins sau supus altor proceduri care ar putea permite determinarea validităţii sale. Orice persoană care aprobă un asemenea document poartă responsabilitatea pentru consecinţele ce decurg din acest fapt.

Entitatea parteneră trebuie să ia la cunoştinţă prevederile Codului de Practici şi Proceduri şi Politica de Certificare (garanţii şi responsabilităţi).

2.2. Responsabilitate

2.2.1. Responsabilitatea Furnizorului de Servicii de Certificare (FSC)

Răspunderea AlfaTrust Certification S.A. ca furnizor de servicii de certificare este reglementată de lege în sensul că, în art. 41 din Legea nr. 455/2001 privind semnătura electronică, se prevede că furnizorul de servicii de certificare, care eliberează certificate prezentate ca fiind calificate sau care garantează asemenea certificate, este răspunzător pentru prejudiciul adus oricărei persoane care îşi întemeiază conduita pe efectele juridice ale respectivelor certificate:

a) în ceea ce priveşte exactitatea, în momentul eliberării certificatului, a tuturor informaţiilor pe care le conţine;

b) în ceea ce priveşte asigurarea că, în momentul eliberării certificatului, semnatarul identificat în cuprinsul acestuia deţinea datele de generare a semnăturii corespunzătoare datelor de verificare a semnăturii menţionate în respectivul certificat;

c) în ceea ce priveşte 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;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

d) în ceea ce priveşte revocarea certificatului, în cazurile şi cu respectarea condiţiilor prevăzute la art. 17 alin. (1), (2) şi (3);

e) în privinţa îndeplinirii tuturor obligaţiilor prevăzute la art. 13-17 şi la art. 19-22, cu excepţia cazurilor în care furnizorul de servicii de certificare probează că, deşi a depus diligenţa necesară, nu a putut împiedica producerea prejudiciului.

De asemenea, AlfaTrust Certification S.A. ca furnizor de servicii de certificare poate să indice în cuprinsul unui certificat calificat restricţii ale utilizării acestuia, precum şi limite ale valorii operaţiunilor pentru care acesta poate fi utilizat, cu condiţia ca respectivele restricţii să poată fi cunoscute de terţi.

AlfaTrust Certification S.A. ca furnizorul de servicii de certificare nu va fi răspunzătoare pentru prejudiciile rezultând din utilizarea unui certificat calificat cu încălcarea restricţiilor prevăzute în cuprinsul acestuia (art. 42 din Legea nr. 455/2001 privind semnătura electronică).

Garanţiile şi limitele responsabilităţii dintre o AI şi AC care asistă emiterea certificatelor pe de o parte, şi utilizatorul respectiv, pe de altă parte, se supun şi sunt guvernate de către acordurile dintre aceştia cu respectarea legilor în vigoare.

2.2.1.1. Garanţiile Furnizorului de Servicii de Certificare

AlfaTrust Certification S.A. ca furnizor de servicii de certificare calificată, dispune de resurse financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfăşurării activităţilor legate de certificarea semnăturilor electronice. În acest sens, asigurarea s-a realizat prin subscrierea unei poliţe de asigurare la o societate de asigurări.

Suma asigurată este conform celei stipulate de către Ministerul Comunicaţiilor si Societății Informaționale, în calitate de autoritate de reglementare si supraveghere specializată în domeniu. (art. 22 din Legea nr. 455/2001 privind semnătura electronică).

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

- Nu există interpretări greşite ale entităţilor care aprobă cererile pentru certificat sau care emit certificatul,
- Nu există erori privind informaţiile referitoare la certificat, făcute de entităţile care răspund de aprobarea cererii pentru certificat, aceleaşi care răspund şi de emiterea certificatului,
- Certificatele utilizatorilor satisfac toate cerinţele acestui CPP,
- Serviciile de revocare şi utilizarea depozitului (sau registrului) conform cu acest CPP în toate aspectele importante.

Acordurile părţilor contractante conţin o garanţie pentru părţi care se bazează pe un certificat în care:

- Toate informaţiile din sau incorporate într-un astfel de certificat, excepţie făcând informaţiile 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 şi utilizatorul a acceptat certificatul în concordanţă cu specificaţiile prezentului CPP;
- Entităţile care aprobă cererile pentru certificat şi emit certificate au respectat acest CPP atunci când au emis certificatele.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

2.2.1.2. Forţa majoră

În măsura limitelor legale, serviciile AlfaTrust Certification S.A. şi acordurile părţilor contractante includ o clauză de forţă majoră care protejează părţile.

2.2.2. Responsabilitatea utilizatorului

Serviciile AlfaTrust Certification S.A. cer abonaţilor să garanteze că:

- Fiecare semnătura digitală creată prin utilizarea cheii private corespunzătoare cheii publice din certificat este semnătura digitală a utilizatorului şi că certificatul a fost acceptat şi este operaţional (nu este expirat sau revocat) la momentul în care semnătura digitală a fost creată;
- Nici o persoană neautorizată nu a avut acces la cheia privată a utilizatorului;
- Toate relatările făcute de utilizator în cererea pentru certificat sunt adevărate;
- Toate informaţiile furnizate de utilizator şi conţinute de certificat sunt adevărate;
- Certificatul este folosit exclusiv pentru scopul declarat, în concordanţă cu CPP;
- Utilizatorul este un utilizator final, nu un AC şi nu foloseşte cheia privată corespunzătoare cheii publice din certificat pentru semnarea digitală a oricărui certificat (sau orice alt format de cheie publică certificată) sau lista de revocare a certificatelor, ca AC sau în altă calitate.

Titularii de certificate sunt obligaţi să solicite, de îndată, revocarea certificatelor, în cazul în care:

- au pierdut datele de creare a semnăturii electronice;
- au motive să creadă că datele de creare a semnăturii electronice au ajuns la cunoştinţa unui terţ neautorizat;
- informaţiile esenţiale cuprinse în certificat nu mai corespund realităţii.

2.2.3. Responsabilitatea părților contractante

Părţile contractante admit că au informaţii suficiente pentru a lua o decizie în măsura în care au ales să se bazeze pe informaţiile dintr-un certificat, că sunt singurii responsabili pentru decizia de a se baza sau nu pe astfel de informaţii, şi că vor suporta consecinţele legale în cazul nerespectării obligaţiilor de către părţi, conform capitolului 2.1.5. din prezentul CPP.

2.3. Responsabilități financiare

În măsura limitelor legale, S.C. AlfaTrust Certification S.A. solicită abonaţilor să o despăgubească în unul din următoarele cazuri:

1. Falsitate sau relatare greşită în cererea pentru certificate;
2. Relatarea greşită a unei informaţii importante în cererea pentru certificat, dacă relatarea greşită sau omisiunea a fost făcută din neglijenţă sau cu intenţia de a înşela una dintre părţi;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

3. Neprotejarea cheii private sau neluarea măsurilor de protecţie necesare prevenirii, compromiterii, pierderii, dezvăluirii, modificării sau folosirii neautorizate a cheii private a utilizatorului;
4. Utilizatorul a folosit un nume (inclusiv un nume comun, nume de domeniu sau adresa de e-mail), care încalcă drepturile de proprietate intelectuală a unui terţ.

AlfaTrust Certification S.A. va acoperi prejudiciile pe care le-ar putea cauza cu prilejul desfăşurării activităţi de certificare persoanelor care îşi întemeiază conduita pe efectele juridice ale certificatelor calificate, până la concurenţa echivalentului în lei al sumei de 10.000 euro pentru fiecare risc asigurat. Riscul asigurat este fiecare prejudiciu produs, chiar dacă se produc mai multe asemenea prejudicii ca urmare a neîndeplinirii de către furnizor a unei obligaţii prevăzute de lege.

2.4. Legea aplicabilă și soluționarea litigiilor

Prevederile cuprinse în prezentul Cod de Practici si Proceduri se supun legii române în materie, lege care guvernează şi interpretarea clauzelor cuprinse în acest document.

În situaţia apariţiei unei neînţelegeri între părţile contractante, acestea vor încerca soluţionarea acestora în termen de 60 de zile de la notificarea transmisă de către o parte către cealaltă parte (perioadă de negociere iniţială) şi, în cazul în care părţile nu ajung la o soluţie acceptată de comun acord, acestea se pot adresa instanţei de judecată competente.

2.5. Prețul serviciilor prestate

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

Serviciile oferite de AlfaTrust Certification S.A. sunt stabilite după cum urmează:

a) **servicii de certificare individuale** – preţul este stabilit pentru fiecare serviciu în parte, de exemplu, pentru fiecare certificat vândut sau un număr mic de certificate,

b) **pachete de servicii de certificare** – preţul este stabilit pentru pachete de servicii prestate unei singure entităţi,

c) **servicii prestate pe baza de abonament** – preţul este stabilit pentru servicii prestate lunar; valoarea sumelor plătite depinde de tipul şi numărul serviciilor accesate şi este utilizat în special (dar nelimitându-se la acestea) pentru serviciile de marcare temporală şi de verificare a stării certificatelor prin intermediul protocolului OCSP,

d) **servicii indirecte** – preţul este stabilit pentru fiecare serviciu oferit clienţilor săi de un partener AlfaTrust Certification S.A., care îşi bazează activitatea pe infrastructura AlfaTrust Certification; de exemplu, dacă o Autoritate de Certificare comercială este certificată de AlfaTrust Certification, atunci AlfaTrust Certification va percepe un preţ pentru fiecare certificat emis de Autoritatea de Certificare respectivă.

Plăţile se vor face in numerar, prin ordin de plata, inclusiv folosind carduri bancare pe baza de factura, conform reglementarilor legale în vigoare.

AlfaTrust Certification S.A. poate presta şi alte servicii contra cost, cum ar fi:

* vânzarea de dispozitive criptografice de orice tip, în funcţie de nevoile utilizatorului,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- generarea cheilor pentru Autorităţile de Certificare sau utilizatori,
- testarea aplicaţiilor şi includerea lor în lista aplicaţiilor recomandate,
- vânzarea de licenţe,
- activităţi de proiectare, implementare şi instalare,
- activități de consultanță și audit în domeniul securității informației,
- vânzarea de copii tipărite ale Codului de Practici şi Proceduri, Politicii de certificare, manuale, ghiduri de utilizare etc.
- cursuri de instruire.

AlfaTrust Certification S.A. face eforturi pentru a asigura cel mai înalt nivel de securitate pentru serviciile oferite. Dacă un utilizator sau o entitate parteneră nu este mulţumită de serviciile oferite, pot solicita revocarea certificatului şi rambursarea sumelor plătite în 30 de zile de la data emiterii certificatului. După această perioada, utilizatorul are dreptul de a solicita revocarea certificatului şi rambursarea sumelor aferente perioadei rămase până la expirarea certificatului dacă AlfaTrust Certification S.A. nu-şi îndeplineşte obligaţiile şi îndatoririle specificate în Codul de Practici şi Proceduri.

Cererile de rambursare trebuie trimise la adresa specificată în Capitolul 1.4.

2.6. Publicarea și înregistrarea informațiilor

2.6.1. Publicarea informațiilor de către AlfaTrust Certification S.A.

Depozitul (repository) este o interfaţă publică către următoarele informaţii:

- versiunea curentă şi cea anterioară a Politicii de Certificare şi a Codului de Practici şi Proceduri,
- Modelele de contract cu utilizatorii finali şi Entităţile Partenere,
- Declaraţia AlfaTrust Certification S.A. cu privire la asigurarea confidenţialităţii informaţiilor recepţionate şi procesate,
- Registrul (în accepţiunea Legii 455/2001 a semnaturii electronice),
- certificatul AlfaTrust Certification ROOT CA, precum şi certificatele tuturor Autorităţilor de Certificare care aparţin sau sunt legate la domeniul AlfaTrust Certification,
- certificatele utilizatorilor finali (entităţi fizice şi juridice, inclusiv angajaţii AlfaTrust Certification S.A. şi maşinile / aplicaţiile software deţinute de aceştia şi care sunt indispensabile pentru serviciile PKI) conform Legii 455/2001 a semnaturii electronice.

În plus, în Depozit se găsesc informaţii legate de funcţionarea certificatelor, cum ar fi:

- Listele de certificate Revocate (CRL); CRL-urile sunt disponibile în aşa numitele puncte de distribuţie a CRL-urilor, a căror adresă este specificată în fiecare certificat emis de AlfaTrust Certification; locaţia principala de distribuţie a CRL-urilor este în depozit la adresa: http://crl.AlfaSign.ro,
- Alte informaţii ce se modifică frecvent sau în timp real,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Conţinutul depozitului este disponibil prin Internet la adresa: http://www.AlfaSign.ro/depozit sau prin intermediul protocolului LDAP v3, la adresa "***ldap.AlfaSign.ro, port 346***".

2.6.2. Frecvența publicării

Informaţiile publicate de AlfaTrust Certification sunt actualizate cu următoarea frecvenţă:

- Politica de Certificare şi Codul de Practici şi Proceduri – la aprobarea inițială și ori de câte ori se modifică,
- certificatele Autorităţilor de Certificare din cadrul AlfaTrust Certification – după emiterea unui nou certificat,
- certificatul Autorităţii de Înregistrare – după emiterea unui nou certificat,
- certificatele Abonaţilor – după fiecare emitere a unui nou certificat,
- Lista certificatelor Revocate – vezi Capitolul "frecvența de emitere a CRL-ului",
- Rapoartele de audit efectuate de instituţiile autorizate – în momentul în care AlfaTrust Certification intră în posesia lor,
- Informaţiile suplimentare – după fiecare actualizare.

2.6.3. Controlul accesului la informații

Toate informaţiile publicate de AlfaTrust Certification în depozit la adresa http://www.AlfaSign.ro/depozit sunt accesibile public.

AlfaTrust Certification a implementat mecanisme logice şi fizice de protecţie împotriva adăugării, ştergerii şi modificării informaţiilor publicate în depozit.

În momentul descoperirii unor breşe ce afectează integritatea informaţiilor din depozit, AlfaTrust Certification va lua măsurile corespunzătoare pentru a restabili integritatea informaţiilor, va trage la răspundere pe cei vinovaţi şi va notifica entităţile afectate.

2.7. Auditul de conformitate

Auditurile au ca obiectiv verificarea consistenţei acţiunilor AlfaTrust Certification sau a entităţilor delegate de aceasta cu declaraţiile şi procedurile acestora (inclusiv Politica de Certificare şi Codul de Practici şi Proceduri).

Auditurile desfăşurate de AlfaTrust Certification urmăresc în principal centrele de procesare a datelor şi procedurile de gestiune a cheilor. De asemenea, aceste audituri au în vedere şi Autorităţile de Certificare de pe calea de certificare a AlfaTrust Certification ROOT CA, Autoritatea de Înregistrare sau alte elemente ale infrastructurii de chei publice, cum ar fi de exemplu serverele OCSP.

Auditurile desfăşurate de AlfaTrust Certification pot fi efectuate de echipe interne (audit intern) sau de organizaţii independente (audit extern). În ambele cazuri, auditul se desfăşoară la cererea şi sub supravegherea administratorului de securitate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

2.7.1. Frecvența auditului de conformitate

Auditul extern prin care se verifică compatibilitatea cu reglementările legale şi procedurale (în special cu Politica de Certificare şi Codul de Practici şi Proceduri) se desfăşoară cel puţin o dată la patru ani, în timp ce un audit intern este efectuat cel puţin o dată pe an.

2.7.2. Identitatea/calificarea auditorului

Auditul extern este realizat de către o instituţie cu activitatea în domeniul consultanței și al auditului sistemelor informatice sau al managementului securității informației şi care este independentă faţă de AlfaTrust Certification S.A. O asemenea instituţie trebuie să:

* angajeze personal având cunoştinţe şi experienţă tehnică corespunzătoare (să dispună de documente care să certifice acest lucru) în domeniul infrastructurilor de chei publice, tehnologiilor şi dispozitivelor de securitate informatică şi de auditare a securităţii sistemelor,
* fie organizaţie sau societate înregistrată şi de renume.

Auditul intern este realizat de către departamentul de calitate şi audit al AlfaTrust Certification S.A.

2.7.3. Ariile supuse

Auditurile interne şi externe se desfăşoară conform regulilor şi procedurilor acceptate pe plan internaţional pentru Autorităţile de Certificare şi vizează:

- securitatea fizică a AlfaTrust Certification,
- procedurile de verificare a identităţii utilizatorilor,
- serviciile de certificare şi procedurile de furnizare a serviciilor,
- securitatea aplicaţiilor software şi a accesului la reţea,
- securitatea personalului AlfaTrust Certification,
- jurnalele de evenimente şi procedurile de monitorizare a sistemului,
- arhivarea şi restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru CA-uri,
- înregistrările referitoare la analizele şi verificările efectuate pentru aplicaţiile software şi dispozitivele hardware.

2.7.4. Acțiuni acceptate ca rezultat al neconformităților

Rezultatele auditurilor interne şi externe sunt transmise managementului AlfaTrust Certification S.A. În termen de 10 zile de la transmiterea rezultatelor, acesta va pregăti o opinie scrisă cu privire la

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

neconformitățile sesizate şi va propune un plan de acţiune şi termene de rezolvare, pentru închiderea neconformităților. Informaţiile referitoare la modul de închidere a neconformităților vor fi trimise auditorului.

În cazul neconformităților majore ce reprezintă o ameninţare directă asupra procesului de certificare a Autorităților de Certificare din domeniul AlfaTrust Certification, administratorul de securitate poate lua decizia suspendării temporare a activităţii acestora. Toţi clienţii AlfaTrust Certification vor fi anunţaţi de măsura luată şi timpul estimativ în care autoritatea respectivă îşi va relua activitatea. Notificarea se poate face prin intermediul depozitului, prin e-mail şi – în cazuri absolut necesare – prin publicarea în presă.

2.8. Confidențialitate

Toate informaţiile pe care le deţine AlfaTrust Certification S.A. au fost obţinute, păstrate şi procesate în concordanţă cu legile în vigoare, în mod special cu Legea românească privind protecţia datelor cu caracter personal (Legea 677/2001) şi cu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice. Relaţiile dintre un utilizator, o entitate parteneră şi AlfaTrust Certification se bazează pe încredere.

O terţă parte poate avea acces doar la informaţiile disponibile public în certificate. Celelalte date furnizate în aplicaţiile trimise către AlfaTrust Certification nu vor fi dezvăluite în nici o circumstanţă vreunei terţe părţi, în mod voluntar sau intenţionat (cu excepţia situaţiilor prevăzute de lege).

AlfaTrust Certification S.A. poate avea acces la cheile private ale utilizatorilor doar în cazurile:

1. cererilor de generare şi arhivare a cheilor, trimise de utilizator,
2. trimiterii chei generate local, pentru arhivare în bazele de date AlfaTrust Certification.

Arhivarea cheilor de criptare se face doar la solicitarea expresă a clientului. AlfaTrust Certification nu arhivează niciodată cheile de semnare.

O parte va fi exonerată de răspunderea pentru dezvăluirea de informaţii confidenţiale, dacă:

a) informaţia era cunoscută părţii contractante înainte ca ea să fi fost primită de la cealaltă parte contractantă;

sau

b) informaţia a fost dezvăluită după ce a fost obţinut acordul scris al celeilalte părţi pentru asemenea dezvăluire;

sau

c) partea a fost obligată în mod legal să dezvăluie informaţia.

Dezvăluirea oricărei informaţii faţa de persoanele implicate în îndeplinirea obligaţiilor, se va face confidenţial şi se va extinde numai asupra acelor informaţii necesare în vederea îndeplinirii obligaţiilor.

2.8.1. Tipuri de informații confidențiale

AlfaTrust Certification S.A., angajaţii acesteia precum şi entităţile care desfăşoară activităţi de certificare sunt obligate să păstreze secretul informaţiilor, atât pe durata, cât şi după încetarea contractului de muncă, în cazul angajaţilor.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Sunt catalogate drept informaţii private sau confidenţiale:

- informaţiile furnizate de utilizatori, în plus faţă de informaţiile ce trebuie transmise reevaluate pentru efectuarea serviciilor de certificare; în celelalte cazuri, dezvăluirea informaţiilor primite necesita în prealabil o aprobare scrisă din partea proprietarului informaţiei sau în alte condiţii prevăzute de lege,
- informaţiile furnizate de, sau către utilizatori (de exemplu, conţinutul contractelor încheiate cu utilizatorii finali sau Entităţile Partenere, conturi bancare, aplicaţiile de înregistrare, emitere, reînnoire, revocare certificate – cu excepţia informaţiilor incluse în certificate sau din depozit, conform prezentului Cod de Practici şi Proceduri); o parte din informaţiile menţionate mai sus poate fi dezvăluită doar cu aprobarea şi în scopul menţionat de proprietarul informaţiilor (de exemplu, utilizatorul),
- înregistrările corespunzătoare tranzacţiilor din sistem (toate tipurile de tranzacţii, precum şi datele pentru controlul tranzacţiilor, aşa numitele loguri ale tranzacţiilor din sistem),
- înregistrările corespunzătoare evenimentelor (loguri) ce ţin de serviciile de certificare, păstrate de către AlfaTrust Certification,
- rezultatele auditurilor interne şi externe, dacă acestea reprezintă o ameninţare pentru securitatea AlfaTrust Certification,
- planurile în caz de urgenţă,
- informaţiile referitoare la măsurile luate pentru protecţia dispozitivelor hardware şi aplicaţiilor software, informaţiile referitoare la modul de administrare a serviciilor de certificare şi a regulilor de înregistrare planificate.

Obligaţia de confidenţialitate nu se răsfrânge şi asupra faptului că AlfaTrust Certification a oferit servicii de certificare unei părţi. Persoanele responsabile de păstrarea confidenţialităţii informaţiilor şi care se supun regulilor referitoare la modul de gestiune a informaţiilor poartă răspunderea penală conform legislaţiei în vigoare.

2.9. Drepturi de proprietate intelectuală

Toate mărcile, patentele, siglele, licenţele, imaginile grafice etc. folosite de către AlfaTrust Certification S.A. sunt şi vor rămâne proprietatea intelectuală a deţinătorilor legali ai acestora. AlfaTrust Certification S.A. se obligă să specifice acest lucru conform cerinţelor impuse de deţinători.

Toate mărcile, patentele, siglele, licenţele, imaginile grafice etc., aparţinând AlfaTrust Certification S.A. sunt şi rămân proprietatea acesteia, indiferent dacă sunt însoţite sau nu de patente, modele de utilitate, copyright sau altele asemenea şi nu pot fi reproduse sau furnizate unei terţe părţi fără acordul prealabil în scris al AlfaTrust Certification S.A.

Fiecare pereche de chei asociata unui certificat emis de AlfaTrust Certification este proprietatea subiectului acelui certificat, specificat în câmpul *Subject* al certificatului, cu excepţia certificatelor utilizatorilor persoane juridice, caz în care proprietarul este persoană juridică.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

3. Identificare și autentificare

Acest capitol prezintă regulile generale pentru verificarea identităţii Abonatului, reguli care se aplică la emiterea de certificate de către AlfaTrust Certification. Acestea au la bază anumite tipuri de informaţii care sunt incluse în certificate şi specifică mijloacele indispensabile pentru a se asigura că informaţia este precisă şi credibilă la momentul emiterii certificatului.

Verificarea este făcută în mod obligatoriu în etapa de înregistrare şi de modificare a datelor utilizatorului precum şi la cererea AlfaTrust Certification în cazul oricărui alt serviciu de certificare.

3.1. Înregistrarea inițială

Înregistrarea utilizatorului final are loc atunci când un utilizator care cere înregistrarea nu deţine un certificat valid emis de nici o Autoritate de Certificare afiliată la AlfaTrust Certification.

Înregistrarea presupune un număr de proceduri care permit unei Autorităţi de Înregistrare – înainte de a emite un certificat către un utilizator – să adune date valide cu privire la o anumită entitate pentru identificarea acesteia.

Fiecare utilizator este supus unui proces de înregistrare o singură dată. După verificarea datelor puse la dispoziţie de un utilizator, acesta este inclus pe lista utilizatorilor autorizaţi ai serviciilor AlfaTrust Certification şi i se acordă un certificat de cheie publică.

Fiecare utilizator care solicită servicii specifice infrastructurilor de chei publice şi care cere emiterea unui certificat trebuie (înainte de emiterea certificatului) să:

- completeze un formular de înregistrare disponibil on-line, sau ca document ce poate fi downloadat de pe site-ul Web al AlfaTrust Certification (www.AlfaSign.ro),
- genereze o pereche de chei asimetrice RSA şi să furnizeze Autorităţii de Înregistrare dovada deţinerii unei chei private; opţional, utilizatorul poate să însărcineze o Autoritate de Certificare sau Autoritatea de Înregistrare cu generarea acestei perechi de chei,
- sugereze un nume distinctiv (ND, vezi Capitolul 3.1.1),
- completeze şi să trimită un formular de înregistrare care conţine o cheie publică şi dovada posesiei cheii private corespunzătoare acesteia,
- să se prezinte, opţional, la Autoritatea de Înregistrare şi să furnizeze documentele necesare (dacă se cere acest lucru de politica de certificare pe baza căreia se emite certificatul),
- încheie un contract cu un funcționar al Autorităţii de Înregistrare în legătură cu furnizarea serviciilor de către AlfaTrust Certification; prezentul Cod de Practici şi Proceduri este parte integrantă a acestui contract.

Procedura de înregistrare poate solicita utilizatorului, sau unui reprezentant autorizat al acestuia, să contacteze personal Autoritatea de Înregistrare. Cu toate acestea, AlfaTrust Certification permite trimiterea cererilor de înregistrare prin poştă, e-mail, site-uri Web etc.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

3.1.1. Tipuri de nume

Certificatele emise de AlfaTrust Certification respectă standardul X.509 v3. Aceasta înseamnă că emitentul de certificate şi Autoritatea de Înregistrare care acţionează în numele emitentului aprobă numele utilizatorului, conform standardului X.509 (cu referire la recomandările seriei X.500). Numele de bază ale utilizatorilor şi ale emitenţilor de certificate plasaţi în certificatele AlfaTrust Certification sunt în concordanţă cu Numele Distinctive – ND – (cunoscute şi ca nume directoare), create respectând recomandările X.500 şi X.520. În cadrul ND, este posibilă definirea de atribute ale Domain Name Service (DNS). Aceasta permite utilizatorilor să folosească două tipuri de nume: ND şi DNS simultan. Această opţiune este foarte importantă în cazul emiterii de certificate către servere sub administrarea utilizatorului.

Pentru a asigura o comunicare electronica facilă cu utilizatorul, în certificatele AlfaTrust Certification este folosit un nume suplimentar pentru utilizator. Acest nume poate de asemenea să conţină adresa de e-mail a utilizatorului, în concordanţă cu recomandările RFC 822.

Numele directoarelor unde sunt reţinute certificatele, CRL-urile şi Politica de Certificare, ca şi numele punctelor de distribuţie ale CRL-urilor respectă prevederile protocolului LDAP referitoare la sintaxa numelui (vezi RFC 1778).

3.1.2. Necesitatea ca numele să aibă sens

Numele incluse în Numele Distinctiv al utilizatorului trebuie să aibă un sens în limba română sau în altă limbă care utilizează alfabet latin. Structura Numelui Distinctiv, aprobat / atribuit şi verificat de o Autoritate de Înregistrare, depinde de tipul utilizatorului.

Pentru entităţi private (persoane fizice sau angajaţi ai companiilor), ND constă din următoarele câmpuri, obligatorii sau nu (descrierea câmpului este urmată de abrevierea sa care respectă recomandările RFC 3280 şi X.520):

- **câmpul C** – abrevierea internaţională pentru numele ţării (RO pentru România),
- **câmpul S** – judeţul / sectorul în care locuieşte utilizatorul,
- **câmpul L** – oraşul în care utilizatorul are domiciliul,
- **câmpul Street** – adresa utilizatorului,
- **câmpul CN** – numele utilizatorului; numele unui produs sau echipament poate de asemenea să fie specificat aici,
- **câmpul O** – numele instituţiei în cadrul căreia lucrează utilizatorul, în cazul în care certificatul este emis către o persoană juridică,
- **câmpul OU** – numele departamentului în care este angajat utilizatorul, în cazul în care certificatul este emis către o persoană juridică,
- **câmpul T** – funcţia utilizatorului,
- **câmpul SN** – numele de familie al utilizatorului,
- **câmpul G** – prenumele utilizatorului,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- **câmpul P** – pseudonimul utilizatorului pe care acesta îl foloseşte în mediul său, sau pe care doreşte să îl folosească pentru a nu-şi face public numele sau prenumele real,
- **câmpul Phone** – numărul de telefon,
- **câmpul Serial Number** – codul personal de identificare al utilizatorului în sensul Legii 455/201 a semnaturii electronice.

Pentru persoanele juridice, ND constă în următoarele câmpuri opţionale (descrierea câmpului este urmată de abrevierea sa care respectă recomandările X.520):

- **câmpul C** – abrevierea internaţională pentru numele ţării (RO pentru România),
- **câmpul O** – numele instituţiei,
- **câmpul OU** – numele departamentului organizaţiei,
- **câmpul S** – judeţul / sectorul în care funcţionează organizaţia,
- **câmpul L** – oraşul în care utilizatorul locuieşte sau are domiciliu,
- **câmpul CN** – numele instituţiei,
- **câmpul Phone** – numărul de telefon,

Numele utilizatorului trebuie confirmat de un operator al Autorităţii de Înregistrare şi aprobat de o Autoritate de Certificare. AlfaTrust Certification asigură (în cadrul domeniului său) unicitatea ND-urilor.

3.1.3. Unicitatea numelor

Interpretarea câmpurilor din certificatele emise de AlfaTrust Certification se face în concordanţă cu profilele de certificate descrise în Profilul certificatelor şi al CRL-urilor (Capitolul 6). În crearea şi interpretarea ND-ului se face apel la recomandările specificate în subcapitolul 3.1.2.

Identificarea fiecărui deţinător de certificate emise de AlfaTrust Certification se realizează pe baza ND-ului. AlfaTrust Certification asigură unicitatea ND-ului asignat fiecărui utilizator.

ND-ul utilizatorului este sugerat de acesta în cererea sa. Dacă numele este în concordanţă cu cerinţele generale specificate în subcapitolul 3.1.1 şi 3.1.2, un operator al Autorităţii de Înregistrare acceptă temporar sugestia. Dacă operatorul Autorităţii de Înregistrare are acces la baza de date cu ND-uri, acesta va verifica şi unicitatea numelui în domeniul AlfaTrust Certification. Dacă testul confirmă unicitatea, ND-ul este acceptat. În cazul lipsei accesului la baza de date a AlfaTrust Certification, decizia cu privire la acceptarea sau refuzul ND-ului se ia de către operatorul Autorităţii de Certificare.

Dacă un ND sugerat de utilizator încalcă drepturile altor entităţi la acest nume (vezi subcapitolul 3.1.4), AlfaTrust Certification poate adăuga alte atribute ND-ului (ex. numărul serial), care asigură unicitatea acestui nume în cadrul domeniului AlfaTrust Certification. Un utilizator este îndreptăţit să refuze un ND sugerat în procedura specificată în subcapitolul 4.2.5.

Formatul numelui unic global pentru un utilizator are următoarea formă:

AlfaSign.ro / numele emitentului / numele utilizatorului

în care AlfaSign.ro este numele domeniului AlfaTrust Certification, numele emitentului este ND-ul uneia din Autorităţile de Certificare şi numele utilizatorului este ND-ul câmpului *Subject* din certificat.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Valorile ultimelor două câmpuri sunt extrase din certificat.

Dacă un utilizator renunţă la serviciile AlfaTrust Certification, eventuala cererea de atribuire a ND-ului său altui utilizator va fi respinsă.

AlfaTrust Certification poate înregistra un utilizator cu un Nume Distinctiv folosit în trecut de alt utilizator numai cu acordul scris al acestuia din urmă.

3.1.4. Procedura aplicabilă în litigiile referitoare la dreptul la nume

Numele care nu aparţin unui utilizator nu pot fi folosite în cererile sale de certificat. AlfaTrust Certification nu verifică dacă un utilizator este îndreptăţit să folosească numele menţionat în cererea de înregistrare şi nici nu intenţionează să-şi asume rolul de arbitru în rezolvarea disputelor privind drepturile de proprietate asupra oricărui Nume Distinctiv, marcă comercială sau nume comercial.

În disputele privind revendicările de nume, AlfaTrust Certification este îndreptăţită să respingă sau să suspende cererea unui utilizator fără a-şi asuma vreo responsabilitate în acest sens. AlfaTrust Certification este de asemenea îndreptăţită să ia toate deciziile cu privire la sintaxa numelui unui utilizator şi să atribuie unui utilizator numele care rezultă ca urmare a acestor decizii.

3.1.5. Metode de a dovedi posesia cheii private

Dacă o entitate deţine o cheie privată când cere emiterea unui certificat, Autorităţile de Certificare şi Autoritatea de Înregistrare care funcţionează în cadrul AlfaTrust Certification se vor asigura că entitatea deţine o cheie privată corespunzătoare cheii publice furnizate.

Verificarea posesiei cheii private se face pe baza aşa numitei dovezi de posesie (DP) a cheii private. Această dovadă reprezintă confirmarea că o cheie publică supusă procedurilor de certificare este perechea unei chei private deţinută în mod exclusiv de utilizator.

Forma dovezii depinde de tipul perechii de chei ce va fi certificată (pereche de chei pentru crearea unei semnaturi electronice, pentru semnare de cod sau pentru negocierea de cheie).

Dovada de bază se realizează prin mecanisme criptografice (semnatura electronica şi / sau criptare), aplicate în procesul de înregistrare şi modificare a datelor şi, periodic, pe cererea de reînnoire a cheii / certificatului.

Cerinţa de prezentare a dovezii de posesie a cheii private nu se aplică dacă, la cererea utilizatorului, perechea de chei este generată de Autoritatea de Certificare sau de către Autoritatea de Înregistrare.

Cheile private se recomandă a fi generate în interiorul unui dispozitiv criptografic (token) sau, în cazul generării lor în afara token-ului, prin intermediul unui generator software sau hardware urmând ca apoi să fie importate pe token. Orice entitate poate deţine un token la momentul generării şi importului cheii, sau token-ul poate fi furnizat entităţii după procesul de generare de cheie. În ultimul caz, AlfaTrust Certification garantează că token-ul şi cheia vor ajunge în mod sigur, direct la entitatea respectivă (vezi subapitolul 5.1.1.1.2).

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

3.1.6. Autentificarea identității persoanelor juridice

Autentificarea identităţii unei persoane juridice se realizeaza pentru a dovedi că, la momentul procesării cererii, persoana juridică stipulată în cerere există; de asemenea, este necesar sa se dovedeasca că o persoană fizică solicitantă a unui certificat in numele societatii, sau care-l primeşte este autorizată de către această persoană juridică să o reprezinte.

Procedurile de autentificare a identităţii persoanelor juridice sunt iniţiate dacă entitatea:

- se comportă ca un utilizator şi însărcinează o Autoritate de Certificare cu orice serviciu de certificare,
- cere emiterea unui certificat pentru un dispozitiv hardware sau pentru o aplicaţie (software) deţinută de această entitate,
- se comportă ca o entitate care cere includerea sa în lista Autorităţilor de Certificare din subordinea AlfaTrust Certification,
- doreşte să presteze alte servicii de certificare, cum ar fi: Autoritate de Marcă Temporala, OCSP etc.

Autentificarea identităţii unei persoane juridice se poate face fie prin prezenţa personală a reprezentantului autorizat al persoanei juridice la Autoritatea de Înregistrare, fie prin prezenţa în persoană a reprezentantului autorizat al Autorităţii de Înregistrare la sediul persoanei juridice (specificat în cerere).

Reprezentanţii autorizaţi ai instituţiei, indiferent de nivelul certificatului pe care îl cer, sunt obligaţi să prezinte, la cererea unui reprezentant al Autorităţii de Înregistrare, următoarele documente:

* copie certificata „conform cu originalul” dupa certificatul de inmatriculare al societatii;
* copie factura de utilitati (telefonie, altele) emisa pe numele societatii;
* documente care să confirme identitatea solicitantului (cartea de identitate sau paşaportul) şi autorizaţia prin care reprezintă compania;
* cerere de achizitie;
* declaratie tip a titularului de domeniu (in cazul certificatelor WEB, cand solicitantul certificatului nu este proprietarul domeniului ce se doreste a fi securizat).

Procedura de verificare la AÎ a identităţii persoanei juridice şi a identităţii reprezentantului său autorizat constă în:

* verificarea documentelor furnizate de utilizator,
* verificarea cererii, care constă în:
    i. verificarea conformităţii datelor menţionate în cerere cu cele din documentele furnizate,
    ii. (opţional) verificarea dovezii posesiei cheii private (dacă cererea implică o pereche de chei pentru crearea unei semnaturi electronice) şi măsura în care Numele Distinctiv este cel potrivit,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- verificarea autorizaţiei şi identităţii reprezentantului persoanei juridice care trimite cererea (inclusiv cereri de acreditare ca Autoritate de Certificare) în numele acestei entităţi,
- verificarea in serviciul whois operat de ROTLD (www.rotld.ro) a faptului ca proprietarul domeniului este chiar cel care face solicitarea de certificat SSL, sau cel care a dat autorizatia de utilizare a domeniului solicitantului,
- verificarea contului de mail care apare in cererea de certificat este controlat de catre abonat. Cererea de certificat nu poate fi facuta/validata in aplicatia software AÎ daca abonatul nu isi valideaza contul de email.

Autoritatea de Înregistrare se angajează să verifice corectitudinea şi autenticitatea tuturor datelor furnizate în cererea de certificat.

Dacă verificările sunt încheiate cu succes, un operator autorizat al Autorităţii de Înregistrare:

- atribuie un nume distinctiv persoanei juridice sau aprobă numele sugerat de aceasta prin înaintarea cererii,
- emite o confirmare prin care atestă conformitatea datelor din cererea în curs de procesare cu datele prezentate şi trimite această confirmare la Autoritatea de Certificare,
- face copii tuturor documentelor şi certificatelor folosite de operator pentru verificarea identităţii persoanei juridice şi identitatea reprezentantului său care acţionează în numele acesteia,
- în numele Autorităţii de Certificare, încheie un contract cu persoana juridică cu privire la prestarea serviciilor de certificare; contractul se încheie dacă persoana juridică joacă rolul de utilizator, de Autoritate de Certificare, sau o entitate care prestează alte servicii de certificare.

Confirmarea este trimisă Autorităţii de Certificare care verifică dacă aceasta a fost emisă de o Autoritate de Înregistrare autorizată.

Procesul de autentificare este înregistrat. Tipul informaţiilor înregistrate şi acţiunile depind de nivelul de încredere al certificatului ce face obiectul cererii şi privesc:

- identitatea operatorului Autorităţii de Înregistrare care verifică identitatea solicitantului,
- trimiterea declaraţiei operatorului (semnată de mână) prin care se atestă faptul că acesta a verificat identitatea solicitantului în concordanţă cu cerinţele prezentului Cod de Practici şi Proceduri,
- data verificării,
- identificatorul operatorului şi al solicitantului în cazul în care acesta din urmă este prezent în persoană la Autoritatea de Înregistrare (presupunând că solicitantului i s-a atribuit un astfel de identificator),
- declaraţia solicitantului (semnată de mână) cu privire la corectitudinea datelor incluse în cerere, în concordanţă cu cerinţele prezentului Cod de Practici şi Proceduri,

AlfaTrust Certification respinge cererea de înregistrare a unui solicitant dacă descoperă că persoana juridică în cauză este deja înregistrată.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

3.1.7. Autentificarea identității persoanelor fizice

Autentificarea identităţii persoanelor fizice (entităţi private) are două scopuri. Autentificarea trebuie să dovedească

1) că datele dintr-o cerere se referă la o entitate privată existentă

şi

2) că solicitantul este într-adevăr entitatea privată menţionată în cerere.

Autentificarea persoanelor fizice se realizează pe baza documentelor personale (carte de identitate sau paşaport) care confirmă identitatea solicitantului, şi dacă utilizatorul doreşte să includă datele unei instituţii (persoană juridică) pentru care lucrează:

a) autorizaţia scrisă, cu aprobarea explicită a companiei privind includerea datelor sale în certificatul persoanei fizice,

b) extrasul valid de la Registrul Comerţului din România,

c) alte documente.

Procedura pentru persoanele fizice realizată în faţa Autorităţii de Înregistrare constă în:

* verificarea documentelor furnizate de utilizator (carte de identitate sau paşaport in original sau copie legalizata), inclusiv bazele de date ale AC sau ale altor instituţii,
* verificare cererii înaintate:
    - verificarea consecvenţei datelor din cerere cu cele din documente,
    - (opţional) verificarea dovezii posesiei unei chei private şi a gradului de potrivire a ND-ului.
* verificarea setului de informaţii din cerere folosind alte surse (Registrul Comerţului din România, Registrul de Evidenţă a Populaţiei etc.),
* verificarea faptului ca contul de mail care apare in cererea de certificat este controlat de catre abonat. Cererea de certificat nu poate fi facuta/validata in aplicatia software AÎ daca abonatul nu isi valideaza contul de email.

3.1.8. Autentificarea dispozitivelor

În multe cazuri, un certificat de cheie publică este emis pentru dispozitive fizice (hardware), cum ar fi un router, un firewall, sau un server. În aceste cazuri se consideră că fiecare dispozitiv este proprietatea unei persoane fizice sau juridice (are un sponsor). Sponsorul este responsabil de trimiterea datelor asociate dispozitivului:

- identificatorul dispozitivului,
- cheia publică a dispozitivului,
- caracteristicile şi autorizaţiile dispozitivului (în cazul în care acestea trebuie specificate în certificat),

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- datele de contact ale sponsorului, care să permită Autorităţii de Înregistrare sau FSC-ului să contacteze rapid sponsorul.

Verificarea informaţiilor care se înregistrează depinde de nivelul de încredere al certificatului. Sunt două metode de autentificare a originii unui dispozitiv şi a integrităţii datelor furnizate:

- verificarea cererii semnate electronic trimise de un sponsor (cererea trebuie semnată cu o cheie privată asociată cu un certificat cu un nivel de încredere egal sau mai mare decât al certificatului solicitat),
- în timpul înregistrării personale de către sponsor a unui dispozitiv; identitatea sponsorului este confirmată în concordanţă cu cerinţele stipulate în Capitolul 3.1.7.

3.2. Autentificarea identităţii la reînnoirea sau modificarea certificatului

Pentru a păstra continuitatea certificatului, înainte de expirarea sa, utilizatorul trebuie să solicite un nou certificat. Noul certificat poate conţine aceeaşi cheie (reînnoire) dacă se respectă condiția ca durata de viaţă a cheilor să nu depăşească o durată de două ori mai mare decât durata maximă de viaţă a unui certificat. In caz contrar se va emite un nou certificat.

Reînnoirea este permisă numai înainte de expirarea certificatului. Ea se poate face cu maxim 30 de zile înainte de expirare şi numai o singură dată.

Identitatea utilizatorilor care cer reînnoirea certificatului, sau modificarea acestuia este verificată. Procedurile utilizate urmăresc verificarea faptului că persoana sau organizaţia care cer un nou certificat pentru un utilizator, sunt îndreptăţite la acest lucru.

Utilizatorii care trimit cereri direct la o Autoritate de Înregistrare vor fi verificati de această autoritate pe baza semnăturii electronice şi a certificatului cheii publice asociat cu această semnatură.

3.2.1. Reînnoirea unui certificat

Un utilizator sau o Autoritate de Certificare foloseşte reînnoirea dacă deţine deja un certificat şi o cheie privată asociată acestuia şi doreşte să continue să folosească aceeaşi pereche de chei. Noul certificat, creat ca rezultat al înnoirii, constă în aceeaşi cheie publică, acelaşi nume şi restul informaţiilor care se preiau din certificatul anterior, dar perioada de valabilitate, numărul serial şi semnatura emitentului sunt diferite faţă de datele din certificatul anterior.

Reînnoirea se aplică numai certificatelor a căror perioadă de validitate nu a expirat, nu au fost revocate şi informaţiile conţinute de acestea sunt intacte.

Fiecare cerere de reînnoire este procesată în mod off-line, adică necesită acceptarea manuală a operatorului Autorităţii de Certificare.

3.2.2. Modificarea unui certificat

Modificarea certificatului se referă la crearea unui nou certificat pe baza certificatului deţinut în prezent de utilizator. Un nou certificat are o cheie publică diferită, un nou număr serial, dar diferă prin cel puţin un

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

câmp (prin conţinut sau prin apariţia unui câmp complet nou) faţă de certificatul pe baza căruia este emis. Modificarea poate fi necesară, de exemplu, în cazul schimbării poziţiei în cadrul companiei sau al schimbării numelui, cu condiţia ca aceste date să fi fost menţionate iniţial în certificat, sau dacă trebuie adăugate. Dacă datele, verificate pe baza unor documente în concordanţă cu procedurile de autentificare ale utilizatorului au fost modificate, fiecare cerere trebuie confirmată de Autoritatea de Înregistrare. Pot fi modificate numai certificatele valide care nu au fost revocate şi al căror nume al utilizatorului şi alte caracteristici nu au fost schimbate.

3.3. Autentificarea identităţii la revocarea unui certificat

Cererile de revocare pot fi trimise prin e-mail direct emitentului certificatului sau indirect, Autorităţii de Înregistrare. Se pot trimite cereri şi în alt format decât cel electronic.

* în primul caz, utilizatorul trebuie să trimită o cerere autentificată pentru revocarea certificatului. Utilizatorul autentifică cererea aplicându-i o semnatura electronica.
* Utilizatorul care a pierdut o cheie privată activă (sau i-a fost furată) trebuie să folosească a doua metodă. Cererea de revocare trebuie să fie certificată de Autoritatea de Înregistrare.

În ambele cazuri, trebuie să existe o identificare fără echivoc a identităţii utilizatorului. Cererea de revocare poate să vizeze mai multe certificate. Autentificarea şi identificarea utilizatorului la Autoritatea de Înregistrare se realizează ca şi la înregistrarea iniţială (vezi Capitolul 3.1).

Autentificarea utilizatorului la Autoritatea de Certificare constă în verificarea autenticităţii cererii. Procedura detaliată de revocare este descrisă în subcapitolul 4.3.

4. Cerințe operaționale

În acest capitol sunt prezentate procedurile ce țin de procesul de certificare. Fiecare procedură începe cu trimiterea, de către utilizatorul final, a unei cereri: ***indirect*** (după confirmarea inițială a cererii de către Autoritatea de Înregistrare) sau ***direct*** către o Autoritate de Certificare. Pe baza cererii, Autoritatea de Certificare ia o decizie în legătură cu furnizarea / respingerea serviciului cerut.

Cererile trimise trebuie să conţină informaţiile necesare pentru identificarea corectă a utilizatorului.

AlfaTrust Certification oferă acces la următoarele servicii de bază:

i. înregistrarea, certificarea, reînnoirea, modificarea de certificate;

ii. revocarea certificatelor;

iii. verificarea valabilităţii certificatelor.

Programul de lucru

Serviciile sunt oferite atât on-line, cât şi la sediul firmei. Serviciile online sunt oferite permanent, iar cele de la sediul firmei, de luni până vineri, între orele 10 şi 16. Pentru toate clasele de certificate serviciile de revocare a certificatelor sunt oferite în maxim 24 de ore de la solicitare.

Dacă cererea trimisă conţine o cheie publică, cheia trebuie pregătită în aşa fel încât să lege criptografic cheia publică cu alte date stipulate în cerere, în special cu datele de identificare ale utilizatorului. O cerere poate conţine, în loc de o cheie publică, solicitarea utilizatorului final de a genera o cheie asimetrică în

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

numele său. Aceasta poate fi îndeplinită de către Autoritatea de Înregistrare. În urma generării, cheile sunt trimise pe o cale sigură către utilizatorul final, astfel încât cheile să nu poată fi activate de către o persoană neautorizată.

4.1. Trimiterea cererii

Cererile pentru eliberarea unui certificat sunt trimise de utilizator către Autoritatea de Înregistrare. Cererile sunt trimise prin protocoale de comunicaţie precum HTTP, S/MIME sau TCP/IP. AlfaTrust Certification emite certificate numai pe baza cererilor de înregistrare, modificare sau reînnoire de certificate trimise de un utilizator final.

Cererile pot fi trimise de diferite entităţi şi pot viza certificate a căror aplicabilitate depinde de nevoile entităţii:

* certificate pentru persoane fizice – emise ca urmare a înaintării unei cereri,
* certificate pentru persoane fizice – emise ca urmare a înaintării unei cereri când o Autoritate de Certificare sau Autoritatea de Înregistrare generează perechea de chei şi un certificat şi, folosind un dispozitiv criptografic (token), le trimite unei persoane fizice,
* certificate pentru persoane fizice – emise ca urmare a înaintării unei cereri de către un reprezentant în numele persoanei fizice,
* certificate pentru persoane fizice – emise ca urmare a înaintării unei cereri de către reprezentanţi sau angajaţi ai organizaţiei care deleagă acestora autorizarea respectivă,
* certificate pentru dispozitive (care se aplică, de exemplu, serverelor) sau certificate ale aplicaţiilor deţinute de persoane fizice (angajaţi ai organizaţiei sau reprezentanți ai lor) autorizate să folosească acest dispozitiv sau aplicaţie.

4.1.1. Cererea de înregistrare

O cerere de înregistrare este trimisă de către un utilizator final către Autoritatea de Înregistrare şi conţine cel puţin următoarele informaţii:

i. numele complet al instituţiei sau numele şi prenumele utilizatorului final,
ii. numele distinctiv a cărui structură depinde de categoria utilizatorului final (vezi Capitolul 3.1.2),
iii. identificatori: Codul de Înregistrare al Firmei / Codul Numeric Personal
iv. adresa utilizatorului final,
v. tipul de certificat cerut,
vi. identificatorul politicii de certificare pe baza căruia este emis certificatul,
vii. adresa de e-mail,
viii. cheia publică care va fi certificată.

Ca urmare a autentificării identităţii utilizatorului final (vezi Capitolele 3.1.8 şi 3.1.9) şi după primirea confirmării Autorităţii de Înregistrare, cererea este trimisă unei Autorităţi de Certificare.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

4.1.2. Cererea de reînnoire sau modificare certificat

O cerere de modificare sau reînnoire certificat, trebuie să conţină cel puţin:

i. numele distinctiv al solicitantului (utilizatorului final);

ii. tipul de certificat pe care-l solicită utilizatorul;

iii. identificatorul politicii de certificare pe baza căreia trebuie emis certificatul;

iv. cheia publică (folosită anterior în cazul înnoirii certificatului sau nouă în cazul schimbării de cheie de certificat) care va fi certificată.

4.1.3. Cererea de revocare a unui certificat

Informaţiile incluse în cererea de revocare a unui certificat sunt următoarele:

i. numele distinctiv al solicitantului (utilizatorului final),

ii. lista de certificate de revocat sau suspendat, sub forma unei perechi: numărul serial, motivul revocării.

Datele parţiale sau complete incluse în cererea de mai sus trebuie autentificate prin semnatura electronica, dacă utilizatorul deţine o cheie privată validă pentru crearea de semnatura.

O cerere de revocare poate fi trimisă prin e-mail împreună cu datele de autentificare, sub formă scrisă (scrisoare, fax), sau sub formă orală (telefon). În ultimele două cazuri, certificatul este suspendat până când cererea va fi trimisă electronic.

În momentul suspendării certificatului, operatorii Autorităţii de Înregistrare anunță utilizatorul final în legătură cu acest lucru.

4.2. Tratarea cererilor de certificare

AlfaTrust Certification acceptă cereri înaintate individual sau colectiv. Cererile pot fi trimise on-line şi offline.

Cererea trimisă on-line se realizează prin intermediul paginilor web de pe serverul AlfaTrust Certification la adresa: https://www.AlfaSign.ro. Un utilizator care intră pe site-ul respectiv completează (conform instrucţiunilor de pe site) un formular de cerere şi îl trimite Autorității de Înregistrare a FSC-ului. Cererile pentru certificate simple (necalificate) sunt procesate automat, în timp ce cererile de certificate calificate sunt procesate manual.

Cererea trimisă off-line se poate face:

* Prin prezentarea în persoană a solicitantului sau a reprezentantului autorizat al companiei la Autoritatea de Înregistrare a Furnizorului de Servicii de Certificare (FSC), caz în care se completează şi se semnează de mână cererea, se semnează contractul cu privire la prestarea serviciilor de certificare şi se generează o parola cu ajutorul căreia utilizatorul va putea face managementul certificatului sau se generează un cod PIN pentru accesul securizat la dispozitivul criptografic ce conţine cheile şi certificatele,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

* Prin trimiterea prin poştă a cererii şi a copiilor documentelor (conform subcapitolelor 3.1.6 şi 3.1.7) necesare verificării identităţii solicitantului; verificarea este urmată de generarea unei parole cu ajutorul căreia utilizatorul va putea face managementul certificatului, sau generarea unui cod PIN pentru accesul securizat la dispozitivul criptografic ce conţine cheile şi certificatele; dispozitivul criptografic este trimis înapoi solicitantului (codul PIN este trimis separat).

Trimiterile off-line privesc de asemenea cererile colective. Aceste cereri sunt confirmate de către un operator al Autorităţii de Înregistrare şi procesate în grup.

4.2.1. La Autoritatea de Înregistrare (AÎ)

Fiecare cerere scrisă pe hârtie este procesată după cum urmează:

1. operatorul Autorităţii de Înregistrare primeşte cererea solicitantului,
2. operatorul verifică datele din cerere, cum ar fi datele personale ale solicitantului (vezi subcapitolele 3.1.6 și 3.1.7) şi verifică existenţa dovezii posesiei cheii private (vezi subcapitolul 3.1.5),
3. ca urmare a verificării, operatorul confirmă identitatea dintre datele declarate şi cele cuprinse în cerere; dacă cererea conţine date neconforme este respinsă,
4. cererea confirmată este trimisă la Autoritatea de Certificare,
5. Autoritatea de Înregistrarea mai verifică şi alte date care nu sunt specificate în cerere dar sunt necesare pentru emiterea certificatului.

4.2.2. La Autoritatea de Certificare (AC)

Autoritatea de Certificare verifică faptul că cererile au fost confirmate de către Autoritatea de Înregistrare a Furnizorului de Servicii de Certificare (FSC).

4.2.3. Emiterea certificatelor

După primirea şi procesarea unei cereri (vezi capitolele 4.1 şi 4.2), Autoritatea de Certificare emite un certificat. Un certificat este considerat valid (în stare activă sau pregătit) în momentul acceptării lui de către utilizatorul final (vezi subcapitolul 4.2.5). Perioada de valabilitate a certificatelor emise depinde de tipul de certificat şi de categoria utilizatorului final şi sunt în conformitate cu perioadele prezentate în subcapitolul 5.1.1.3.2.

Fiecare certificat este emis on-line. Procedura de emitere este următoarea:

* cererea procesată este trimisă serverului de emitere de certificate,
* dacă cererea conţine solicitarea generării unei perechi de chei, serverul cere generatorului hardware de chei acest lucru,
* se testează calitatea cheilor publice generate sau emise de Autoritatea de Certificare,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- dacă procedurile sunt încheiate cu succes, serverul emite un certificat şi însărcinează modulul hardware de securitate cu semnarea certificatului; certificatul este stocat în baza de date a Autorităţii de Certificare,
- Autoritatea de Certificare pregăteşte răspunsul conţinând certificatul emis (dacă a fost emis) şi îl trimite utilizatorului; certificatul nu este publicat în depozitul de la nivelul Autorității de Validare până la primirea confirmării din partea utilizatorului final cu privire la acceptarea certificatului.

Autoritatea de Certificare AlfaTrust Certification foloseşte două metode de bază pentru anunţarea unui utilizator final despre emiterea unui certificat:

- prima metodă presupune folosirea poştei sau a poştei electronice şi constă în trimiterea (la adresa furnizată de utilizator) a informaţiilor ce permit utilizatorului să-şi ridice certificatul. Această metodă este folosită şi când este necesară anunţarea tuturor utilizatorilor finali ai unei anumite Autorităţi de Certificare despre emiterea unui nou certificat pentru autoritatea respectivă;
- A doua metodă constă în emiterea unui certificat şi plasarea acestuia (de obicei împreună cu o cheie privată) pe un dispozitiv criptografic şi trimiterea certificatului (prin poştă) la adresa utilizatorului final (un cod PIN este trimis separat).

Fiecare certificat emis este publicat în depozitul AlfaTrust Certification operat la nivelul Autorității de Validare. Publicarea certificatului este echivalentă cu notificarea altor Entităţi Partenere despre faptul că un certificat a fost emis pentru un utilizator. AlfaTrust Certification publică un certificat în depozit după acceptarea certificatului de către utilizatorul final.

Perioadele de timp pentru emiterea certificatelor depind în primul rând de acurateţea datelor trimise în cerere şi de modul de cooperare dintre AlfaTrust Certification şi solicitant, precum și de modul cum s-a făcut cererea – individual sau în grup, dar această perioadă nu va fi mai mare de 5 zile lucrătoare.

În cazul în care datele necesare nu sunt puse la dispoziţia Autorităţii de Înregistrare în termen, sau este necesară o completare a documentaţiei, termenul de emitere a certificatului va fi prelungit.

4.2.4. Respingerea cererii de certificat

AlfaTrust Certification poate refuza în condiții bine precizate emiterea unui certificat oricărui solicitant fără a-şi asuma vreo obligaţie sau responsabilitate pentru posibilele daune sau pierderi pe care le poate suferi solicitantul ca urmare a acestui refuz. Autoritatea de Înregistrare va restitui solicitantului taxa de certificat (dacă acesta a plătit-o), cu excepţia cazului în care solicitantul a menţionat date false în cererea sa.

Refuzul emiterii de certificat poate surveni în următoarele situaţii:

- dacă identificatorul solicitantului (ND) coincide cu identificatorul altui utilizator,
- dacă există suspiciune sau certitudine cu privire la falsificarea sau folosirea unor date false de către solicitant,
- dacă solicitantul, într-o manieră de natură să producă prejudicii, angajează resurse şi mijloace de procesare ale AlfaTrust Certification prin trimiterea unui număr de cereri în mod clar mai mare decât nevoile pe care le are acesta,
- din alte motive decât cele de mai sus, cu condiția ca acestea să fie argumentate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Informaţiile privind decizia refuzului de emitere de certificat şi motivele acesteia sunt trimise solicitantului. Solicitantul poate cere din nou emiterea unui certificat numai după ce motivele care au dus la refuzul emiterii au fost închise sau soluționate.

4.2.5. Acceptarea certificatelor

La primirea unui certificat, utilizatorul se angajează să verifice conţinutul acestuia, în special corectitudinea datelor şi complementaritatea cheii publice cu cea privată pe care o deţine. Dacă certificatul are nereguli sau greşeli ce nu pot fi acceptate de utilizator, acesta din urmă va sesiza imediat Autoritatea de Înregistrare a Furnizorului de Servicii de Certificare, în vederea revocării certificatului.

Certificatul este considerat acceptat în ipoteza apariţiei unuia dintre următoarele evenimente în termen de maxim 7 zile calendaristice de la data primirii certificatului de către utilizator:

- acceptarea explicită a certificatului emis, la momentul ridicării certificatului de pe site-ul AlfaTrust Certification,
- primirea unui pachet înregistrat (trimis de AlfaTrust Certification) conţinând certificatul.

Dacă un certificat nu este respins în 7 zile calendaristice de la data primirii sale, certificatul este considerat acceptat.

Fiecare certificat acceptat este publicat în depozitul Autorității de Validare şi este accesibil publicului. Acceptarea certificatului este o decizie unilaterală a solicitantului, anterior utilizării lui în efectuarea oricărei operaţii criptografice, prin care se consideră că a acceptat termenii şi condiţiile stipulate în prezentul Cod de Practici şi Proceduri, Politica de Certificare şi Contractul de prestări servicii de certificare. În cazul trimiterii electronice a cererii, solicitantul acceptă în mod automat certificatul la momentul cererii acestui certificat.

Prin acceptarea certificatului, utilizatorul final acceptă regulile Codului de Practici şi Proceduri şi a Politicii de Certificare şi subscrie să respecte prevederile contractul încheiat cu AlfaTrust Certification S.A.

4.2.6. Folosirea certificatelor și a cheilor

Abonaţii trebuie să folosească cheia privată şi certificatele:

- în concordanţă cu scopul lor declarat în prezentul Cod de Practici şi Proceduri şi în concordanţă cu conţinutul certificatului (câmpurile *keyUsage* şi *extendedKeyUsage*),
- în concordanţă cu prevederile contractului dintre utilizatorul final şi AlfaTrust Certification S.A.,
- numai în perioada de valabilitate (nu se aplică certificatelor pentru verificarea semnaturii electronice).

Când certificatul este suspendat, până la eventuala sa revocare, utilizatorul nu poate folosi cheia privată pentru crearea unei semnaturi.

Entităţile Partenere, trebuie să folosească cheile publice şi certificatele:

- în concordanţă cu scopul lor declarat în prezentul Cod de Practici şi Proceduri şi în concordanţă cu conţinutul certificatului (câmpurile *keyUsage* şi *extendedKeyUsage*),

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- în concordanţă cu prevederile contractului dintre entitatea parteneră şi AlfaTrust Certification S.A.,
- numai după verificarea stării acestora şi verificarea semnaturii Autorităţii de Certificare care a emis acel certificat.

4.3. Revocarea certificatelor

Revocarea unui certificat are o influenţă semnificativă asupra utilizării acestuia şi asupra obligaţiilor unui utilizator care deţine un astfel de certificat. Imediat după revocarea certificatului unui utilizator final, certificatul trebuie considerat invalid (în stare de revocare). Similar, în cazul certificatului Autorităţii de Certificare – anularea validităţii unui certificat de acest tip semnifică retragerea drepturilor de emitere de certificate pentru proprietarul său şi revocarea tuturor certificatelor emise de aceasta.

Revocarea nu afectează tranzacţiile făcute înainte de revocare şi nici obligaţiile care rezultă din respectarea prezentului Cod de Practici şi Proceduri.

Acest capitol specifică condiţiile necesare pentru ca o Autoritate de Certificare să aibă motive de revocare a certificatului.

Dacă o cheie privată, care corespunde unei chei publice, conţinută într-un certificat revocat, rămâne sub controlul utilizatorului final, după revocare ar trebui stocata în siguranţă, până este distrusă fizic.

4.3.1. Circumstanțele revocării certificatului

Certificatul se revoca atunci când:

* informaţia conţinută de certificat s-a schimbat,
* o cheie privată, asociată unei chei publice, conţinută în certificat sau pe dispozitivul de stocare, a fost compromisă sau există un motiv serios pentru a suspecta ca a putut fi compromisă,
* părţile decid să înceteze contractul încheiat de acestea; în acest caz, revocarea este strict legată de anularea înregistrării utilizatorului final la Autoritatea de Înregistrare a FSC-ului; dacă utilizatorul însuşi nu cere revocarea, Autoritatea de Certificare sau un reprezentant al instituţiei la care este angajat utilizatorul, au dreptul să o facă,
* Abonatul, deţinătorul unei chei publice, cere revocarea,
* poate fi revocat de emitent (Furnizorul de Servicii de Certificare), dacă un utilizator nu respectă Politica de Certificare, Codul de Practici şi Proceduri sau contractul, ori alte documente emise de Furnizorul de Servicii de Certificare,
* Furnizorul de Servicii de Certificare îşi încetează activitatea; în acest caz toate certificatele emise de această Autoritate de Certificare, înainte de expirarea perioadei declarate pentru oprirea serviciilor, trebuie revocate împreună cu certificatul Autorităţii de Certificare,
* Abonatul întârzie sau nu plăteşte contravaloarea serviciile prestate de către Furnizorul de Servicii de Certificare,
* cheia privată sau securitatea unei Autorităţi de Certificare a fost compromisă intr-un mod în care pune în pericol credibilitatea certificatelor,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- Abonatul, angajat al unei organizaţii, nu a returnat dispozitivul criptografic folosit pentru stocarea certificatului şi a cheii private corespunzătoare, la încheierea contractului de muncă,
- în alte cazuri în care utilizatorul final nu se conformează regulilor acestui Cod de Practici şi Proceduri, Politicii de Certificare, sau contractului.

Sintagma “cheie privată compromisă” este folosită în unul din următoarele sensuri:

- accesul neautorizat la cheia privată sau un motiv întemeiat pe baza căruia să se suspecteze că acest acest acces s-a petrecut,
- pierderea cheii private sau apariţia unui motiv de a suspecta o astfel de pierdere,
- furtul cheii private sau apariţia unui motiv de a suspecta un astfel de furt,
- ştergerea accidentală a cheii private.

Cererea de revocare poate fi trimisă (vezi subcapitolul 4.1.3) prin intermediul Autorităţii de Înregistrare (aceasta implică contactarea autorităţii de către utilizator).

Cererea de revocare trebuie să conţină informaţii care să permită autentificarea sigură a utilizatorul final de către Autoritatea de Înregistrare, în concordanţă cu prevederile subcapitolelor 3.1.6 și 3.1.7. Dacă autentificarea identităţii utilizatorul final nu se realizează cu succes, Autoritatea de Înregistrare respinge cererea de revocare şi suspendă certificatul până când cererea de revocare va fi examinată în detaliu.

4.3.2. Cine poate solicita revocarea

Următoarele entităţi pot trimite cereri de revocare a certificatului unui utilizator final:

- utilizatorul însuși, cu condiția să fie proprietarul certificatului,
- un reprezentant autorizat al Furnizorul de Servicii de Certificare,
- un reprezentant al utilizatorul final, de exemplu angajatorul sau; utilizatorul trebuie imediat informat despre acest lucru,
- Autoritatea de Înregistrare poate cere revocarea în numele unui utilizator, sau în nume propriu, dacă are informaţii care justifică revocarea certificatului.

Când partea care cere revocarea certificatului nu este proprietarul certificatului (utilizatorul), Autoritatea de Înregistrare va:

- verifica faptul că respectiva parte are dreptul să emita o astfel de cerere,
- cere o justificare a respectivei cereri,
- trimite o notificare utilizatorul final despre revocare, sau despre iniţierea procesului de revocare.

Fiecare cerere va fi trimisă trimisă:

- direct Autorităţii de Înregistrare sub formă electronică, cu sau fără confirmarea Autorităţii de Înregistrare,
- indirect (prin intermediul unui terț) la sediul Furnizorul de Servicii de Certificare, sub formă ne-electronica (document pe hârtie, fax, telefon etc.).

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

4.3.3. Procedura de revocare

Revocarea certificatului se poate face în următoarele moduri:

i. prin trimiterea unei cereri de revocare în format electronic către o Autoritate de Înregistrare; o astfel de revocare poate fi iniţiată numai la cererea utilizatorul final; această metodă se aplică în situaţiile în care:

   a. Abonatul a pierdut cheia sa privată sau parola ei, sau cheia privată a fost furată sau

   b. cererea de revocare a fost trimisă de reprezentantul utilizatorul final, cu condiţia de a exista suficiente motive pentru a cere o astfel de revocare;

ii. prin trimiterea unei cereri ne-electronice autentificate (document pe hârtie, fax, telefon etc.) către AlfaTrust Certification ; autentificarea unui document pe hârtie (inclusiv faxul) poate fi efectuată la Autoritatea de Înregistrare, de exemplu cu o ştampilă şi o semnatura de mână a unei persoane recunoscute de AlfaTrust Certification; o cerere făcută prin telefon este îndeplinită numai după ce se trimit şi documentele de autentificare a solicitantului; după verificarea cu succes a cererii, Autoritatea de Înregistrare pregăteşte confirmarea electronica a cererii de revocare şi o înaintează Autorităţii de Certificare.

Informaţiile despre certificatele revocate sunt plasate în Lista de Certificate Revocate (vezi subcapitolul 6.2), la nivelul Autorității de Validare AlfaTrust Certification. Autoritatea de Înregistrare notifică entitatea care cere revocarea certificatului despre această revocare, sau despre decizia de a anula cererea, împreună cu motivele anulării.

Fiecare cerere de revocare de certificat trebuie să ofere mijloace de identificare indubitabilă a certificatului de revocat, să conţină motivele pentru care se cere revocarea şi trebuie să fie autentificată.

Procedura de revocare a unui certificat se desfăşoară astfel:

* Autoritatea de Înregistrare, ca urmare a primirii unei cereri de revocare certificat, o verifică; dacă cererea este făcută electronic, Autoritatea de Înregistrare verifică corectitudinea certificatului de revocat şi corectitudinea certificatului ataşat cererii; cererea făcută pe hârtie necesită autorizarea solicitantului; o astfel de confirmare poate fi obţinută prin telefon, fax sau prin prezentarea în persoană a utilizatorul final la un reprezentant autorizat al Autorităţii de Înregistrare (sau invers);

* dacă cererea este verificată cu succes, Autoritatea de Certificare plasează informaţiile despre revocarea certificatului în Lista certificatelor Revocate (CRL), împreună cu informaţii privind motivele de revocare (vezi subcapitolul 6.2.1);

* Autoritatea de Înregistrare notifică, electronic sau prin poştă, entitatea care cere revocarea despre revocare sau decizia de anulare a cererii împreună cu motivele anulării.

* în plus, dacă partea care cere revocarea nu este utilizatorul final, Autoritatea de Înregistrare va notifica utilizatorul în privinţa revocării certificatului, sau iniţierii procesului de revocare.

Dacă un certificat, sau o cheie privată corespunzătoare unui certificat de revocat au fost stocate pe un dispozitiv criptografic, ca urmare a revocării certificatului, dispozitivul criptografic trebuie distrus fizic sau şters în codiţii de maximă securitate. Această operaţie se îndeplineşte de către posesorul dispozitivului criptografic – o persoană fizică sau juridică (un reprezentant al unei astfel de entităţi). Deţinătorul

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

dispozitivului criptografic trebuie să-l păstreze astfel încât să prevină furtul sau utilizarea neautorizată a sa până la distrugerea fizică sau la ştergerea cheii private.

Perioada maximă de revocare a unui certificat, daca s-a realizat cu succes autentificarea solicitantului, este de maxim 24 ore pentru orice tip de certificat.

Informaţiile despre revocarea unui certificat sunt stocate în baza de date a AlfaTrust Certification, iar certificatele revocate sunt plasate în Lista certificatelor Revocate (CRL) în concordanţă cu perioadele de publicare a CRL-urilor.

În momentul revocării certificatului, operatorii Autorităţii de Înregistrare şi utilizatorii implicaţi sunt informaţi automat despre această revocare. Informaţii despre starea curentă a certificatului sunt disponibile prin serviciul de verificare a stării certificatelor imediat după perioada de graţie declarată. Acest serviciu poate fi cerut, de exemplu, de către o Entitate Parteneră, care verifică validitatea unei semnaturi electronice aplicate unui document primit de la utilizatorul final.

4.3.4. Frecvența de emitere a CRL-urilor

Fiecare Autoritate de Certificare care face parte din domeniul AlfaTrust Certification emite diferite Liste de Certificate Revocate. Un nou CRL este publicat în depozit după fiecare revocare de certificat, într-un interval de maxim o zi. Dacă motivul revocării este compromiterea cheii, noul CRL este emis imediat după procesarea cererii de revocare. Perioada de valabilitate a CRL-ului este de 48 de ore si se actualizeaza zilnic.

Lista de certificate Revocate (CRL) pentru autoritatea AlfaTrust Certification ROOT CA este emisă cel puţin în fiecare an cu condiţia să nu existe nici o revocare de certificat a uneia dintre autorităţile direct subordonate.

În cazul revocării certificatului unei autorităţi afiliate la AlfaTrust Certification, acest certificat este imediat publicat în Lista de certificate Revocate.

4.3.5. Verificarea listei de certificate revocate (CRL)

O Entitate Parteneră, ca urmare a primirii unui document electronic semnat de un utilizator final, este obligată să verifice dacă certificatul cheii publice corespunzătoarea cheii private a utilizatorului, folosită pentru crearea de semnaturi electronice, nu este plasat în Lista de certificate Revocate. Entitatea Parteneră este obligată să folosească CRL-ul curent.

Verificarea stării unui certificat se poate baza în exclusivitate pe consultarea CRL-ului numai în cazurile în care frecvenţa perioadelor de emitere a CRL-ului, declarata de AlfaTrust Certification, nu poate aduce daune serioase sau pierderi pentru Entitatea Parteneră. În alte cazuri, o Entitate Parteneră este obligata să folosească serviciul de verificare on-line a stării certificatelor (OCSP).

Dacă un certificat de verificat este plasat într-un CRL, entitatea parteneră este obligată să respingă documentul asociat acestui certificat, dacă motivul revocării este unul dintre următoarele:

i. **unspecified** – necunoscut,
ii. **keyCompromise** – compromiterea securităţii cheii private,
iii. **cACompromise** – compromiterea securităţii Autorităţii de Certificare,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

iv. **cessationOfOperation** – încetarea serviciilor asociate cheii private,

Decizia finală asupra credibilităţii certificatului se va lua de către Entitatea Parteneră dacă un certificat a fost revocat din următoarele motive:

v. **affiliationChanged** – modificarea datelor,

vi. **superseded** – modificarea cheii.

4.3.6. Verificarea on-line a stării certificatelor (OCSP)

AlfaTrust Certification oferă serviciul de verificare în timp real a stării unui certificat. Acest serviciu se realizează pe baza protocolului OCSP, descris în RFC 2560. Folosind OCSP este posibil să se obţină date mai exacte (în comparaţie cu folosirea exclusivă a CRL-ului) despre starea unui certificat.

OCSP funcţionează pe baza modelului cerere-răspuns. Ca răspuns la o cerere, serverul OCSP, oferă următoarele informaţii despre starea certificatului:

* ***good*** – semnificând un răspuns pozitiv pentru cerere, care trebuie interpretat ca fiind confirmarea validităţii certificatului,
* ***revoked*** – însemnând că certificatul a fost revocat,
* ***unknown*** – semnificând că certificatul nu a fost emis de nici una dintre Autorităţile de Certificare afiliate.

Serviciul OCSP este disponibil oricărui utilizator final şi Entitate Parteneră care a semnat contractul cu AlfaTrust Certification în legătură cu oferirea acestor servicii.

Starea certificatului este întotdeauna oferită în timp real (imediat după revocarea certificatului) pe baza informaţiilor din baza de date a AlfaTrust Certification şi conţine informaţii mai noi decât cele din CRL-ul publicat.

O Entitate Parteneră nu este obligată să verifice on-line starea certificatelor pe baza serviciilor şi mecanismelor de mai sus. Totuşi, este recomandată folosirea serviciului OCSP atunci când riscul falsificării documentelor electronice prin folosirea semnaturii electronice este mare sau dacă acest lucru este cerut de alte reglementări care vizează astfel de situaţii.

4.3.7. Revocarea certificatului Autorității de Certificare (AC)

Certificatul aparţinând unei Autorităţi de Certificare poate fi revocat de către autoritatea emitentă. O astfel de revocare poate să apară în următoarele situaţii:

- Autoritatea de Certificare are motive să creadă că datele din certificatul autorităţii respective nu corespund realităţii,
- cheia privată a Autorităţii de Certificare sau sistemul său informatic au fost compromise astfel încât afectează credibilitatea certificatelor emise de această autoritate,
- Autoritatea de Certificare a încălcat obligaţiile materiale care reies din acest Cod de Practici şi Proceduri, Politica de Certificare, sau contract.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

4.4. Schimbarea cheii unei Autorități de Certificare (AC)

Procedurile de schimbare a cheii (*key changeover*) se aplică cheilor Autorităţilor de Certificare afiliate la AlfaTrust Certification şi descriu modul în care se face schimbarea cheilor certificatelor autorităţilor, folosite pentru semnarea certificatelor utilizatorilor sau CRL-urilor. Procedura de schimbare a cheii se bazează pe emiterea de către Autoritatea de Certificare a unui certificat special, ce permite unui utilizator care deţine vechiul certificat al autorităţii să-l obţină pe cel nou iar noilor utilizatori care au deja noul certificat al autorităţii să-l obţină pe cel vechi pentru verificarea datelor curente. Fiecare schimbare de cheie a Autorităţii de Certificare este anunţată în avans prin intermediul paginilor de web ale AlfaTrust Certification şi difuzată prin poşta electronica către fiecare utilizator al Autorităţii de Certificare a cărei chei urmează a fi schimbate. În plus, în cazul schimbării cheii AlfaTrust Certification ROOT CA, informaţiile despre acest eveniment vor fi publicate prin intermediul mass-media cu o luna înainte de momentului expirării perioadei de valabilitatea a cheii private. Frecvenţa schimbării cheilor unei Autorităţi de Certificare afiliată la AlfaTrust Certification este dată de perioada de valabilitate a certificatului autorităţii.

Din momentul schimbării cheii, Autoritatea de Certificare foloseşte numai noua cheie privată pentru semnarea certificatelor emise şi a CRL-urilor.

4.5. Încetarea activității unui Furnizor de Servicii de Certificare (FSC) sau transferarea serviciilor

Obligaţiile prezentate mai jos sunt stabilite pentru a minimiza efectele negative asupra utilizatorilor finali şi Entităţilor Partenere, ce pot apare ca urmare a deciziei unui Furnizor de Servicii de Certificare de a-şi înceta activitatea şi se refera la obligaţiile de a notifica în prealabil toţi utilizatorii că îşi încetează activitatea şi transferarea responsabilităţilor (servicii oferite utilizatorilor finali, baza de date, etc.), conform reglementărilor în vigoare, unui alt Furnizor de Servicii de Certificare.

4.5.1. Transferul responsabilității

Înainte ca un Furnizor de Servicii de Certificare să-şi înceteze activitatea, este obligat să:

1. anunţe Autoritatea de Certificare care a emis certificatul său despre intenţia de a-şi înceta activitatea ca Furnizor de Soluții de Certificare; notificarea trebuie făcută cu 90 de zile înainte de data stabilită pentru încetarea efectivă a activităţii,
2. să anunţe (cu cel puţin 30 de zile înainte) utilizatorii săi care au certificate active (neexpirate şi nerevocate) emise de autoritatea respectivă despre decizia de a-şi înceta activitatea,
3. să revoce toate certificatele care rămân active (neexpirate şi nerevocate) în momentul declarat al încetării activităţii, indiferent dacă utilizatorul a trimis sau nu o cerere în acest sens,
4. să anunţe toţi utilizatorii Furnizorului de Soluții de Certificare despre încetarea activităţii,
5. să depună toate eforturile pentru a minimiza efectele negative asupra intereselor utilizatorilor şi persoanelor juridice angajate în procese de verificare a semnăturilor electronice folosind certificate digitale emise de FSC-ul care îşi încheie activitatea,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

6. să propună încheierea unui contract (de exemplu cu un alt Furnizor de Soluții de Certificare) prin care să se garanteze protecţia datelor,
7. să plătească compensaţii (care să nu depăşească taxele de emitere şi depozitare a certificatelor) utilizatorilot al căror certificat neexpirat şi nerevocat va fi revocat înainte de data expirării.

4.5.2. Emiterea certificatelor de către succesor

Pentru a asigura continuitatea serviciilor de emitere de certificate pentru utilizatorii finali, Furnizorul de Servicii de Certificare care îşi încetează activitatea poate semna un contract cu alt FSC ce oferă servicii similare, pentru a emite certificate care să înlocuiască certificatele rămase în uz, emise de FSC-ul care îşi încheie activitatea.

Prin emiterea unui certificat care să-l înlocuiască pe cel vechi, succesorul Furnizorului de Servicii de Certificare care îşi încetează activitatea preia drepturile şi obligaţiile acestei autorităţi în ceea ce priveşte managementul certificatelor care rămân în uz.

5. Măsurile de securitate InfoSEC

Prin definiție, termenul InfoSEC reprezintă protecția surselor generatoare de informații. În sens mai larg, prin InfoSEC se înțelege ansamblul măsurilor şi structurilor de protecţie a informaţiilor care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice și de comunicaţii şi al altor sisteme electronice, împotriva ameninţărilor şi a oricăror acţiuni care pot aduce atingere confidenţialităţii, integrităţii, disponibilităţii, autenticităţii şi non-repudierii informaţiilor, precum şi afectarea funcţionării sistemelor informatice, indiferent dacă acestea apar accidental sau intenţionat.

Măsurile de securitate (controalele) InfoSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum şi depistarea şi prevenirea ameninţărilor la care sunt expuse informaţiile şi sistemele.

În sensul celor de mai sus definim și:

* **securitatea comunicaţiilor (ComSEC)** = aplicarea măsurilor de securitate în rețelele de comunicaţii, cu scopul de a proteja mesajele dintr-un sistem de comunicaţii, care ar putea fi interceptate, studiate, analizate şi, prin reconstituire, pot conduce la dezvăluiri de informaţii sensibile. ComSEC reprezintă ansamblul de:
  - măsuri de securitate a transmisiilor (TranSEC);
  - măsuri de securitate împotriva radiaţiilor (EmSEC sau TEMPEST);
  - măsuri de securitate criptografică;
  - măsuri de securitate fizică, procedurală, de personal şi a documentelor;
* **securitatea calculatoarelor și a rețelelor de calculatoare (CompuSEC)** = aplicarea la nivelul fiecărui calculator și/sau rețea de calculatoare a facilităţilor de securitate hardware, software şi firmware, pentru a preveni divulgarea, manevrarea, modificarea sau ştergerea neautorizată a informaţiilor sensibile ori invalidarea neautorizată a unor funcţii;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.1. Controale ComSEC

5.1.1. Controale de securitate criptografică (cryptosecurity)

Acest capitolul descrie procedurile de generare şi management a perechilor de chei criptografice a Furnizorul de Servicii de Certificare şi a utilizatorul final, inclusiv cerinţele tehnice asociate.

5.1.1.1. Generarea şi folosirea perechii de chei

Procedurile de management a cheii se referă la păstrarea şi folosirea în siguranţă de către proprietar a cheilor sale. O atenţie deosebită se acordă generării şi protecţiei cheii private a AlfaTrust Certification ROOT CA, care influenţează funcţionarea în siguranţă a întregului sistem de certificare a cheilor publice.

Autoritatea de Certificare AlfaTrust Certification ROOT CA deţine cel puţin un certificat autosemnat. Cheia privată corespunzătoare cheii publice conţinută de certificatul autosemnat este folosită exclusiv în scopul semnării cheilor publice ale Autorităţilor de Certificare direct subordonate (de pe nivelul 1 de certificare), prin semnarea certificatelor operaţionale şi a Listei de certificate Revocate, necesare pentru funcţionarea autorităţilor respective.

Perechile de chei deţinute de fiecare Autoritate de Certificare de pe nivelul 1 de certificare (SubCA-urile) permit semnarea de certificate şi CRL-uri - o cheie publică asociată cu o cheie privată autentificată cu un certificat autosemnat (în cazul AlfaTrust Certification ROOT CA) sau certificat (în cazul SubCA-urilor).

Semnatura electronica este creată prin folosirea algoritmului RSA în combinaţie cu rezumatul criptografic SHA-1.

5.1.1.1.1. Generarea perechilor de chei

Cheile Autorităților de Certificare de pe nivelul 1 de certificare (SubCA-urile), precum şi ale altor autorităţi subordonate acestora sunt generate în cadrul locaţiei AlfaTrust Certification, în prezenţa unui grup de persoane de încredere (administratorul de securitate şi administratorul Autorităţii de Certificare sunt membri ai acestui grup).

Perechile de chei pentru Autorităţile de Certificare care funcţionează în cadrul AlfaTrust Certification sunt generate la anumite staţii de lucru autentificate şi conectate la module hardware de securitate (HSM), conforme cu cerinţele FIPS 140-2 Nivel 3. Ele sunt menţinute în permanenţă criptate pe aceste dispozitive.

Procesul de generare de perechi de chei pentru Autorităţile de Certificare este similar cu procedura acceptată de generare a cheilor în cadrul AlfaTrust Certification. Acţiunile întreprinse în momentul generării perechii de chei sunt înregistrate, datate şi semnate de fiecare persoană prezentă în timpul generării. Înregistrările sunt păstrate din motive de audit sau pentru verificările obişnuite ale sistemului.

Operatorii Autorităţii de Înregistrare deţin numai chei pentru autentificarea tuturor acţiunilor lor. Aceste chei sunt generate de operator (în prezenţa administratorilor de secrete) prin intermediul unei aplicaţii software autentificată, furnizată de Autoritatea de Certificare şi conectată la un modulul hardware de securitate conform cu cerinţele FIPS 140-2 Nivel 2.

În general, fiecare utilizator final îşi generează singur perechea de chei. Pentru aceasta se va folosi de aplicaţia disponibila pe site-ul web al AlfaTrust Certification, în momentul creării cererii. Aplicaţia permite

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

crearea cheilor atât pe dispozitive securizate (tokenuri, smart carduri), cat şi în format “PKCS#12” criptat. Generarea poate fi, de asemenea, făcută de către o Autoritate de Certificare.

AlfaTrust Certification poate, la cererea utilizatorului sau la cererea operatorului Autorităţii de Înregistrare, să genereze o pereche de chei şi să o trimită în siguranţă utilizatorul final. În astfel de cazuri sunt folosite aplicaţii şi dispozitive criptografice conforme cu FIPS 140-2 Nivel 2.

Procedurile de generare a cheilor iniţiale ale Autorităţii de Certificare Primară

Procedurile de generare a cheii iniţiale a AlfaTrust Certification ROOT CA sunt folosite numai la iniţierea sistemului AlfaTrust Certification sau în cazul suspectării faptului că cheia privată a Autorităţii de Certificare Primară a fost compromisă. Procedura include:

- generarea în siguranţă a perechii principale de chei pentru semnarea de certificate şi CRL-uri şi distribuirea cheii private,
- emiterea unui certificat de cheie publică autosemnat.

După generarea perechii de chei pentru semnarea de certificate şi CRL-uri, activarea cheii private în modulul hardware de securitate, cheile pot fi folosite în operaţiile criptografice până la expirarea perioadei de validitate sau până când au fost compromise.

Procedura de schimbare a cheii certificatului pentru Autoritatea de Certificare Primară

Cheile criptografice ale Autorității de Certificare Primară (AlfaTrust Certification ROOT CA) au o perioadă de viaţă limitată; dacă această perioadă a expirat, cheile trebuie actualizate.

Actualizarea perechii de chei folosite pentru semnarea de certificate şi CRL-uri se face folosind o procedură specifică. Aceasta se bazează pe emiterea de certificate speciale de către AlfaTrust Certification ROOT CA.

Certificatele dau posibilitatea utilizatorilor care au instalat deja un certificat expirat al AlfaTrust Certification ROOT CA să treacă în siguranţă la utilizarea noului certificat; noii utilizatori care posedă deja noul certificat pot să obţină în siguranţă certificatul expirat, care poate fi necesar la verificarea datelor semnate în trecut.

Pentru a obţine efectul descris mai sus, AlfaTrust Certification ROOT CA aplică o procedură prin intermediul căreia generarea unei noi perechi de chei va permite autentificarea noii chei publice prin folosirea cheii private vechi şi invers (o cheie publică veche este autentificată cu o cheie privată nouă). Aceasta înseamnă că, drept rezultat al actualizării certificatului Autorităţii de Certificare, certAlfaTrust CertificationSIGN ROOT CA, în afară de certificatul nou, mai sunt create încă două certificate.

După actualizarea cheii, sunt create patru certificate pentru semnarea de certificate şi CRL-uri:

- certificatul vechi ***OldWithOld*** (cheia publică veche este semnată cu cheia privată veche),
- certificatul nou ***NewWithNew*** (cheia publică nouă este semnată cu cheia privată nouă),
- certificatul ***OldWithNew*** (cheia publică veche este semnată cu cheia privată noua) şi
- certificatul ***NewWithOld*** (cheia publică nouă este semnată cu cheia privată veche).

Procedura de actualizare a perechii de chei pentru AlfaTrust Certification ROOT CA, folosită pentru semnarea de certificate şi CRL-uri, se desfăşoară astfel:

- generarea unei perechi de chei noi,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- crearea unui certificat conţinând cheia publică nouă a AlfaTrust Certification ROOT CA, semnat cu cheia privată vechea (certificatul *NewWithOld*),
- dezactivarea cheii private vechi şi activarea celei noi în modulul hardware de securitate – este încărcată cheia privată nouă pentru semnarea de certificate şi CRL-uri,
- crearea unui certificat conţinând cheia publică veche a AlfaTrust Certification ROOT CA, semnat cu cheia privată nouă (certificatul *OldWithNew*),
- crearea unui certificat conţinând cheia publică nouă a AlfaTrust Certification ROOT CA, semnat cu cheia privată nouă (certificatul *NewWithNew*),
- publicarea în depozit a noilor certificate, difuzarea de informaţii despre noile certificate disponibile şi, opţional, publicarea rezumatului criptografic al noii chei publice în ziare.

După generarea şi activarea cheii private noi (acest lucru se poate face în orice moment, în timpul perioadei de validitate a vechiului certificat), autoritatea AlfaTrust Certification ROOT CA semnează noile certificate folosind exclusiv noua cheie privată.

Vechea cheie publică (vechiul certificat) este disponibilă publicului până când toţi utilizatorii obţin noul certificat (noua cheie publică) a AlfaTrust Certification ROOT CA (acesta trebuie obţinută înaintea datei de expirare a vechiului certificat).

Începutul şi expirarea perioadei de validitate a certificatului *OldWithNew* este aceeaşi cu data de început şi de expirare a certificatului vechi.

Perioada de validitate a certificatului *NewWithOld* începe din momentul generării noii perechi de chei şi expiră în momentul în care toţi utilizatorii finali vor obţine noile certificate (certificatul noii chei publice) ale AlfaTrust Certification ROOT CA. Momentul expirării nu este mai mare decât cel al expirării vechiului certificat.

Perioada de validitate a certificatului *NewWithNew* începe din momentul generării noii perechi de chei şi expiră la cel puţin 180 de zile după data următoarei generări de perechi de chei. Acest lucru înseamnă că Autoritatea de Certificare AlfaTrust Certification ROOT CA încetează a mai folosi cheia privată pentru semnarea de certificate şi CRL-uri cu cel puţin 180 de zile înainte de data expirării certificatului corespunzător acestei chei private.

Procedurile de generare a cheilor iniţiale ale AlfaTrust Certification SubCA-uri (cele de pe nivelul 1 de certificare)

Procedurile de generare a cheilor iniţiale pentru AlfaTrust Certification SubCA-uri includ:

- generarea în siguranţă a perechii principale de chei pentru semnarea de certificate şi CRL-uri şi distribuirea cheii private,
- emiterea unui certificat de cheie publică semnat de AlfaTrust Certification ROOT CA.

După generarea perechii de chei pentru semnarea de certificate şi CRL-uri şi activarea cheii private în modulul hardware de securitate, cheile pot fi folosite în operaţiile criptografice până la expirarea perioadei de validitate sau până la o eventuala compromitere.

Procedura de schimbare a cheii certificatelor autorităţilor subordonate de pe nivelul 1 de certificare

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Procedura de schimbare (actualizare) a cheilor Autorităţilor de Certificare pentru AlfaTrust Certification SubCA-uri se desfăşoară în mod similar cu cea pentru AlfaTrust Certification ROOT CA cu excepţia unui singur pas: certificatul *NewWithNew* este emis de către autoritatea superioară.

5.1.1.1.2. Distribuirea cheii private

Dacă perechea de chei a utilizatorului este generată de către o Autoritate de Certificare, cheile se distribuie utilizatorului astfel:

- cheile sunt stocate pe un dispozitiv criptografic (de exemplu, token), sau în format PKCS#12 pentru anumite cazuri şi sunt livrate personal utilizatorul final, sau printr-o scrisoare poştală recomandată; datele pentru activarea cardului (codul PIN) sau pentru decriptarea cheii (parola) sunt trimise separat de mediul de stocare care conţine perechile de chei; cardurile emise sunt personalizate şi înregistrate de Furnizorul de Servicii de Certificare.

AlfaTrust Certification garantează că după generarea perechii de chei la cererea unui utilizator, cheile nu vor fi folosite pentru crearea de semnaturi electronice şi că Autoritatea de Certificare nu va crea condiţii pentru crearea de semnaturi de către nici o entitate neautorizată, cu excepţia proprietarului cheii private.

5.1.1.1.3. Distribuirea cheii publice către Autoritatea de Certificare (AC)

Abonaţii trimit cheia lor publică generată sub formă de cerere electronica, al cărui format trebuie să respecte standardul PKCS#10 (CRS).

Cererile trimise unei Autorităţi de Înregistrare pot necesita, în anumite cazuri, o confirmare emisă de Autoritatea de Înregistrare.

Trimiterea cheii publice nu este necesară atunci când perechea de chei este generată, la cererea utilizatorului sau la cererea operatorului Autorităţii de Înregistrare, de către Autoritatea de Certificare, care emite simultan un certificat pentru perechea de chei generată.

5.1.1.1.4. Distribuirea cheii publice a Autorității de Certificare (AC)

Cheile publice ale unei Autorităţi de Certificare care emite certificate către utilizatori sunt distribuite în exclusivitate sub formă de certificate conform recomandărilor ITU-T X.509 v.3. În cazul Autorităţii de Certificare AlfaTrust Certification ROOT CA, certificatele sunt autosemnate.

Autorităţile de Certificare AlfaTrust Certification distribuie certificatele proprii în două moduri diferite:

- prin plasarea în depozitul public al AlfaTrust Certification; obţinerea certificatelor necesită vizitarea paginii web disponibilă la http://www.AlfaSign.ro/depozit,
- distribuirea împreună cu aplicaţiile software (browsere Web, clienţi de email etc.), care permit folosirea serviciilor oferite de AlfaTrust Certification .

In cazul schimbării (actualizării) cheii Autorităţii de Certificare AlfaTrust Certification-ROOT CA, depozitul va conţine toate certificatele autosemnate sau certificatele emise ca urmare a execuţiei procedurii descrise în subcapitolul 5.1.1.1.1.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.1.1.1.5. Dimensiunea cheilor

Dimensiunea cheilor folosite de Autorităţile de Certificare, operatorii Autorităţii de Înregistrare şi utilizatorii finali sunt :

* AlfaTrust Certification ROOT CA = 2048 biți;
* AlfaTrust Certification SubCA-uri = 2048 biți;
* Operatorii Autorității de Înregistrare = 1024 biți;
* Persoane (fizice sau juridice) și dispozitivele hardware ale acestora = 1024 biți.

5.1.1.1.6. Parametrii de generare a cheilor publice și verificarea calității parametrilor

Cine generează o cheie este responsabil de verificarea calităţii parametrilor cheii generate.

Acesta trebuie să verifice:

- posibilitatea de a efectua operaţii de criptare şi decriptare, inclusiv creare de semnaturi electronice şi verificare a acestora,
- procesul de generare a cheii trebuie să se bazeze pe generatoare puternice de numere aleatoare – surse fizice de zgomot alb, dacă este posibil,
- imunitatea la atacuri cunoscute (în cazul algoritmilor RSA şi DSA).

5.1.1.1.7. Generarea cheilor hardware și/sau software

Metodele permise pentru generarea de chei depind de Politica de Certificare aplicată şi sunt:

* pentru certificatele simple – hardware sau software, la alegerea clientului,
* pentru certificatele calificate pentru autentificarea utilizatorului, semătură electronică și criptare – exclusiv pe dispozitive securizate de creare a semnăturii electronice (DSCS-uri),
* pentru certificatele SSL (pentru autentificarea serverelor web și schimbul de chei simetrice), certificate de dispozitiv sau de semnare de cod – generat software de utilizator.

În cazul Autorităţilor de Certificare, cheile sunt generate prin intermediul modulelor hardware de securitate care respectă prevederile prezentate în subcapitolul 5.1.1.2.1.

Cheile operatorilor Autorităţii de Înregistrare sunt generate utilizând module hardware de securitate (HSM) care îndeplinesc standarde de nivel mai scăzut (decât cel descris în subcapitolul 5.1.1.2.1.). În cazul generării cheii de către un utilizator, Autoritatea de Certificare acceptă atât metode de generare hardware cât şi software.

5.1.1.1.8. Folosirea cheilor

Scopurile în care pot fi folosite cheile sunt date de câmpul *KeyUsage* (vezi subapitolul 6.1.2.) din cadrul extensiilor standard ale certificatelor X.509 v3. Acest câmp trebuie verificat în mod obligatoriu de aplicaţia utilizatorul final care face managementul certificatelor.

Folosirea biţilor din câmpul *KeyUsage* trebuie să respecte următoarele reguli:

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

a. ***digitalSIGNature***: certificat pentru verificarea de semnaturi electronice,

b. ***nonRepudiation***: certificat pentru furnizarea de servicii de non-repudiere către persoane fizice, cât şi pentru alte scopuri decât cele descrise la punctele f) şi g). Bitul de non-repudiere poate fi setat numai într-un certificat de cheie publică cu care se intenţionează verificarea semnaturilor electronice şi nu trebuie combinat cu cele descrise la punctele c) - e) şi în legătură cu asigurarea confidenţialităţii,

c. ***keyEncipherment***: folosit pentru a cripta cheile pentru algoritmi simetrici, oferind confidenţialitatea datelor,

d. ***dataEncipherment***: folosite pentru criptarea datelor utilizatorului, altele decât cele de la punctele c) şi e),

e. ***keyAgreement***: folosit în protocoale de schimb de chei,

f. ***keycertSIGN***: cheia publică este folosită pentru verificarea semnaturii electronice în certificatele emise de entităţi care oferă servicii de certificare,

g. ***cRLSign***: cheia publică este folosită pentru verificarea semnaturilor electronice de pe listele de certificate revocate şi suspendate emise de entităţile care oferă servicii de certificare,

h. ***encipherOnly***: poate fi folosit exclusiv cu bitul de keyAgreement pentru a indica criptarea datelor în procesul de schimb de chei,

i. ***decipherOnly***: poate fi folosit exclusiv cu bitul de *keyAgreement* pentru a indica decriptarea datelor în procesul de schimb de chei.

5.1.1.2. Protecţia cheii private

Fiecare utilizator, operator al Furnizorului de Servicii de Certificare şi Autoritate de Certificare generează şi stochează cheia sa privată folosind un sistem sigur care previne pierderea, dezvăluirea, modificarea sau accesul neautorizat la această cheie. Dacă o Autoritate de Certificare generează o pereche de chei la cererea utilizatorul final, trebuie să o livreze acestuia în siguranţă şi să impună utilizatorului protejarea cheii sale private.

5.1.1.2.1. Standarde pentru modulele criptografice

Modulele hardware de securitate (HSM) folosite de Autorităţile de Certificare respectă cerinţele standardului FIPS 140-2. În cazul utilizatorilor care folosesc mecanisme hardware de protecţie a cheii, se recomandă de asemenea respectarea cerinţelor FIPS 140-2 sau Common Criteria.

Crearea de semnatura electronica şi criptarea datelor se face conform standardului PKCS#7.

Cheile private (ca şi cheile publice) pot fi în una dintre următoarele stări (în conformitate cu standardul ISO/IEC 11770-1):

- ***în aşteptare pentru activare (pregătită)*** – cheia a fost deja generată, dar nu este utilizabilă (data curentă nu este încă aceeaşi cu data începerii perioadei de validitate a certificatului),
- ***activă*** – cheia poate fi folosită în operaţiile criptografice (de exemplu pentru crearea de semnaturii electronice), data curentă este în cadrul perioadei de validitate a certificatului, cheia nu a fost revocată,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- ***inactivă*** – cheia aflată în această stare poate fi folosită numai pentru verificarea de semnaturii electronice sau pentru operaţii de decriptare (utilizatorului nu-i este permisă folosirea cheii private pentru crearea de semnaturi electronice – validitatea cheii a expirat; în cazul unei chei publice, utilizatorului nu îi este permisă criptarea informaţiei); data curentă este în afara perioadei de validitate a certificatului.

5.1.1.2.2. Controlul dual al accesului cheii private

Controlul dual a unei chei private se aplică doar cheilor private ale Autorităţilor de Certificare de pe nivelurile 0 și 1 de certificare, folosite pentru semnarea de certificate şi CRL-uri.

Controlul dual al accesului se realizează prin distribuirea de secrete operatorilor autorizaţi. Secretele sunt stocate pe carduri criptografice sau token-uri, protejate printr-un cod PIN şi transferate în mod autentificat deţinătorilor acestora.

Pentru operaţiuni de tipul: iniţierea modulului criptografic hardware (HSM), transferul cheilor private ale Autorităţilor de Certificare, se implementează scheme prag de acces (de forma k din n) prin distribuire de secrete partajate. Numărul acceptat de secrete partajate şi numărul necesar de secrete care permit restaurarea cheii private sunt:

* *numărul de secrete partajate:* ***2***
* *numărul total de secrete distribuite:* ***3***

Pentru asigurarea serviciului de recuperare a cheilor private ale utilizatorilor finali se utilizează de asemenea scheme prag de acces. Numărul acceptat de secrete partajate este **2** şi numărul necesar de secrete care permit restaurarea cheii private este **3**.

Procedura de transfer a secretului partajat implică prezenţa deţinătorului de secret pe timpul procesului de generare a cheii şi a distribuirii sale, acceptarea secretului dat şi a responsabilităţilor care reies din păstrarea sa.

5.1.1.2.2.1. Acceptarea păstrării secretului de către deţinători

Fiecare deţinător de secret partajat, înainte de a primi partea sa de secret, trebuie să asiste personal la împărţirea secretului, să verifice corectitudinea secretului creat şi distribuirea sa.

Fiecare parte a secretului partajat trebuie transferată deţinătorului pe un card criptografic protejat de un cod PIN, ales de deţinător şi ştiut numai de el. Primirea secretului partajat şi crearea sa sunt confirmate printr-o semnatura de mână pe un formular, a cărui copie este păstrată în arhivele Autorităţii de Certificare şi de către deţinătorul de secret.

5.1.1.2.2.2. Protecţia secretului partajat

Deţinătorii secretului partajat trebuie să protejeze partea lor împotriva dezvăluirii. Deţinătorul declară că:

- nu va dezvălui, copia sau împărţi secretul cu nimeni şi că nu va folosi partea sa din secret într-un mod neautorizat,
- nu va dezvălui (direct sau indirect) că este deţinătorul secretului

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.1.1.2.2.3. Disponibilitatea şi ştergerea (transferul) secretului partajat

Deţinătorul secretului partajat trebuie să permită accesul la partea sa din secret persoanelor juridice autorizate (printr-un formular corespunzător semnat de către deţinător înaintea oferirii părţii sale din secret), numai după autorizarea transmiterii secretului. Această situaţie trebuie înregistrată în mod corespunzător în log-urile de securitate.

În cazul dezastrelor naturale, deţinătorul secretului trebuie să se prezinte la locul de recuperare în caz de urgenţă al AlfaTrust Certification, în conformitate cu instrucţiunile primite. Secretul partajat trebuie livrat personal de către deţinător la locul recuperării în caz de urgenţă, într-un mod care să permită folosirea lui pentru restaurarea condiţiilor normale de activitate ale AlfaTrust Certification.

5.1.1.2.2.4. Responsabilităţile deţinătorului de secret partajat

Deţinătorul de secret partajat trebuie să-şi îndeplinească îndatoririle şi obligaţiile conform cerinţelor acestui Cod de Practici şi Proceduri, în mod responsabil în orice situaţie posibilă. Un deţinător de secret partajat trebuie să anunţe emitentul secretului în cazul furtului, pierderii, dezvăluirii neautorizate sau compromiterii securităţii secretului, imediat după incident. Un deţinător de secret partajat nu este responsabil pentru neîndeplinirea îndatoririlor/obligaţiilor sale din cauza unor motive ce sunt imposibil de controlat de către acesta, dar este responsabil pentru dezvăluirea inoportună a secretului sau pentru neglijarea obligaţiilor de a notifica emitentul secretului despre dezvăluirea inoportună sau violarea securităţii secretului ca urmare a greşelilor, neglijenţei sau iresponsabilităţii deţinătorului.

5.1.1.2.3. Back-up-ul cheilor private

Autorităţile de Certificare care operează în cadrul AlfaTrust Certification creează o copie de siguranţă a cheii lor private. Copiile sunt folosite în cazul punerii în aplicare a procedurilor standard, sau de urgenţă (de exemplu, după dezastru) de recuperare a cheii. Copiile cheilor private sunt protejate prin secrete partajate.

AlfaTrust Certification nu păstrează copii ale cheilor private ale operatorilor Autorităţii de Certificare. Copiile cheilor private ale utilizatorilor sunt create numai la cererea utilizatorul final şi în conformitate cu Codul de Practici și Proceduri și Politicile de Certificare.

Copiile cheilor private de criptare ale utilizatorilor sunt pastrate criptat in baza de date a Autoritatilor de Certificare.

Astfel, fiecare cheie privata a utilizatorului este criptata simetric cu o cheie de sesiune. Cheile de sesiune sunt criptate cu o cheie master de decriptare. Accesul la aceasta cheie de decriptare se face prin secrete partajate, pe principiul K din N. Cheile private de semnare ale utilizatorilor nu sunt salvate.

5.1.1.2.4. Arhivarea cheii private

Cheile private ale Autorităţii de Certificare folosite pentru crearea de semnaturi electronice nu sunt arhivate – sunt distruse imediat după terminarea operaţiilor criptografice ce necesită aceste chei sau la expirarea/revocarea certificatului cheii publice asociate.

5.1.1.2.5. Introducerea cheii private în modulul criptografic

Operaţiunea de introducere a unei chei private într-un modul criptografic se aplică în următoarele cazuri:

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- când cheile sunt generate în afara modulului criptografic; această situaţie apare, de exemplu, în cazul generării cheii de către o Autoritate de Certificare la cererea utilizatorului, la introducerea lor într-un dispozitiv criptografic, înainte de trimiterea suportului de stocare către utilizatorul final. O operaţie similară de introducere a cheii într-un modul criptografic poate fi îndeplinită de un utilizator când cheile sunt livrate sub formă criptată şi necesită stocare locală pe un dispozitiv criptografic,
- în cazul creării copiilor de siguranţă ale cheilor private stocate într-un modul criptografic, poate fi necesară, ocazional (ex. în cazul compromiterii sau defectării modulului), introducerea unei perechi de chei într-un modul de securitate diferit,
- când este necesară transferarea unei chei private din modulul operaţional folosit pentru operaţii standard ale entităţii, pe un alt modul; situaţia poate apărea în cazul defectării modulului sau în cazul necesităţii distrugerii acestuia.

Introducerea unei chei private într-un modul de securitate este o operaţiune critică şi de aceea trebuie implementate măsuri şi proceduri care să prevină dezvăluirea, modificarea sau falsificarea cheii private.

Introducerea unei chei private într-un modul hardware de securitate (HSM) al Autorităţilor de Certificare de pe nivelele 0 și 1 de certificare necesită restaurarea cheii de pe carduri în prezenţa unui număr corespunzător de deţinători de secret partajat care protejează modulul ce conţine cheile private.

Deoarece fiecare Autoritate de Certificare poate deţine o copie criptată a cheii sale private, cheile pot fi de asemenea transferate între module.

5.1.1.2.6. Metoda de activare a cheii private

Metodele de activare a cheii private, deţinute de diverşi utilizatori sau utilizatori ai sistemului AlfaTrust Certification, se referă la activarea cheii înainte de orice folosire a sa, sau de începerea unei sesiunii de lucru ce necesită folosirea cheii respective (de exemplu, conectarea la Internet). O cheie odată activată poate fi folosită până la dezactivare.

Executarea procedurilor de activare (şi dezactivare) a unei chei private depinde de tipul entităţii care deţine cheia respectivă (utilizator final, Autoritate de Înregistrare, Autoritate de Certificare, dispozitiv hardware etc.), de senzitivitatea datelor protejate de cheie şi de intervalul de timp în care cheia trebuie să rămână activă (pe timpul unei singure operaţiuni, sesiuni sau pentru o perioadă nelimitată).

Toate cheile private ale Autorităţilor de Certificare AlfaTrust Certification de pe nivelele 0 și 1 de certificare, introduse în modul după generare, importate sub formă criptată dintr-un alt modul sau restaurate dintr-un secret partajat, rămân în stare activă până la ştergerea lor fizică de pe modul sau până la scoaterea lor din serviciile AlfaTrust Certification. Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea este realizată pe baza unui card criptografic deţinut de operator. După introducerea cardului în modulul criptografic şi folosirea codului PIN, cheia privată rămâne în stare activă până la scoaterea cardului din modul.

Cheile private ale operatorilor Autorităţii de Înregistrare sunt activate după autentificarea operatorului (folosirea codului PIN) şi numai pentru durata unei singure operaţii criptografice care necesită folosirea cheii respective. Ca urmare a încheierii acestei operaţii, cheia privată este dezactivată automat şi trebuie reactivată înaintea executării altei operaţii criptografice.

Activarea cheii private a unui utilizator final se face în mod similar cu procedura de activare a cheii private a operatorilor Autorităţii de Certificare, indiferent dacă sunt stocate pe un card criptografic sau sub formă

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

criptată, ca fişier pe o dischetă sau orice alt mediu de stocare. În cazul utilizatorilor finali persoane juridice (organizaţii, instituţii etc.) activarea trebuie să se facă de către o persoană autorizată a utilizatorului.

5.1.1.2.7. Metoda de dezactivare a cheii private

Metodele de dezactivare a cheii private se referă la dezactivarea cheii după folosirea acesteia sau ca urmare a terminării unei sesiuni în timpul căreia a fost folosită cheia.

În cazul unui utilizator final sau al unui operator al Autorităţii de Înregistrare, dezactivarea cheii private de semnatura se face imediat după încheierea sesiunii (la ieşire din aplicaţie). Dacă în timpul executării operaţiei criptografice, cheia privată a fost stocată în memoria aplicaţiei, aplicaţia trebuie să prevină refacerea neautorizată a cheii private. Dacă o cheie privată este deţinută de un utilizator persoană juridică, cheia poate fi dezactivată numai de reprezentantul autorizat al acestui utilizator.

În cazul AlfaTrust Certification, dezactivarea unei chei private se face de către ofiţerul de securitate numai în cazul în care o sesiune de lucru a fost încheiată, perioada de validitate a cheii a expirat, cheia a fost revocată sau este necesar să se suspende imediat activităţile sistemului. Dezactivarea unei chei private se face prin scoaterea cardului din modul.

5.1.1.2.8. Metoda de distrugere a cheii private

Ştergerea cheii private a unui utilizator sau operator al Autorităţii de Înregistrare presupune ştergerea ei de pe mediul de stocare (dischetă, card criptografic, memorie, modul hardware de securitate etc.). Dacă o cheie privată aparţine unui utilizator persoană juridică, cheia poate fi distrusă numai de către reprezentantul autorizat al utilizatorului.

Fiecare distrugere de cheie privată este înregistrată în jurnalul de evenimente.

5.1.1.3. Alte aspecte cu privire la managementul perechilor de chei

Cerinţelor din acest capitol se referă la procedurile de arhivare a cheii publice şi la perioada de validitate a cheilor publice şi private ale fiecărui utilizator, inclusiv ale Autorităţilor de Certificare.

5.1.1.3.1. Arhivarea cheilor publice

Scopul arhivării cheilor publice este acela de a crea posibilitatea verificării semnaturii electronice după eliminarea unui certificat din depozit. Acest lucru este foarte important în cazul serviciilor de non-repudiere, cum ar fi serviciul de marcă temporala sau serviciul de verificare a stării unui certificat.

Arhivarea cheilor publice presupune arhivarea certificatelor care conţin aceste chei.

Fiecare autoritate care emite certificate arhivează cheile publice ale utilizatorilor către care au fost emise certificatele. Cheile publice ale Autorităţii de Certificare sunt arhivate împreună cu cheile private. Certificatele pot fi, de asemenea, arhivate local de către utilizatorii finali, în special când acest lucru este cerut de aplicaţiile folosite (de exemplu, sistemele de poştă electronica).

Arhivele cheilor publice trebuie protejate în aşa fel încât să se prevină adăugarea, inserarea, modificarea şi ştergerea neautorizată de chei din arhivă. Protecţia este realizată prin autentificarea entităţii care face arhivarea şi autorizarea cererilor.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Administratorul de securitate verifică lunar integritatea arhivelor de chei publice. Scopul acestei verificări este de a asigura faptul că nu sunt goluri în arhive şi că certificatele din arhive nu au fost modificate. Mecanismul de verificare a integrităţii arhivelor ţine cont de faptul că perioada de păstrare poate fi mai lungă decât cea a mecanismelor de securitate folosite la crearea arhivelor.

Cheile publice sunt păstrate în arhivele cu certificate digitale 15 ani după momentul expirării.

5.1.1.3.2. Perioadele de folosire a cheilor private și publice

Perioada de folosire a cheilor publice este definită de valoarea câmpului validitate a fiecărui certificat de cheie publică. Există, de asemenea, şi o perioadă de validitate a cheii private. Perioada maxima de utilizare a cheilor utilizatorilor nu poate depăşi de 2 ori durata de viata a unui certificat. Valorile standard ale perioadei maxime de folosire a certificatelor Autorităţii de Certificare și a certificatelor utilizatorilor fiali sunt după cum urmează:

* pentru certificatul autosemnat al AlfaTrust Certification ROOT CA = **25** ani,
* pentru certificatele SubCA-urilor de pe nivelul 1 de certificare = **10** ani,
* pentru orice SubCA-uri off-site mai jos de nivelul 1 de certificare AlfaTrust Certification = **3** ani,
* pentru certificate client (simple sau calificate) = **1** an.

Perioada de folosire a certificatelor şi a cheilor private corespunzătoare poate fi mai scurtă în cazul revocării unui certificat.

În general, data de început a validităţii certificatului corespunde cu data emiterii sale. Nu este permisă stabilirea acestei date în trecut sau în viitor.

5.1.1.4. Datele de activare

Datele de activare sunt folosite pentru activarea unei chei private cu care operează o Autoritate de Înregistrare, o Autoritate de Certificare, sau un utilizator final. De obicei sunt folosite pentru autorizarea entităţilor şi pentru a controla accesul la cheia privată.

5.1.1.4.1. Generarea și instalarea datelor de activare

Datele de activare sunt folosite în două situaţii principale:

- ca element al unei proceduri de autentificare bazată pe unul sau mai mulţi factori (passphrase, parolă, cod PIN etc.),
- ca parte a unui secret partajat.

Operatorii Autorităţii de Înregistrare şi ai Autorităţilor de Certificare, precum şi alte persoane care îndeplinesc rolurile descrise în subcapitolul 5.1.1.7, folosesc parole rezistente la atacuri prin încercări repetate (forţa brută). Se recomandă ca şi utilizatorii finali să folosească astfel de parole.

În cazul activării cheii private, se recomandă să se folosească proceduri de autentificare bazate pe mai mulţi factori, de exemplu un card criptografic şi o frază de autentificare (passphrase) sau un jeton criptografic (token) şi un dispozitiv biometric (de exemplu, cititor de amprente).

Fraza de autentificare menţionată mai sus trebuie generată în concordanţă cu cerinţele FIPS-112.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Secretele partajate folosite pentru protejarea cheii private a Autorităţii de Certificare sunt generate în concordanţă cu cerinţele prezentate în subcapitolul 5.1.1.2. şi păstrate pe carduri criptografice. Cardurile sunt protejate printr-un cod PIN, creat în concordanţă cu cerinţele FIPS-112. Secretele partajate devin date de activare după activarea acestora, de exemplu, prin introducerea corectă a codului PIN care protejează cardul.

5.1.1.4.2. Protecţia datelor de activare

Protecţia datelor de activare include metodele de control a acestor date prin care se previne dezvăluirea lor. Metodele de control a datelor de activare depind de natura acestora: dacă sunt fraze de autentificare sau dacă acest control este bazat pe distribuirea informaţiilor de activare în secrete partajate. În cazul frazei de autentificare, trebuie impuse recomandările descrise în FIPS-112, pe când protejarea secretelor partajate necesită implementarea standardului FIPS-140.

Se recomandă ca datele de activare folosite pentru activarea cheii private să fie protejate prin controale criptografice şi de acces fizic. Datele de activare pot fi datele biometrice sau memorate (nu scrise) de către entitatea de autentificat. Dacă datele de autentificare sunt scrise, nivelul de protecţie trebuie să fie acelaşi cu cel al datelor pe care le protejează prin folosirea cardului criptografic. Mai multe încercări nereuşite de a accesa modulul criptografic trebuie să ducă la blocarea acestuia. Datele de activare stocate nu trebuie să fie păstrate niciodată împreună cu cardul criptografic.

5.1.1.4.3. Alte aspecte cu privire la datele de activare

Datele de activare sunt stocate într-un singur exemplar. Datele de activare care protejează accesul la cheia privată stocată pe carduri criptografice pot fi schimbate periodic. Datele de activare fac obiectul arhivării.

5.1.2. Măsuri de securitate fizică, procedurală, de personal şi a documentelor

Acest capitol descrie cerinţele generale privind securitatea fizică, procedurală și a documentelor, precum şi activitatea personalului AlfaTrust Certification în activitatea de generare de chei, verificarea autenticităţii entităţilor, emiterea şi publicarea certificatelor, revocarea certificatelor, audit şi crearea de copii de siguranţă.

5.1.2.1. Controale de securitate fizică

Sistemele de calcul, terminalele operatorilor şi resursele informaţionale ale AlfaTrust Certification sunt dispuse într-o zonă dedicată, protejată fizic împotriva accesului neautorizat, distrugerilor sau perturbării activităţii. Aceste locaţii sunt monitorizate. Fiecare intrare şi ieşire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum şi temperatura sunt de asemenea monitorizate şi controlate.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.1.2.1.1. Accesul fizic

Accesul fizic în cadrul AlfaTrust Certification este controlat şi monitorizat de un sistem de alarmă integrat. AlfaTrust Certification dispune de sisteme de prevenire a incendiilor, sisteme de detectare a intruziunilor şi sisteme de alimentare cu energie electrică în caz de urgenţă.

Sediul AlfaTrust Certification şi Autoritatea de Înregistrare sunt accesibile publicului în fiecare zi lucrătoare între 10:00 şi 16:00. În restul timpului (inclusiv în zilele nelucrătoare), accesul este permis numai persoanelor autorizate de către conducerea AlfaTrust Certification. Vizitatorii locaţiilor aparţinând AlfaTrust Certification trebuie să fie însoţiţi permanent de persoane autorizate.

Zonele ocupate de AlfaTrust Certification se împart în:

* **Zona de securitate clasa I** – nu este permis accesul (nici măcar însoțit) al nici unei persoane (vizitator, client sau personal al AlfaTrust Certification) cu excepția administratorilor de securitate și administratorilor de sistem. Persoanele autorizate de a pătrunde în această zonă de securitate nu vor intra niciodată singure ci vor respecta condiția de acces de minim 2 persoane (“***four eyes or two men rule”***). Această zonă de securitate este compusă din:
    - zona serverelor și a echipamentelor de comunicații,
    - zona administratorilor Autorităților de Certificare și a Autorității de Validare.

  Zona serverelor este echipată cu un sistem de securitate monitorizat continuu, alcătuit din senzori de mişcare, efracţie şi incendiu. Accesul în această zonă este permis numai personalului autorizat, de exemplu, administratorul de securitate, administratorul Autorității de Certificare şi administratorul de sistem. Monitorizarea drepturilor de acces se face folosind carduri şi cititoare, montate lângă punctul de acces. Fiecare intrare şi ieşire din zonă este înregistrată automat în jurnalul de evenimente.

* **Zona de securitate clasa a II-a** – în aceste zone este permis accesul numai persoanelor autorizate de conducerea AlfaTrust Certification, accesul și activitatea în aceste zone conformându-se principiului compartimentării muncii și a principiului nevoii de a cunoaște “***need to know***”. Această zonă este compusă din:
    - zona operatorilor Autorității de Înregistrare şi administratorilor,
    - zona de dezvoltare şi testare,
    - zona de depozitare a echipamentelor informatice, de comuncații sau criptografice.

  Controlul accesului în zona operatorilor şi administratorilor se face prin intermediul cardurilor şi a cititoarelor de carduri. Deoarece toate informaţiile senzitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor şi administratorilor necesită în prealabil autorizarea acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. Cheile de acces pot fi ridicate numai de personalul autorizat. În această zonă au acces numai angajaţii AlfaTrust Certification şi persoanele autorizate; ultimilor nu le este permisă prezenţa în zonă neînsoţiţi.

  Zona de dezvoltare şi testare este protejată într-o manieră similară cu zona operatorilor şi administratorilor. Dacă este necesar un altfel de acces, atunci el se poate face numai în prezenţa administratorul de securitate. Proiectele în curs de implementare şi software-ul aferent este testat în mediul de dezvoltare al AlfaTrust Certification.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

* **Zone administrative** – în această categorie intră orice alte zone din locația Furnizorului de Servicii de Certificare AlfaTrust Certification ce nu se încadrează în primele două clase de zone de securitate. În zonele administrative nu este permis accesul vizitatorilor sau a clienților decât dacă sunt însoțiți de personal al AlfaTrust Certification. Aceste zone se compun din:
    - birourile personalului,
    - zonele de primire a clienților AlfaTrust Certification.

5.1.2.1.2. Energie și climatizare

Zona operatorilor şi administratorilor, precum şi zona de dezvoltare şi testare sunt prevăzute cu surse de climatizare a mediului ambiental. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a grupului electrogen ce deservește toate facilitățile AlfaTrust Certification.

5.1.2.1.3. Expunerea la apă

AlfaTrust Certification şi-a luat precauţii deosebite pentru a minimiza impactul expunerii la apă a sistemelor AlfaTrust Certification.

5.1.2.1.4. Prevenirea și protecția împotriva incendiilor

AlfaTrust Certification şi-a luat precauţii deosebite pentru a preveni şi a stinge focul sau alte expuneri la flacără sau fum. Măsurile AlfaTrust Certification de prevenire şi protecţie împotriva focului au fost stabilite pentru a respecta reglementările cu privire la prevenirea si stingerea incendiilor şi siguranţa la foc.

5.1.2.1.5. Mediile de stocare

Toate mediile în care există software de producţie şi date, verificare, arhivă sau informaţii salvate se află în locaţiile AlfaTrust Certification sau intr-o locaţie off-site de înmagazinare securizată cu controale de acces fizic şi logic, pentru a limita accesul numai pentru personalul autorizat şi pentru a proteja aceste medii împotriva pagubelor accidentale (cauzate de apa, foc sau câmp electromagnetic).

5.1.2.1.6. Aruncarea lucrurilor nefolositoare

Documentele şi materialele sensibile sunt distruse (tocate) înainte de a fi aruncate. Mijloacele folosite pentru a strânge sau a transmite informaţiile sensibile nu mai pot fi citite, înainte de a fi aruncate. Înainte de a fi aruncate, dispozitivele criptografice sunt distruse fizic sau sterse într-o manieră sigură, în concordanţă cu îndrumările anterioare ale producătorului. Alte lucruri nefolositoare sunt aruncate, ţinând cont de cerinţele AlfaTrust Certification.

5.1.2.1.7. Depozitarea backup-urilor în afara locaţiei

Copiile parolelor, codurile PIN şi cardurile criptografice sunt stocate în containere speciale, situate în afara locaţiei AlfaTrust Certification.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Stocarea în afara locaţiei se aplică şi în cazul arhivelor, copiilor curente ale informaţiilor procesate de sistem şi kit-urilor de instalare ale aplicaţiilor AlfaTrust Certification. Acest lucru permite refacerea de urgenţă a oricărei funcţii a AlfaTrust Certification în 48 de ore, în locaţia principală a AlfaTrust Certification, sau în locaţia auxiliară.

5.1.2.2. Controale procedurale

Acest capitol prezintă rolurile ce pot fi atribuite personalului aparţinând AlfaTrust Certification, Autorităţii de Înregistrare, utilizatorilor finali şi entităților partenere. De asemenea, tot în acest capitol sunt descrise responsabilităţile şi sarcinile specifice fiecărui rol.

5.1.2.2.1. Funcții de încredere

Printre persoanele de încredere se numără toţi angajaţii, furnizorii şi consultanţii care au acces la sau controlează operaţiile de autentificare şi criptare și care pot influenţa:

* Validarea informaţiilor din cererile pentru certificate;
* Acceptarea, respingerea sau alte procesări ale cererilor pentru certificate, ale cererilor de revocare, ale cererilor de înnoire sau ale informaţiilor de înscriere;
* Emiterea sau revocarea certificatelor, inclusiv personalul care are acces la părţi restricţionate ale registrului său;
* Manipularea informaţiilor sau cererilor utilizatorului.

Printre persoanele de încredere se numără, dar nu se limitează numai la atât:

- Personalul de la serviciu clienţi,
- Personalul care se ocupa de operaţiile criptografice ale activităţii,
- Personalul de securitate,
- Personalul de la sistemul de administrare,
- Personalul de la departamentul tehnic,
- Directorii care se ocupă cu administrarea facilităților și infrastructurii.

În AlfaTrust Certification sunt definite următoarele roluri de încredere, care pot fi atribuite uneia sau mai multor persoane:

* ***Administrator de securitate*** = Responsabilitate globală pentru implementarea politicilor şi procedurilor de securitate. În plus poate aproba/revoca/suspenda certificate;
    - ✓ iniţiază instalarea, configurarea şi managementul aplicaţiilor software şi hardware (inclusiv resursele de reţea) ale AlfaTrust Certification;
    - ✓ iniţiază şi suspendă serviciile oferite de AlfaTrust Certification;
    - ✓ coordonează administratorii, iniţiază şi supraveghează generarea de chei şi secrete partajate;
    - ✓ atribuie drepturi din punct de vedere al securităţii şi privilegiilor de acces ale utilizatorilor;
    - ✓ creează conturile pentru utilizatorii AlfaTrust Certification;

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- ✓ atribuie parole pentru conturile utilizatorilor noi;
- ✓ verifică jurnalele de evenimente;
- ✓ supervizează auditurile interne şi externe;
- ✓ primeşte şi răspunde la rapoartele de audit;
- ✓ supervizează eliminarea deficienţelor constatate în urma auditului;
- ✓ supraveghează operatorii Furnizorului de Servicii de Certificare;
- ✓ configurează sistemele şi reţeaua, activează şi configurează mecanismele de protecţie a reţelei;
- ✓ verifică log-urile de sistem;
- ✓ verifică respectarea Politicii de Certificare şi a Codului de Practici şi Proceduri;
- ✓ generează secrete partajate şi chei;
- ✓ administrează Lista de Certificate Revocate;
- ✓ creează copiile de siguranţă;
- ✓ modifică numele şi adresele serverelor.

* ***Administratorul de secrete*** = își desfășoară activitatea la nivelul Autorităților de Certificare și Autorității de Validare;
  - ✓ supervizează şi transferă secretele (cheile criptografice şi alte date protejate) către operatorii Autorităţii de Înregistrare;
  - ✓ ia parte la activarea modulului criptografic şi la încărcarea cheilor operatorilor (în prezenţa acestora);
  - ✓ transferă şi activează cardurile de identitate ale operatorilor (dacă aceste carduri sunt blocate);
  - ✓ mediază contactele dintre Autoritatea de Înregistrare şi Autoritățile de Certificare;
* ***Administratorul de sistem*** = Autorizat să instaleze, configureze şi să întreţină sistemele de încredere ale Furnizorului de Servicii de Certificare AlfaTrust Certification pentru înregistrarea, generarea de certificate, iniţializarea dispozitivelor şi gestiunea revocărilor de certificate;
  - ✓ Instalează dispozitivele hardware şi sistemele de operare;
  - ✓ instalează şi configurează echipamentele de reţea;
  - ✓ instalează programe;
  - ✓ configurează sistemul şi aplicaţiile;
  - ✓ activează şi configurează resursele de securitate;
  - ✓ creează conturi şi parole pentru operatori;
  - ✓ creează copii de siguranţă şi arhivează datele;
  - ✓ verifică jurnalele de evenimente (log-uri) şi (împreună cu operatorul Autorităţii de Înregistrare), la ordinul administratorului de secrete, şterge datele în exces.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- ***Operatorul de sistem*** = Responsabil de operarea zilnică a sistemelor de încredere ale Furnizorului de Servicii de Certificare AlfaTrust Certification;
  - ✓ autorizat să execute operaţiile de backup şi restaurare a sistemului;
  - ✓ are acces la certificatele utilizatorilor finali;
  - ✓ revocă certificatele utilizatorilor;
  - ✓ asigură continuitatea copiilor de siguranţă şi arhivelor bazelor de date şi a creării log-urilor de sistem;
  - ✓ administrează bazele de date;
  - ✓ are acces la informaţii confidenţiale despre utilizatori, dar nu poate accesa fizic nici o altă resursă a sistemului;
  - ✓ transferă copiile de siguranţă ale arhivei şi ale datelor curente în afara locaţiei AlfaTrust Certification.
- ***Operatorii Autorității de Înregistrare*** = își desfășoară activitatea în zona de securitate clasa a II-a și în zonele administrative de la nivelul Autorității de Înregistrare;
  - ✓ verifică identitatea solicitanților de certificate şi corectitudinea cererilor primite;
  - ✓ emit confirmări ale cererilor pe care le trimit Autorităţii de Certificare;
  - ✓ generează cheile şi iau parte la generarea certificatelor, trimiţând informaţiile din cerere la o Autoritate de Certificare;
  - ✓ arhivează (sub formă de documente pe hârtie) cererile şi confirmările emise, care fac obiectul ştergerii, la ordinul administratorului de secrete şi în prezenţa acestuia,
- ***Auditorul de sistem*** = autorizat să acceseze arhivele şi log-urile de audit ale sistemelor de încredere ale Furnizorului de Servicii de Certificare AlfaTrust Certification. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici şi Proceduri și a Politicilor de Certificare de către Furnizorul de Servicii de Certificare; această responsabilitate se extinde şi asupra Autorităţii de Înregistrare care operează în cadrul AlfaTrust Certification.

  În cadrul AlfaTrust Certification, rolul de auditor nu poate fi combinat cu nici un alt rol. O entitate care are un rol diferit de cel de auditor nu poate prelua responsabilităţile auditorului.
- ***Administratorul depozitului*** = își desfășoară activitatea la nivelul Autorității de Validare și administrează directoarele AlfaTrust Certification disponibile publicului, creează şi actualizează conţinutul directoarelor din depozit, creează paginile web şi administrează legăturile (link-urile).

5.1.2.2.2. Numărul de persoane necesare pentru fiecare sarcină

Procesul de generare de chei – pentru semnarea certificatelor şi al CRL-urilor – este una din operaţiile ce necesită o atenţie deosebită. Generarea necesită prezenţa a cel puţin două persoane: un administrator de securitate şi un administrator de sistem. Procesul de generare a cheii Autorităţii de Certificare poate fi de asemenea observat de către posesori de secrete partajate care păstrează partea lor de cheie în locaţii sigure.

Prezenţa administratorului de securitate, a administratorului Autorităţii de Certificare şi a unui număr corespunzător de posesori de secrete partajate este necesară şi la încărcarea cheii criptografice a

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

Autorităţii de Certificare în modulul hardware de securitate (HSM). Încărcarea cheii criptografice a Autorităţii de Înregistrare în modulul hardware de securitate (daca este cazul) necesită prezenţa administratorului de secrete şi a unui operator al Autorităţii de Înregistrare.

Orice altă operaţiune sau rol, descris în cadrul CPP-ului sau care are legătură cu un utilizator final, poate fi efectuată de o singură persoană, special desemnată în acest sens.

5.1.2.2.3. Identificarea și autentificarea pentru fiecare rol

Personalul AlfaTrust Certification este supus identificării şi autentificării în următoarele situaţii:

- plasarea pe lista de persoane care au dreptul de a accesa locaţiile AlfaTrust Certification ,
- plasarea pe lista de persoane care au acces fizic la sisteme şi resurse de reţea aparţinând AlfaTrust Certification,
- emiterea confirmării care autorizează îndeplinirea rolului asignat,
- asignarea unui cont şi a unei parole în sistemul informatic al AlfaTrust Certification.

Fiecare cont desemnat:

* trebuie să fie unic şi desemnat direct unei anumite persoane,
* nu poate fi folosit în comun cu nici o altă persoană,
* trebuie restricţionat conform funcţiei (ce reiese din rolul îndeplinit de persoana respectivă) pe baza software-ului de sistem al AlfaTrust Certification, a sistemului de operare şi a controalelor de aplicaţii.

5.1.2.3. Controale de personal

AlfaTrust Certification garantează că se asigură că persoana care îndeplineşte responsabilităţile funcţiei, conform cu rolul atribuit în cadrul unei Autorităţi de Certificare, Validare sau Înregistrare:

- ✓ a absolvit cel puţin liceul,
- ✓ este cetăţean român,
- ✓ a semnat un contract care descrie rolul şi responsabilităţile sale în cadrul sistemului,
- ✓ a beneficiat de un stagiu de pregătire avansată în conformitate cu obligaţiile şi sarcinile asociate funcţiei sale,
- ✓ a fost instruit cu privire la protecţia datelor personale şi informaţiilor confidenţiale sau private,
- ✓ a semnat un contract ce conţine clauze referitoare la protejarea informaţiilor senzitive (din punctul de vedere al securităţii AlfaTrust Certification) şi a datelor confidenţiale şi private ale utilizatorilor finali,
- ✓ nu îndeplineşte sarcini care pot genera conflicte de interese între Autoritatea de Certificare şi Autoritatea de Înregistrare care acţionează în numele acesteia.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.1.2.3.1. Cerințe privind trecutul, calificările și experiența

Personalul care doreşte să se numere printre persoanele de încredere din AlfaTrust Certification trebuie să prezinte dovada îndeplinirii cerinţelor legate de trecut, calificări şi experienţă, necesare pentru a îndeplini în mod competent şi satisfăcător responsabilităţile postului respectiv, precum şi dovada oricăror acceptări guvernamentale, dacă există, necesare pentru a îndeplini servicii de certificare în baza unor contracte guvernamentale. Verificarea informaţiilor cu privire la personal se repetă la cel puţin 5 ani pentru personalul care ocupă poziţii de încredere.

Înainte de începerea serviciului într-o funcţie de încredere, AlfaTrust Certification face verificări asupra informaţiilor cu privire la personal, cuprinzând următoarele:

* Confirmarea locului de muncă anterior;
* Verificarea referinţelor profesionale;
* Confirmarea celei mai înalte sau relevante instituţii de învăţământ urmate;
* Solicitarea cazierului judiciar;
* Solicitarea rapoartelor financiare;
* Solicitarea rapoartelor privind permisul de conducere;
* Solicitarea rapoartelor privind asistenţa socială.

În măsură în care, oricare dintre cerinţele impuse de această secţiune, nu poate fi satisfăcută din cauza unei interziceri sau limitări din legea locala sau din cauza altor circumstanţe, AlfaTrust Certification S.A. va folosi o tehnică de investigaţie care este permisă de lege şi care furnizează informaţii asemănătoare, inclusiv, dar nu limitându-se la, obţinerea unei verificări a trecutului, realizată de agenţia guvernamentală adecvată.

Factorii implicaţi în verificarea trecutului, ce pot duce la respingerea candidaţilor pentru funcţiile de încredere sau la luarea de măsuri împotriva celor care fac parte deja dintre persoanele de încredere, includ în general următoarele:

- Prezentarea greşită a informațiilor cerute făcută de către candidat sau de către persoana de încredere;
- Referinţe personale nefavorabile sau care nu inspira încredere;
- Condamnări penale;
- Indicii ale lipsei de responsabilitate financiară.

Rapoartele care conţin astfel de informaţii sunt evaluate de personalul de la resurse umane şi securitate, care determină cursul potrivit al acţiunii, în funcţie de tipul, importanţa şi frecvenţa comportamentului dezvăluit de verificarea trecutului. Aceste acţiuni pot include măsuri care pot ajunge la anularea ofertelor de angajare pentru candidaţii la funcţii de răspundere sau la scoaterea din funcţie a persoanelor de încredere.

Folosirea informaţiilor găsite prin verificarea trecutului pentru a întreprinde astfel de acţiuni este supusă reglementarilor in vigoare din România.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.1.2.3.2. Cerințe de pregătire

AlfaTrust Certification S.A. asigură personalului pregătirea necesară pentru a îndeplini în mod competent şi satisfăcător responsabilităţile funcţiei. AlfaTrust Certification S.A. trece în revista periodic şi intensifică programele de pregătire, atunci când este nevoie.

Programele de pregătire ale AlfaTrust Certification S.A. sunt realizate ţinând cont de responsabilităţile individuale şi includ următoarele:

- ✓ Concepte de bază despre infrastructura cheii publice (PKI);
- ✓ Responsabilităţile funcţiei;
- ✓ Politicile şi procedurile de securitate şi operaţionale ale AlfaTrust Certification S.A.;
- ✓ Folosirea şi funcţionarea hardware-ului şi software-ului existent;
- ✓ Raportarea şi tratarea cazurilor de incident şi compromis;
- ✓ Procedurile de recuperare în caz de dezastru şi de continuare a activităţii.

5.1.2.3.3. Cerințele și frecvența cursurilor de perfecționare

AlfaTrust Certification S.A. furnizează cursuri de perfecţionare şi de actualizare pentru personal, în măsura şi cu frecvenţa care permit asigurarea menţinerii nivelului necesar pentru îndeplinirea competentă şi satisfăcătoare a responsabilităţilor de serviciu. Se asigură periodic pregătire de securitate.

5.1.2.3.4. Sancțiuni pentru acțiuni neautorizate

Se iau măsuri disciplinare adecvate pentru acţiunile neautorizate sau pentru alte violări ale politicilor şi procedurilor AlfaTrust Certification S.A. Acţiunile disciplinare pot include măsuri care duc până la încetarea contractului şi sunt luate în funcţie de frecvenţa şi severitatea acţiunilor.

5.1.2.3.5. Cerințe pentru contractarea personalului

În circumstanţe limitate, se pot folosi contractanţi sau consultanţi independenţi pentru a ocupa funcţii de încredere. Orice astfel de contractant sau consultant este menţinut după aceleaşi criterii funcţionale şi de securitate care se aplică şi în cazul angajaţilor AlfaTrust Certification, care se află într-o poziţie asemănătoare.

Contractanţii şi consultanţii independenţi care nu au desăvârşit procedurile de verificare a trecutului specificate la punctul 5.1.2.3.1 pot accesa locaţiile securizate ale AlfaTrust Certification numai dacă sunt escortaţi şi supravegheaţi direct de persoane de încredere.

5.1.2.3.6. Documentație furnizată personalului

Personalul AlfaTrust Certification implicat în funcţionarea serviciilor infrastructurii cheii publice ale AlfaTrust Certification trebuie să citească, sa înteleagă şi să-şi însuşească acest cod de practici şi proceduri şi politica de securitate a AlfaTrust Certification. AlfaTrust Certification S.A. oferă angajaţilor săi pregătirea necesară şi altă documentaţie necesară pentru a îndeplini competent şi satisfăcător responsabilităţile funcţiei.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.2. Controale CompuSEC

Sarcinile angajaților, colaboratorilor sau entităților partenere Furnizorului de Servicii de Certificare care lucrează în mediul AlfaTrust Certification sunt realizate prin intermediul unor dispozitive hardware (sisteme informatice și de comunicații, dispozitive criptografice, etc.) şi aplicaţii software de încredere.

5.2.1. Cerințele de securitate specifice

Cerinţele tehnice prezentate în acest capitol se referă la controalele de securitate specifice calculatoarelor, rețelelor de calculatoare şi aplicaţiilor folosite în mediul AlfaTrust Certification. Măsurile de securitate care protejează sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicaţiilor precum şi din punct de vedere fizic.

Calculatoarele aparţinând FSC-ului şi componentelor asociate acestora au implementate următoarele măsuri (controale) de securitate:

- ✓ autentificarea obligatorie la nivelul sistemului de operare şi al aplicaţiilor,
- ✓ control discreţionar al accesului,
- ✓ posibilitatea de a fi auditate din punct de vedere al securităţii,
- ✓ calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în AlfaTrust Certification ,
- ✓ separarea sarcinilor, conform rolului în cadrul sistemului,
- ✓ identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- ✓ prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,
- ✓ protecţia criptografică a schimburilor de informaţii şi protecţia bazelor de date,
- ✓ arhivarea istoricului operaţiunilor executate pe un calculator şi a datelor necesare auditării,
- ✓ o cale sigură ce permite identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- ✓ metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicaţilor şi a sistemului de operare,
- ✓ mijloace de monitorizare şi alertare în cazul accesului neautorizat la resursele de calcul.

5.2.2. Evaluarea securității calculatoarelor

Sistemele de calcul AlfaTrust Certification respectă cerinţele descrise în standardele ETSI: ETSI TS 101 456 (Cerinţele de Politică pentru Autorităţile de Certificare care emit certificate calificate) şi CEN CWA 14167 (Cerinţele de Securitate pentru Sistemele de Încredere care asigură Managementul certificatelor pentru Semnatura Electronica).

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.2.3. Controale pentru managementul securității informației

Scopul controalelor pentru managementului securităţii este acela de a superviza funcţionalitatea sistemelor AlfaTrust Certification, garantând astfel că acestea operează corect şi în concordanţă cu configurarea acceptată şi implementată.

Configuraţia curentă a sistemelor AlfaTrust Certification, precum şi orice modificare şi actualizare a acestora, este înregistrată şi controlată.

Controalele aplicate sistemelor AlfaTrust Certification permit verificarea continuă a integrităţii aplicaţiilor, versiunii şi autentificarea şi verificarea originii dispozitivelor hardware.

Fiecare aplicaţie, înainte de a fi folosita în producţie de AlfaTrust Certification, este instalata astfel încât să se permită controlul versiunii curente şi să se prevină instalarea neautorizată de programe sau falsificarea celor existente.

Reguli similare se aplică în cazul înlocuirii componentelor hardware, cum ar fi:

* dispozitivele fizice sunt furnizate în aşa fel încât să poată fi urmărita şi evaluată ruta fiecăruia, până la locul său de instalare,
* livrarea unui dispozitiv fizic pentru înlocuire se realizează într-un mod similar celui de livrare al dispozitivului original; înlocuirea se realizează de către personal calificat şi de încredere.

5.2.4. Controale de securitate a rețelei

Serverele şi staţiile de lucru de încredere aparţinând AlfaTrust Certification sunt conectate prin intermediul unei reţele locale (LAN), divizate în mai multe subretele, cu acces controlat. Accesul dinspre Internet către orice segment, este protejat prin intermediul unui firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului şi a filtrelor de trafic aplicate la nivelul ruterelor şi serviciilor Proxy.

5.3. Înregistrarea evenimentelor și procedurile de auditare

Pentru a gestiona eficient sistemele AlfaTrust Certification şi pentru a putea audita acţiunile utilizatorilor şi personalului AlfaTrust Certification, toate evenimentele care apar în sistem sunt înregistrate. Informaţiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente şi trebuie păstrate în aşa fel încât să permită Entităţilor Partenere să acceseze informaţiile corespunzătoare şi necesare rezolvării disputelor, sau să detecteze tentativele de compromitere a securităţii AlfaTrust Certification. Evenimentele înregistrate fac obiectul procedurilor de arhivare. Arhivele sunt păstrate în afara incintei AlfaTrust Certification.

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. Fiecare înregistrarea în log, electronic sau de mână, este păstrata şi dezvăluita atunci când se desfăşoară un audit.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

În sistemele AlfaTrust Certification, auditorul intern de securitate este obligat să realizeze anual un audit referitor la respectarea reglementărilor acestui Cod de Practici şi Proceduri de către mecanismele şi procedurile implementate şi să evalueze eficienţa procedurilor de securitate existente.

5.3.1. Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securităţii AlfaTrust Certification este înregistrată în logurile de evenimente şi arhivată. Arhivele sunt depozitate pe medii de stocare ce nu pot fi suprascrise pentru a preveni modificarea sau falsificarea lor.

Log-urile de evenimente AlfaTrust Certification conţin înregistrări ale tuturor activităţilor generate de componentele software din cadrul sistemului. Aceste înregistrări sunt împărţite în trei categorii separate:

- ✓ *înregistrări de sistem* – conţin informaţii despre cererile clienţilor şi răspunsurile serverului (sau invers) la nivelul protocolului de reţea (de exemplu http, https); datele concrete care se înregistrează sunt: adresa IP a staţiei sau a server-ului, operaţiunile executate (de exemplu: căutare, editare, scriere etc.) şi rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- ✓ *erori* – conţine informaţii despre erori la nivelul protocoalelor de reţea şi la nivelul modulelor aplicaţiilor,
- ✓ *audit* – conţin informaţii specifice serviciilor de certificare, de exemplu: cererea de înregistrarea şi de certificare, acceptarea certificatului, emiterea de certificat şi CRL etc.

Jurnalele de evenimente de mai sus sunt comune fiecărei componente instalate pe un server sau staţie de lucru şi au o capacitate prestabilită. Atunci când se depăşeşte această capacitate, este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat şi şters de pe disc.

Fiecare înregistrare, automată sau manuală, conţine următoarele informaţii:

- tipul evenimentului,
- identificatorul evenimentului,
- data şi ora apariţiei evenimentului,
- identificatorul persoanei responsabile de eveniment.

Conţinutul înregistrărilor se refera la:

- alertele firewall-urilor şi IDS/IPS-urilor,
- operaţiile asociate înregistrării, certificării, înnoirii, revocării, suspendării etc.,
- modificări ale structurii hard sau soft,
- modificări ale reţelei şi conexiunilor,
- înregistrările fizice în zonele securizate şi violările de securitate,
- schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,
- accesul reuşit şi nereuşit la baza de date AlfaTrust Certification şi la aplicaţiile serverului,
- generarea de chei pentru AC, AÎ, AV etc.,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- fiecare cerere primită şi decizia emisă în format electronic schimbate intre utilizator şi AÎ/AC,
- istoria creării copiilor de backup şi a arhivelor cu înregistrări.

Cererile înregistrate, asociate serviciilor oferite, trimise de către un utilizator, în afara utilizării lor în rezolvarea disputelor şi a detectării abuzurilor, permit calcularea taxei de emitere certificat.

Accesul al jurnalele de evenimente (log-uri) este permis în exclusivitate administratorului de securitate, administratorilor de sistem şi auditorilor.

5.3.2. Frecvenţa analizei jurnalelor de evenimente

Înregistrările din jurnalul de evenimente sunt revăzute în detaliu cel puţin o dată pe lună. Orice eveniment având o importanţă semnificativă este explicat şi descris într-un jurnal.

Procesul de verificare a jurnalului include verificarea unor eventuale falsificări, sau modificări şi verificarea fiecărei alerte sau anomalii consemnată în log-uri. Orice acţiune executată ca rezultat al funcţionări defectuoase detectate este înregistrată în jurnal.

5.3.3. Perioada de retenţie a jurnalelor de evenimente

Înregistrările evenimentelor sunt stocate în fişiere pe discul sistem până când acestea ajung la capacitatea maximă permisă. În tot acest timp sunt disponibile on-line, la cererea fiecărei persoane, sau proces autorizat. După depăşirea spaţiului alocat, jurnalele sunt păstrate în arhive şi pot fi accesate numai off-line, de la o anumită staţie de lucru.

Jurnalele arhivate sunt păstrate cel puţin 2 ani.

5.3.4. Protecţia jurnalelor de evenimente

Săptămânal, fiecare înregistrare din jurnale face obiectul arhivării pe bandă magnetică. După depăşirea numărului acceptat de înregistrări pentru un jurnal, conţinutul acestuia este arhivat.

Arhivele pot fi criptate folosind algoritmul Triple DES sau AES. O cheie folosită pentru criptarea arhivelor este plasată sub controlul administratorului de securitate.

Un jurnal de evenimente poate fi revăzut numai de administratorului de securitate, administratorul de sistem, sau de către un auditor. Accesul la jurnalul de evenimente este configurat în aşa fel încât:

- ✓ numai entităţile de mai sus au dreptul să citească înregistrările jurnalului,
- ✓ numai administratorul de securitate poate arhiva sau şterge fişiere (după arhivarea acestora) care conţin evenimentele înregistrate,
- ✓ este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conţin goluri sau falsuri,
- ✓ nici o entitate nu are dreptul să modifice conţinutul unui jurnal.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

În plus, procedurile de protecţie a jurnalului sunt implementate în aşa fel încât, chiar şi după arhivarea jurnalului, este imposibil să ştergi înregistrări, sau să ştergi jurnalul înaintea expirării perioadei de retenţie a jurnalului.

5.3.5. Procedurile de backup pentru jurnalele de evenimente

Procedurile de securitate AlfaTrust Certification solicita ca jurnalul de evenimente să facă obiectul back-up-ului lunar. Aceste backup-uri sunt stocate în locaţii auxiliare ale AlfaTrust Certification.

5.3.6. Notificarea entităţilor responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente şi sesizează automat activităţile suspecte sau pe cele care au ca scop compromiterea securităţii. În cazul activităţilor care au influenţă asupra securităţii sistemului, sunt notificaţi automat administratorul de securitate şi administratorul de sistem. În celelalte cazuri, notificarea este direcţionată numai către administratorul de sistem. Transmiterea informaţiilor către persoanele autorizate despre situaţiile critice – din punctul de vedere al securităţii sistemului – se face prin alte mijloace de comunicare, protejate corespunzător, de exemplu, pager, telefon mobil, poştă electronica. Entităţile notificate iau măsurile corespunzătoare pentru a proteja sistemul faţă de ameninţarea detectată.

5.3.7. Analiza vulnerabilităţilor

Autorităţile de Certificare, Autoritatea de Înregistrare şi Autoritatea de Validare fac o analiză a vulnerabilităţilor pentru fiecare procedură internă, aplicaţie şi sistem informatic. Cerinţele de analiză pot, de asemenea, să fie stabilite de către o instituţie externă, autorizată să auditeze AlfaTrust Certification. Administratorul de securitate are sarcina de a efectua audituri interne prin care să verifice conformitatea înregistrărilor din jurnalul de securitate, corectitudinea copiilor de backup, activităţile executate în cazul apariţiei unei ameninţări şi conformitatea cu Codul de Practici şi Proceduri.

Instituţia externă care efectuează auditul de securitate, trebuie să desfăşoare această activitate respectând recomandările ISO/IEC 13335 (Guidelines for Management of IT Security) şi ISO/IEC 27002 (Code of Practice for Information Security Management).

5.4. Arhivarea înregistrărilor

Este necesar ca toate datele şi fişierele referitoare la informaţiile despre securitatea sistemului, cererile trimise de utilizatori, informaţiile despre utilizatori, certificatele emise şi CRL-urile, cheile folosite de Autorităţile de Certificare şi Înregistrare, şi toată corespondenţa dintre AlfaTrust Certification şi utilizatorii finali să fie arhivate.

Depozitul on-line conţine certificatele active şi poate fi folosit pentru efectuarea unor servicii externe ale Furnizorului de Servicii de Certificare, de exemplu verificarea validităţii unui certificat, publicarea certificatelor pentru proprietarii acestora (restaurarea certificatelor) şi entităţile autorizate.

Arhivele off-line conţin certificate (inclusiv certificatele revocate) expirate cu până la 10 ani înainte de data curentă. Arhiva certificatelor revocate conţine informaţii despre certificatul identificat, motivul

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

revocării, dacă şi când a fost certificatul plasat în CRL. Arhiva este folosită pentru rezolvarea eventualelor dispute, referitoare la documente vechi, semnate electronic de un utilizator.

Pe baza arhivelor se creează copiile de siguranţă care sunt ţinute în afara locaţiei AlfaTrust Certification.

5.4.1. Tipurile de date arhivate

Următoarele date sunt incluse în procesul de arhivare:

- informaţiile rezultate în urma examinării şi evaluării (ca urmare a unui audit) măsurilor de protecţie logice şi fizice ale unei Autorităţi de Certificare, Autorităţii de Înregistrare şi Autorități de Validare,
- cererile primite şi deciziile emise, în formă electronica, trimise de, sau către un utilizator sub formă de fişiere sau mesaje electronice,
- baza de date cu utilizatorii finali,
- baza de date cu certificate,
- Listele de Certificate Revocate emise,
- istoria cheii Autorităţii de Certificare, de la generare până la distrugere,
- istoria cheilor utilizatorilor finali, de la generare până la distrugere, dacă cheia se arhivează în baza de date a Autorităţii de Certificare.

5.4.2. Frecvenţa arhivării datelor

Arhivarea datelor se realizează pe mai multe nivele, astfel:

* baza de date cu certificate şi baza de date cu utilizatori finali sunt păstrate pe mediile AlfaTrust Certification pentru o perioadă de 3 ani (din momentul emiterii certificatului). Pentru următorii 3 ani, arhivele sunt stocate pe benzi magnetice sau CD-uri, rămânând în continuare disponibile on-line. În al şaptelea an (la şase ani după emiterea de certificatului) toate informaţiile despre utilizatori şi certificatele acestora sunt stocate pe CD-uri şi sunt disponibile off-line,
* CRL, corespondenţa electronica şi cererile trimise de utilizatori precum şi deciziile emise sunt arhivate în acelaşi mod şi cu aceeaşi frecvenţă ca şi bazele de date cu certificate şi utilizatori,
* cheile Autorităţilor de Certificare, Înregistrare și Validare sunt stocate – după expirarea certificatelor asociate – pe medii ce nu pot fi suprascrise şi criptate cu cheia controlată de administratorul de securitate; cheile astfel arhivate sunt disponibile numai off-line.

5.4.3. Perioada de păstrare a arhivelor

Datele arhivate (sub formă electronica sau pe hârtie), descrise în subcapitolul 5.4.1 sunt păstrate pentru o perioada de timp de 15 ani. După expirarea perioadei de păstrare declarate, datele arhivate sunt distruse.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.4.4. Cerinţele pentru marcarea temporala a înregistrărilor

Datele arhivate sunt semnate cu o marcă temporala, creată de Autoritatea de Marcare Temporala (TSA) autorizată, având certificatul emis de Autoritatea de Certificare operaţională afiliată la AlfaTrust Certification CA. Serviciul de marcare temporala este disponibil în cadrul AlfaTrust Certification S.A.

5.4.5. Procedurile de acces şi verificarea informaţiilor arhivate

Pentru a verifica integritatea informaţiilor arhivate, datele sunt periodic testate şi verificate prin comparaţie cu datele originale (dacă mai sunt încă accesibile în sistem). Această activitate poate fi realizată numai de către administratorul de securitate şi trebuie înregistrată în jurnalul de evenimente. Dacă sunt detectate deteriorări sau modificări ale datelor originale, acestea sunt corectate cât mai repede posibil.

5.5. Procedura de backup si restaurare

Copiile de siguranţă permit restaurarea completă (dacă este necesar, de exemplu, după distrugerea sistemului) a datelor esenţiale pentru activitatea AlfaTrust Certification. Pentru a realiza acest lucru, sunt copiate următoarele aplicaţii şi fişiere:

- ✓ discurile de instalare a aplicaţiilor sistem (de exemplu sistemul de operare),
- ✓ discurile de instalare a aplicaţiilor pentru Autorităţile de Certificare, Înregistrare și Validare,
- ✓ serverul web,
- ✓ istoricul cheilor, certificatelor şi CRL-urilor autorităţilor,
- ✓ datele din depozit,
- ✓ datele privind utilizatorii finali şi personalul AlfaTrust Certification,
- ✓ jurnalele de evenimente.

Metoda de creare a copiilor de backup are o influenţă deosebită asupra timpului şi costului restaurării sistemelor Furnizorului de Servicii de Certificare după defectarea, sau distrugerea sistemului. AlfaTrust Certification foloseşte atât back-up-uri totale (săptămânale), cat şi back-up-uri incrementale (zilnice), toate copiile sunt clonate şi clonele sunt păstrate în altă locaţie, în aceleaşi condiţii de securitate ca şi cele din locaţia primară.

Procedura de restaurare va fi verificata cel puţin o data la 3 luni, pentru a se verifica utilitatea back-up-ului, in caz de dezastru. Se verifică daca datele salvate pe banda sunt suficiente pentru restaurarea sistemului in cel mai scurt timp posibil. Concluziile testelor vor fi inregistrate.

5.6. Compromiterea securităţii cheii şi recuperarea în caz de dezastru

Acest subcapitol descrie procedurile folosite de AlfaTrust Certification în situaţii anormale (inclusiv dezastrele naturale) pentru a reface serviciile la un nivel garantat. Aceste proceduri sunt aplicate în concordanţă cu Planul de continuitate a afacerii şi de recuperare în caz de dezastru.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

5.6.1. Compromiterea resurselor de calcul, a aplicaţiilor software şi/sau datelor

Politica de securitate a AlfaTrust Certification ia în considerare următoarele ameninţări ce pot influenţa disponibilitatea şi continuitatea serviciilor oferite:

- distrugerea fizică a sistemului de calcul al AlfaTrust Certification, inclusiv a resurselor de reţea – această ameninţare se referă la distrugerile provocate de situaţiile de urgenţă,
- funcţionarea defectuoasă a aplicaţiilor, având ca efect imposibilitatea accesării datelor - aceste deteriorări se referă la sistemul de operare, aplicaţiile utilizatorilor şi executarea de aplicaţii periculoase, cum ar fi viruşii, viermii, caii troieni,
- pierderea unor servicii de reţea importante pentru activitatea AlfaTrust Certification . Acestea se referă în primul rând la căderile de tensiune şi distrugerea legăturilor de reţea,
- distrugerea unei părţi din Intranetul folosit de AlfaTrust Certification pentru a furniza servicii – acest lucru poate duce la obstrucţionarea clienţilor şi refuzul (neintenţionat) serviciilor.

Pentru a preveni sau limita efectele ameninţărilor de mai sus:

* Politica de securitate a AlfaTrust Certification include un Plan de continuitate a afacerii şi recuperare în caz de dezastru,
* În cazul apariţiei unui eveniment ce blochează funcţionarea AlfaTrust Certification, în maxim 48 de ore, va fi activată locaţia auxiliară ce poate substitui toate funcţiile importante ale unei Autorităţii de Certificare până la restaurarea locaţiei principale. Distanta dintre locatia primara si cea secundara este suficienta pentru ca majoritatea potentialelor dezastre care pot afecta locatia primara sa nu afecteze in acelasi timp si locatia secundara,
* Instalarea de versiuni noi ale aplicaţiilor software în producţie se poate face numai după testarea intensivă a acestora într-un mediu de test, în conformitate cu procedurile descrise. Orice modificare a sistemului necesită aprobarea administratorului de securitate al AlfaTrust Certification,
* Sistemul AlfaTrust Certification dispune de aplicaţii pentru crearea copiilor de backup pe baza cărora se poate face în orice moment restaurarea sistemului şi auditarea acestuia. Copiile de siguranţă includ toate datele relevante din punct de vedere al securităţii.

5.6.2. Compromiterea sau suspiciunea compromiterii cheii private a unei Autorităţi de Certificare

În cazul compromiterii cheii private a unei Autorităţi de Certificare (afiliată la AlfaTrust Certification), sau în cazul suspiciunii unei astfel de compromiteri, trebuie luate următoarele măsuri:

- ✓ Autoritatea de Certificare generează o nouă pereche de chei şi un nou certificat,
- ✓ toţi utilizatorii de certificate sunt informaţi imediat despre compromiterea cheii private prin intermediul mass-media sau poştei electronice,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- ✓ certificatul corespunzător cheii compromise va fi pus în Lista de Certificate Revocate,
- ✓ toate certificatele din calea de certificare a certificatului compromis sunt revocate, specificându-se motivul revocării,
- ✓ se generează noi certificate pentru utilizatorii finali,
- ✓ noile certificate sunt trimise utilizatorilor în mod gratuit.

După fiecare recuperare a sistemului ca urmare a unui dezastru, administratorul de securitate sau administratorul de sistem va acţiona în conformitate cu Planul de continuitate a afacerii şi recuperare în caz de dezastru.

6. Profilele certificatelor, a listei de revocare a certificatelor și a protocolului de verificare on-line a stării certificatului

Profilul certificatelor şi al Listei de Certificate Revocate (CRL) respectă formatul descris în standardul ITU-T X.509 v.3, în timp ce profilul OCSP respectă cerinţele RFC 2560. Informaţiile de mai jos descriu semnificaţia câmpurilor din certificat, CRL şi OCSP, standardul aplicat şi extensiile folosite de AlfaTrust Certification.

6.1. Profilul certificatelor

Conform standardului X.509 v.3, un certificat este alcătuit din următoarea secvenţă de câmpuri:

- corpul certificatului (***tbscertificate***),
- informaţii despre algoritmul folosit pentru semnarea certificatului (***signatureAlgorithm***),
- semnatura electronica propriu-zisă a Autorităţii de Certificare (***signatureValue***).

6.1.1. Conținutul certificatului

Conţinutul certificatului include câmpuri de bază şi extensii (*standard* - descrise de norme şi *private* – definite de autoritatea emitentă).

Extensiile definite într-un certificat conform normelor permit adăugarea de atribute suplimentare specifice utilizatorului final şi cheii publice şi simplifică managementul structurii ierarhice a certificatului. Certificatele emise în conformitate cu standardul X.509 v.3 permit definirea unor extensii proprietare, unice pentru o implementare dată.

6.1.1.1. Câmpurile de bază

Certificatele AlfaTrust Certification conțin următoarele câmpuri de bază:

- ***Version***: a treia versiune (X.509 v.3) a formatului de certificat,
- ***SerialNumber***: numărul serial al certificatului, unic în cadrul domeniului Autorităţii de Certificare,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

* ***signatureAlgorithm***: identificatorul algoritmului de semnatura folosit de Autoritatea de Certificare emitentă, poate fi, după caz:
  - md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) sau
  - sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
* ***Issuer***: numele distinctiv (ND) al Autorităţii de Certificare,
* ***Validity***: perioada de validitate, descrisă prin intermediul unei date de începere (***notBefore***) şi a unei date de expirare (***notAfter***) a certificatului, în baza sistemului universal de referinţă temporala (Universal Time Coordinated). AlfaTrust Certification poseda un ceas controlat de Atomic Frequency Standard,
* ***Subject***: numele distinctiv (ND) al utilizatorului final care este subiectul certificatului. Numele distinctiv respectă cerinţele standardului X.501. Valorile unora dintre atributele acestor câmpuri sunt opţionale,
* ***SubjectPublicKeyInfo***: valoarea cheii publice împreună cu identificatorul algoritmului criptografic folosit. Criptat în conformitate cu RFC 3280, poate conţine informaţii despre cheile publice RSA, DSA sau ECDSA (identificatorul cheii, mărimea cheii în biţi şi valoarea cheii publice).

6.1.1.2. Extensiile standard ale certificatelor

Rolul fiecărei extensii este definit de valoarea standard a identificatorului de obiect folosit (Object Identifier - OID). Extensia, funcţie de opţiunea autorităţii emitente, poate fi critică sau non-critică. Dacă o extensie este definită ca fiind critică, aplicaţia care foloseşte certificatul trebuie să respingă orice certificat care conţine o extensie critică nerecunoscută. Pe de altă parte, extensiile definite ca fiind non-critice pot fi omise.

AlfaTrust Certification acceptă următoarele câmpuri de extensii standard:

- ✓ ***AuthorityKeyIdentifier***: identificatorul certificatului de cheie publică al Autorităţii de Certificare, asociat cheii private folosită pentru semnarea certificatelor – această extensie nu este critică,
- ✓ ***SubjectKeyIdentifier*** – identificatorul cheii subiectului - această extensie nu este critică,
- ✓ ***KeyUsage***: scopul în care poate fi folosită cheia - această extensie este critică. Extensia descrie pentru ce poate fi utilizată o cheie, de exemplu, pentru criptarea de date, pentru schimbul de date, pentru semnătură electronică, etc.:
  - *digitalSignature (0)* – cheie pentru crearea de semnaturi electronice,
  - *nonRepudiation (1)* – cheie asociată cu serviciile de ne-repudiere,
  - *keyEncipherment (2)* – cheie pentru schimbul de chei,
  - *dataEncipherment (3)* – cheie pentru criptarea datelor,
  - *keyAgreement (4)* – cheie pentru negocierea de chei,
  - *keycertsign (5)* – cheie pentru semnarea de certificate,
  - *cRLSign(6)* – cheie pentru semnarea de CRL-uri,
  - *encipherOnly (7)* – cheie numai pentru criptare,

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- *decipherOnly (8)* – cheie numai pentru decriptare.

✓ ***ExtKeyUsage***: defineşte restricţiile cu privire la folosirea cheii (RFC 3280 și predecesorii) - extensia nu este critică. Acest câmp defineşte unul sau mai multe domenii de utilizare posibilă a certificatului, adiţional domeniilor standard, definite de câmpul *KeyUsage*. Acest câmp trebuie înţeles ca o restrângere a scopurilor permise definite în câmpul *KeyUsage*. AlfaTrust Certification emite certificate care pot conţine una dintre următoarele valori sau o combinaţie de astfel de valori în câmpul *ExtKeyUsage*:

- *serverAuth* – autentificarea severelor web SSL/TLS; *KeyUsage* are setaţi biţii pentru:
  - *digitalSignature*, *keyEncipherment* sau *keyAgreement*;
- *clientAuth* – autentificarea clienţilor web SSL/TLS; *KeyUsage* are setaţi biţii pentru:
  - *digitalSignature* şi /sau *keyAgreement*;
- *codeSigning* – semnarea codurilor executabile; *KeyUsage* are setat bitul pentru
  - *digitalSignature*;
- *emailProtection* – protecţia e-mail-ului; *keyUsage* are setaţi biţii pentru:
  - *digitalSignature*, *nonRepudiation* şi/sau (*keyEncipherment* sau *keyAgreement*),
- *ipsecEndSystem* – protocolul de autentificare și/sau criptare IPSec,
- *ipsecTunnel* – protocolul IPSec Tunnelling,
- *ipsecUser* – protocolul de protecţie IPSec al aplicaţiilor utilizatorului,
- *timeStamping* – legarea rezumatului (digest) cu timpul furnizat de sursa de încredere; *KeyUsage* are setaţi biţii pentru:
  - *digitalSignature*, *nonRepudiation*.
- *ocspSigning* – asignează dreptul de a emite confirmări privind starea certificatului în numele AC-ului; *KeyUsage* are setaţi biţii pentru:
  - *digitalSignature*, *nonRepudiation*.
- *dvcs* – emiterea unei confirmări de către un notar autorizat, pe baza protocolului DVCS (RFC 3029 - Data Validation and Certification Server Protocols); *KeyUsage* are setaţi biţii pentru:
  - *digitalSignature*, *nonRepudiation*, *keyCertSign*, *cRLSign*.
- *EncryptedFileSystem* – permite folosirea certificatului pentru criptarea sistemului de fişiere (EFS); este cerut obligatoriu de anumite aplicaţii de acest gen (ex. EFS);
- *SmartCardLogon* – permite utilizarea certificatului pentru operaţia de „smartcard logon” - autentificare în sistemul de operare, bazată pe certificat digital;

✓ ***CertificatePolicies*** – extensia indică politica (politicile) sub care va emite certificate o Autoritate de Certificare sau politica (politicile) sub care a fost emis un certificat de către o Autoritate de Certificare. Extensia este o listă de *PolicyInformation* – informaţii (identificatorul, adresa electronica) despre o politică de certificare aplicată. Această extensie nu este critică.

Certificate emise de către Autorităţile de Certificare AlfaTrust Certification includ şi calificatori recomandaţi de RFC 3280:

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- ***PolicyMapping***: map-area politicii – acest câmp nu este critic; acest câmp conţine una sau mai multe perechi de OID, definind echivalenţa politicii emitentului certificatului cu politica subiectului certificatului,
- ***SubjectAlternativeName***: numele alternativ al subiectului – acest câmp nu este critic,
- ***BasicConstraints***: constrângeri de bază – indică tipul certificatului (certificat de AC sau entitate finală), precum şi lungimea maxim admisă pentru lanţul de certificate – acest câmp este critic,
- ***CRLDistributionPoints***: punctul de distribuire a Listei Certificatelor Revocate – acest câmp nu este critic; extensia defineşte adresa din reţea la care se află CRL-ul curent al Autorităţii emitente a certificatului în cauză,
- ***AuthorityInfoAccessSyntax***: accesul la informaţiile despre Autoritatea de Certificare – acest câmp nu este critic; câmpul indică metoda de informare şi furnizare a serviciilor de către emitentul certificatului,
- ***OCSPNoCheck***: dacă este prezentă în cadrul unui certificat al unui responder OCSP, clienţii care primesc răspunsuri OCSP semnate cu o cheie privată asociată certificatului pot avea încredere cu privire la starea acestui certificat pe perioada sa de valabilitate, această extensie este non-critică şi este definită de standardul RFC 2560,
- ***NetscapeCertType***: această extensie limitează utilizarea certificatului numai la anumite aplicaţii specificate de valoarea extensiei. Dacă nu este prezentă, certificatul poate fi folosit pentru orice aplicaţie cu excepţia aplicaţiilor de *ObjectSigning*. Extensia este necritică, iar valoarea să poate fi o combinaţie din următoarele:
    - *SSLClient* (bit 0) – certificatul poate fi folosit pentru autentificarea unui client SSL,
    - *SSLServer* (bit 1) – certificatul poate fi folosit pentru autentificarea unui server SSL,
    - *S/MIME* (bit 2) – certificatul poate fi folosit de clienţi de mail securizat S/MIME,
    - *ObjectSigning* (bit 3) - certificatul poate fi folosit pentru semnarea obiectelor cum ar fi apleturi Java sau plugin–uri,
    - *SSL CA* (bit 5) - certificatul poate fi folosit pentru emiterea de certificate utilizate pentru SSL,
    - *S/MIME CA* (bit 6) - certificatul poate fi folosit pentru emiterea de certificate utilizate pentru S/MIME,
    - *ObjectSigning CA* (bit 7) – certificatul poate fi folosit pentru emiterea de certificate utilizate pentru ObjectSigning,

  Observaţie: pentru valoarea extensiei NetscapeCertType, bitul 4 nu este încă definit fiind rezervat pentru o utilizare viitoare.

Certificatele emise de către AlfaTrust Certification pot conţine diferite combinaţii ale extensiilor definite în cadrul acestui subcapitol.

6.1.2. Identificatorul algoritmului de semnare

Câmpul ***signatureAlgorithm*** conţine identificatorul algoritmului criptografic folosit pentru semnarea electronica a certificatului de către Autoritatea de Certificare. În cazul AlfaTrust Certification este folosit algoritmul RSA, în combinaţie cu funcţia hash SHA-1.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

6.1.3. Câmpul ce conține semnătura electronică

Valoarea câmpului ***signatureValue*** este rezultatul aplicării funcţiei de hash asupra tuturor câmpurilor certificatului (*tbscertificate*) şi a algoritmului de semnare a rezumatului obţinut, folosind cheia privată a autorităţii.

6.2. Profilul listei de certificate revocate (CRL)

Lista de Certificate Revocate (CRL) constă din trei câmpuri;

- primul câmp (***tbscertList***) conţine informaţii despre certificatele revocate,
- al doilea (***signatureAlgorithm***) - informaţii despre identificatorul algoritmului folosit pentru semnarea listei,
- al treilea (***signatureValue***) conţine semnatura electronică a Autorităţii de Certificare.

Câmpul *tbscertList* este o secvenţă de câmpuri obligatorii şi opţionale. Câmpurile obligatorii identifică emitentul CRL-ului în timp ce câmpurile opţionale conţin informaţii despre certificatele revocate şi extensiile CRL-ului.

Conţinutul câmpurilor obligatorii şi opţionale dintr-un CRL sunt următoarele:

- ✓ ***Version***: versiunea formatului de CRL,
- ✓ ***Signature***: identificatorul algoritmului folosit de Autoritatea de Certificare pentru a semna CRL-ul; autorităţile AlfaTrust Certification semnează CRL-urile folosind algoritmul ***sha1WithRSAEncription***,
- ✓ ***Issuer***: numele Autorităţii de Certificare care a emis CRL-ul; fiecare autoritate a AlfaTrust Certification emite propria sa Listă de Certificate Revocate,
- ✓ ***ThisUpdate***: data publicării CRL-ului,
- ✓ ***NextUpdate***: date la care se va publica următorul CRL; dacă câmpul este prezent, valoarea sa descrie data maximă până la care se va face actualizarea CRL-ului,
- ✓ ***RevokedCertificates***: lista certificatelor revocate (câmpul este gol în cazul în care nu a fost revocat nici un certificat); informaţia constă din trei sub-câmpuri:
  - *usercertificates* – numărul serial al certificatului revocat,
  - *revocationDate* – data revocării certificatului,
  - *crlEntryExtensions* – conţine informaţii suplimentarea despre certificatele revocate - opţional.
- ✓ ***crlExtensions***: informaţii suplimentare despre Lista de Certificate Revocate (câmp opţional). Dintre extensiile posibile, cele mai importante sunt următoarele:
  - *AuthorityKeyIdentifier* - care permite identificarea cheii publice corespunzătoare cheii private folosită pentru semnarea listei şi

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

- *cRLNumber*, care conţine un număr serial incrementat monoton al listei emisă de Autoritatea de Certificare (prin intermediul acestei extensii, utilizatorul are posibilitatea de a determine dacă a fost publicat un nou CRL).

6.2.1. Extensiile acceptate în intrările din CRL

Rolul şi semnificaţia extensiilor este aceleaşi ca în cazul extensiilor de certificat. Extensiile dintr-o intrare CRL (*crlEntryExtensions*) acceptate de AlfaTrust Certification conţin următoarele câmpuri:

* ***ReasonCode***: codul motivului revocării certificatului. Acest câmp nu este critic şi permite determinarea motivului revocării unui certificat. Sunt permise următoarele motive de revocare:
  - ✓ *unspecified* – nespecificat;
  - ✓ *keyCompromise* – compromiterea cheii;
  - ✓ *cACompromise* – compromiterea cheii Autorităţii de Certificare;
  - ✓ *affiliationChanged* – modificarea datelor Abonatului;
  - ✓ *superseded* – înnoirea certificatului;
  - ✓ *cessationOfOperation* – sistarea folosirii certificatului;
  - ✓ *removeFromCRL* – eliminarea certificatului din CRL.

6.3. Profilul răspunsului de confirmare OCSP

Protocolul de verificare on-line a stării certificatelor (OCSP) permite determinarea stării unui certificat.

Serviciul OCSP este oferit de AlfaTrust Certification în numele tuturor Autorităţilor de Certificare afiliate. Serverul OCSP, care emite confirmări ale stării certificatelor, foloseşte o pereche specială de chei, generată exclusiv pentru acest scop.

Certificatul serverului OCSP trebuie să conţină extensia *ExtKeyUsage*, descrisă în RFC 3280. Această extensie trebuie declarată ca fiind non-critică şi semnifică faptul că o Autoritate de Certificare care emite certificatul pentru serverului OCSP confirmă prin semnatura sa delegarea autorizării de a emite confirmări ale stării certificatelor (aparţinând utilizatorilor acestei autorităţi).

De asemenea, certificatul serverului OCSP conţine extensia *OCSPNoCheck*, descrisă de RFC 2560. Această extensie trebuie declarată ca fiind non-critică şi semnifică faptul că un client de OCSP care primeşte un răspuns semnat cu cheia privată asociată acestui certificat va putea avea încredere în starea certificatului serverului OCSP, nefiind necesară verificarea stării de revocare a acestuia.

Entitatea care primeşte o confirmare emisă de serverul OCSP trebuie să suporte formatul standard de răspuns având identificatorul ***id-pkix-ocsp-basic***.

Cand raspunsul de OCSP contine un cod (mesaj) de eroare, acest raspuns nu este semnat digital (RFC 2560).

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

6.3.1. Numărul versiunii

Serverul OCSP care operează în cadrul AlfaTrust Certification emite confirmări ale stării certificatelor în conformitate cu RFC 2560. Singura valoare permisă a numărului versiunii este 0 (este echivalentul versiunii v1).

6.3.2. Informațiile despre starea certificatului

Informaţiile despre starea certificatului se află în câmpul *certStatus* al structurii ***SingleResponse***. Acesta poate avea una dintre cele trei valori principale:

- ✓ **GOOD** – indică faptul că certificatul este în stare validă
- ✓ **REVOKED** – indică faptul că certificatul a fost emis şi a fost revocat
- ✓ **UNKNOWN** – indică faptul că nu există suficiente informaţii pentru determinarea stării certificatului respectiv.

6.3.3. Extensiile standard acceptate

În concordanţă cu RFC 2560, serverul OCSP al AlfaTrust Certification acceptă următoarea extensie:

- ✓ ***Nonce*** – leagă o cerere de un răspuns pentru a preveni atacurile prin reluare. Nonce este inclus în *requestExtensions* al ***OCSPRequest*** şi repetat în câmpul *responseExtensions* al ***OCSPResponse***.

7. Managementul Codului de Practici și Proceduri

Fiecare versiune a Codului de Practici şi Proceduri este în vigoare până în momentul aprobării și publicării noii sale versiuni. O nouă versiune este dezvoltată de către AlfaTrust Certification şi publicată pentru comentarii cu menţiunea spre aprobare (dacă este cazul). După primirea şi includerea comentariilor, Codul de Practici şi Proceduri intră în procedura de aprobare interna. Responsabil de aprobarea formei finale a Codului de Practici și Proceduri este un comitet format din directorul general și managerii departamentelor din AlfaTrust Certification. Responsabil pentru intretinerea Codului de Practici si Proceduri este managerul departamentului care asigură furnizarea serviciilor de certificare. După terminarea procedurii de aprobare, noua versiune a CPP este transmisa Autorităţii de Reglementare şi Supraveghere si apoi, in teremen de 10 zile, este publicată şi marcată ca fiind în starea validă. Regulile şi cerinţele descrise mai jos, cu privire la managementul Codului de Practici şi Proceduri guvernează şi managementul Politicii de Certificare.

Utilizatorii finali și entitățile partenere trebuie să respecte numai Politica de certificare şi Codul de Practici şi Proceduri în vigoare în momentul respectiv.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195

7.1. Procedura de modificare a CPP

Modificarea Codului de Practici şi Proceduri poate fi rezultatul depistării unor erori, actualizării sale sau a sugestiilor primite din partea entităţilor interesate. Propunerile de modificare pot fi trimise prin poştă sau e-mail pe adresa AlfaTrust Certification S.A. Propunerile de modificare trebuie să descrie modificările necesare, motivele acestor modificări şi să ofere mijloace de contact ale persoanei care solicită modificarea.

După introducerea unei modificări, este actualizată data emiterii Codului de Practici şi Proceduri sau a Politicii de Certificare şi este modificat numărul versiunii documentului.

Modificările introduse pot fi în general împărţite în două categorii: una care nu necesită consultarea utilizatorilor și entităților partenere şi una care cere (de obicei în avans) consultarea acestora. Prima categorie include modificari de urgenta sau modificari neesentiale.

Identificatorii politicilor de certificare folosite de autorităţile emitente de certificate pot fi, de asemenea, modificaţi ca urmare a implementării următoarelor schimbări:

* schimbarea extensiei pentru un grup de utilizatori de certificate în domenii precum sistemele electronice de plăţi, schimburile de informaţii dintre bănci etc.;
* introducerea unor noi tipuri de certificate;
* permiterea cross-certificării între autorităţile emitente de certificate din cadrul sistemului;
* modificări semnificative ale conţinutului şi modului de interpretare a câmpurilor certificatului şi ale CRL-ului, de ex. modificarea caracterului critic/necritic al unui câmp.

7.2. Publicarea CPP-ului

O copie a Codului de Practici şi Proceduri este disponibilă în formă electronica pe site-ul de web http://www.AlfaSign.ro/depozit sau prin e-mail la adresa office@AlfaSign.ro.

7.2.1. Documente ce nu se publică în CPP

Documentația de securitate (proceduri și instrucțiuni detaliate de lucru), care sunt considerate confidenţiale de AlfaTrust Certification, nu se dezvăluie publicului. În această categorie intră și regulamentele interne, ce nu vor fi făcute publice.

ALFATRUST CERTIFICATION S.A., Calea Victoriei nr. 155, bl. D1, tr. 8, et. 7, 010073, Sector 1, Bucuresti, România
Tel.: +4 021/316 08 96, Fax: +4 021/316 08 97, office@alfastamp.ro, www.alfastamp.ro
CF: 16477015, RC: J40/8982/2004, Cap. Soc.: 200.000 lei, Marfin Bank (România) S.A., Cont: RO79EGNA1010000000276286
Operator de date cu caracter personal cu nr. 18195