



CODUL DE PRACTICI ȘI PROCEDURI ALFATRUST CERTIFICATION

Contents

1. Introducere.....	7
1.1. Rolul Codului de Practici și Proceduri	7
1.1.1. Rezumatul politicii de certificare	8
1.2. Privire de ansamblu asupra infrastructurii de certificare	8
1.3. Sfera de aplicabilitate	10
1.3.1. Sfera de aplicabilitate a prezentului CPP	10
1.3.2. Sfera de aplicabilitate a certificatelor/sigiliilor emise de AlfaTrust Certification	10
1.3.3. Autorități de certificare (AC)	12
1.3.4. Autorități de înregistrare (AÎ)	14
1.3.5. Autoritatea de Validare (AV)	14
1.3.6. Utilizatorii finali și entitățile partenere	14
1.4. Detalii de contact.....	15
2. Dispoziții generale	16
2.1. Obligații.....	16
2.1.1. Obligațiile Autorității de Certificare (AC).....	16
2.1.2. Obligațiile Autorității de Înregistrare (AÎ)	17
2.1.3. Obligațiile Autorității de Validare (AV)	17
2.1.4. Obligațiile utilizatorului final	18
2.1.5. Obligațiile entităților partenere.....	19
2.2. Responsabilitate	21
2.2.1. Responsabilitatea Prestatorului de Servicii de Încredere (FSC)	21
2.2.2. Responsabilitatea utilizatorului	22
2.2.3. Responsabilitatea părților contractante.....	23
2.3. Responsabilități financiare	23
2.4. Legea aplicabilă și soluționarea litigiilor	23
2.5. Prețul serviciilor prestate.....	23
2.6. Publicarea și înregistrarea informațiilor	24
2.6.1. Publicarea informațiilor de către AlfaTrust Certification S.A.	24
2.6.2. Frecvența publicării	25
2.6.3. Controlul accesului la informații.....	26
2.7. Auditul de conformitate	26
2.7.1. Frecvența auditului de conformitate.....	26
2.7.2. Identitatea/calificarea auditorului.....	26
2.7.3. Ariile supuse	27

2.7.4. Acțiuni acceptate ca rezultat al neconformităților	27
2.8. Confidențialitate	27
2.8.1. Tipuri de informații confidențiale	28
2.9. Drepturi de proprietate intelectuală	29
3. Identificare și autentificare	29
3.1. Înregistrarea inițială.....	29
3.1.1. Tipuri de nume.....	30
3.1.2. Necesitatea ca numele să aibă sens	30
3.1.3. Unicitatea numelor.....	31
3.1.4. Procedura aplicabilă în litigiile referitoare la dreptul la nume.....	32
3.1.5. Metode de a dovedi posesia cheii private.....	32
3.1.6. Autentificarea identității persoanelor juridice	33
3.1.7. Autentificarea identității persoanelor fizice.....	35
3.1.8. Autentificarea dispozitivelor	35
3.2. Autentificarea identității la reînnoirea sau modificarea certificatului	36
3.2.1. Reînnoirea unui certificat	36
3.2.2. Modificarea unui certificat	36
3.3. Autentificarea identității la revocarea unui certificat	37
4. Cerințe operaționale.....	37
4.1. Trimiterea cererii	38
4.1.1. Cererea de înregistrare.....	38
4.1.2. Cererea de reînnoire sau modificare certificat.....	39
4.1.3. Cererea de revocare a unui certificat	39
4.2. Tratarea cererilor pentru furnizarea serviciilor de încredere.....	39
4.2.1. La Autoritatea de Înregistrare (AÎ).....	40
4.2.2. La Autoritatea de Certificare (AC).....	40
4.2.3. Emiterea certificatelor	40
4.2.4. Respingerea cererii de certificat.....	41
4.2.5. Acceptarea certificatelor	42
4.2.6. Folosirea certificatelor și a cheilor.....	42
4.3. Revocarea certificatelor.....	43
4.3.1. Circumstanțele revocării certificatului	43
4.3.2. Cine poate solicita revocarea	44
4.3.3. Procedura de revocare	44
4.3.4. Frecvența de emitere a CRL-urilor.....	46
4.3.5. Verificarea listei de certificate revocate (CRL)	46

4.3.6. Verificarea on-line a stării certificatelor (OCSP)	47
4.3.7. Revocarea certificatului Autorității de Certificare (AC)	47
4.4. Schimbarea cheii unei Autorități de Certificare (AC)	47
4.5. Încetarea activității unui Furnizor de Servicii de Încredere (FSC) sau transferarea serviciilor	48
4.5.1. Transferul responsabilității	48
4.5.2. Emiterea certificatelor de către succesor	48
5. Măsurile de securitate InfoSEC	49
5.1. Controale ComSEC	49
5.1.1. Controale de securitate criptografică (cryptosecurity)	49
5.1.1.1. Generarea și folosirea perechii de chei	49
5.1.1.2. Generarea perechilor de chei	50
5.1.1.3. Distribuirea cheii private	52
5.1.1.4. Distribuirea cheii publice către Autoritatea de Certificare (AC)	53
5.1.1.5. Dimensiunea cheilor	53
5.1.1.6. Parametrii de generare a cheilor publice și verificarea calității parametrilor	53
5.1.1.7. Generarea cheilor hardware și/sau software	54
5.1.1.8. Folosirea cheilor	54
5.1.2. Protecția cheii private	55
5.1.2.1. Standarde pentru modulele criptografice	55
5.1.2.2. Controlul dual al accesului cheii private	55
5.1.2.2.1. Acceptarea păstrării secretului de către deținători	56
5.1.2.2.2. Protecția secretului partajat	56
5.1.2.2.3. Disponibilitatea și ștergerea (transferul) secretului partajat	56
5.1.2.2.1. Responsabilitățile deținătorului de secret partajat	56
5.1.2.3. Back-up-ul cheilor private	57
5.1.2.4. Arhivarea cheii private	57
5.1.2.5. Introducerea cheii private în modulul criptografic	57
5.1.2.6. Metoda de activare a cheii private	58
5.1.2.7. Metoda de dezactivare a cheii private	58
5.1.2.8. Metoda de distrugere a cheii private	58
5.1.3. Alte aspecte cu privire la managementul perechilor de chei	59
5.1.3.1. Arhivarea cheilor publice	59
5.1.3.2. Perioadele de folosire a cheilor private și publice	59
5.1.4. Datele de activare	60
5.1.4.1. Generarea și instalarea datelor de activare	60
5.1.4.2. Protecția datelor de activare	60

5.1.4.3.	Alte aspecte cu privire la datele de activare.....	61
5.2.	Măsurile de securitate fizică, procedurală, de personal și a documentelor	61
5.2.1.	Controale de securitate fizică	61
5.2.1.1.	Accesul fizic.....	61
5.2.1.2.	Energie și climatizare	62
5.2.1.3.	Expunerea la apă	62
5.2.1.4.	Prevenirea și protecția împotriva incendiilor	62
5.2.1.5.	Mediile de stocare	63
5.2.1.6.	Aruncarea lucrurilor nefolositoare	63
5.2.1.7.	Depozitarea backup-urilor în afara locației	63
5.2.2.	Controale procedurale.....	63
5.2.2.1.	Funcții de încredere	63
5.2.2.2.	Numărul de persoane necesare pentru fiecare sarcină	66
5.2.2.3.	Identificarea și autentificarea pentru fiecare rol.....	66
5.2.3.	Controale de personal	67
5.2.3.1.	Cerințe privind calificările și experiența	67
5.2.3.2.	Cerințe de pregătire.....	68
5.2.3.3.	Cerințele și frecvența cursurilor de perfecționare	68
5.2.3.4.	Sanctiuni pentru acțiuni neautorizate	68
5.2.3.5.	Cerințe pentru contractarea personalului	69
5.2.3.6.	Documentație furnizată personalului.....	69
5.3.	Controale CompuSEC.....	69
5.3.1.	Cerințele de securitate specifice	69
5.3.2.	Evaluarea securității calculatoarelor	70
5.3.3.	Controale pentru managementul securității informației	70
5.3.4.	Controale de securitate a rețelei.....	70
5.4.	Înregistrarea evenimentelor și procedurile de auditare	71
5.4.1.	Tipuri de evenimente înregistrate.....	71
5.4.2.	Frecvența analizei jurnalelor de evenimente	72
5.4.3.	Perioada de retenție a jurnalelor de evenimente	72
5.4.4.	Protecția jurnalelor de evenimente.....	72
5.4.5.	Procedurile de backup pentru jurnalele de evenimente.....	73
5.4.6.	Notificarea entităților responsabile de tratarea evenimentelor	73
5.4.7.	Analiza vulnerabilităților.....	73
5.5.	Arhivarea înregistrărilor.....	73
5.5.1.	Tipurile de date arhivate	74

5.5.2. Frecvența arhivării datelor	74
5.5.3. Perioada de păstrare a arhivelor	74
5.5.4. Cerințele pentru marcarea temporală a înregistrărilor	75
5.5.5. Procedurile de acces și verificarea informațiilor arhivate	75
5.6. Procedura de backup și restaurare	75
5.7. Compromiterea securității cheii și recuperarea în caz de dezastru	75
5.7.1. Compromiterea resurselor de calcul, a aplicațiilor software și/sau datelor	76
5.7.2. Compromiterea sau suspiciunea compromiterii cheii private a unei Autorități de Certificare ..	76
6. Profilele certificatelor, a listei de revocare a certificatelor și a protocolului de verificare on-line a stării certificatului.....	77
6.1. Profilul certificatelor	77
6.1.1. Conținutul certificatului.....	77
6.1.2. Identificatorul algoritmului de semnare.....	80
6.1.3. Câmpul ce conține semnătura electronică	80
6.2. Profilul listei de certificate revocate (CRL).....	80
6.2.1. Extensiile acceptate în intrările din CRL	81
6.3. Profilul răspunsului de confirmare OCSP	82
6.3.1. Numărul versiunii	82
6.3.2. Informațiile despre starea certificatului	82
6.3.3. Extensiile standard acceptate.....	82
7. Managementul Codului de Practici și Proceduri	83
7.1. Procedura de modificare a CPP	83
7.2. Publicarea CPP-ului	83
7.2.1. Documente ce nu se publică în CPP	84

1. Introducere

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

Acest Cod de Practici și Proceduri (CPP) descrie practicile și procedurile de lucru utilizate de AlfaTrust Certification, în calitate de Prestator de servicii de încredere calificat ("FSC") în furnizarea serviciilor de încredere calificate, respectiv emiterea, administrarea, suspendarea, revocarea și reînnoirea certificatelor digitale calificate pentru semnătura și sigiliul electronic, precum și furnizarea de mărci temporale calificate, în conformitate cu prevederile reglementărilor legale în materie, cu precădere cele prevăzute în:

- **Regulamentul (UE) nr. 910/2014** al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă (Regulamentul eIDAS) **Legea 214/2024** - privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea
- **Ordinul ADR nr. 449/2017** privind procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat
- **Standardele europene aplicabile ETSI EN 319 401, 319 411-1 și 319 421**, precum și alte norme tehnice în vigoare
- **Norma din 2021 privind reglementarea, recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanță utilizând mijloace video**, aprobată prin Decizia Președintelui ADR cu nr. 564/2021

Acest Cod de Practici și 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 și oricărui AC-uri, AÎ-uri sau AV-uri aflate în relație de subordonate sau aflate în relație contractuală cu S.C. AlfaTrust Certification S.A.

Pe tot parcursul acestui document, în cazul în care nu este specificat altfel, noțiunea de certificat calificat va face referire și la sigiliu calificat.

1.1. Rolul Codului de Practici și Proceduri

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

- Îndatoririle autorității de certificare, ale autorității de înregistrare precum și ale utilizatorilor de certificate digitale, în special în cazul certificatelor calificate și a sigiliilor calificate;
- Problemele legale referitoare la serviciile de certificare oferite de compania AlfaTrust Certification S.A.;
- Revizuirea practicilor de securitate și audit la care se supune compania AlfaTrust Certification S.A.;
- Metodele folosite pentru a confirma identitatea solicitanților certificatului/sigiliului;
- Procedurile operaționale pentru serviciile de certificare, realizate de S.C. AlfaTrust Certification S.A.; solicitări cu privire la emiterea, aprobarea, revocarea și reînnoirea certificatelor/sigiliilor;

- Procedurile de securitate operațională pentru înregistrările de verificare, reținerea rapoartelor și recuperarea după dezastru utilizate în cadrul S.C. AlfaTrust Certification S.A.;
- Practicile de securitate fizică, de personal, de management al cheilor și de securitate logică ale S.C. AlfaTrust Certification S.A.;
- Lista de certificate emise, precum și lista de certificate revocate deținute de S.C. AlfaTrust Certification S.A.;
- Administrarea CPP-ului, inclusiv metode de îmbunătățire.

1.1.1. Rezumatul politicii de certificare

AlfaTrust Certification S.A. oferă certificate/sigilii (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 și criptare (schimbul de chei simetrice).

Certificatele calificate AlfaTrust Certification™ pot fi utilizate pentru autentificare, semnătură electronică (bazată pe certificat avansat sau calificat), criptare, autentificare servere Web, semnare de cod, pentru gateway-uri VPN, toate împreună sau separat (în funcție de serviciul ales de beneficiar) ca dovadă a identității în orice tip de tranzacții electronice.

Sigiliile calificate AlfaTrust Certification™ pot fi utilizate pentru semnătură electronică, semnatura electronica extinsa si autentificare.

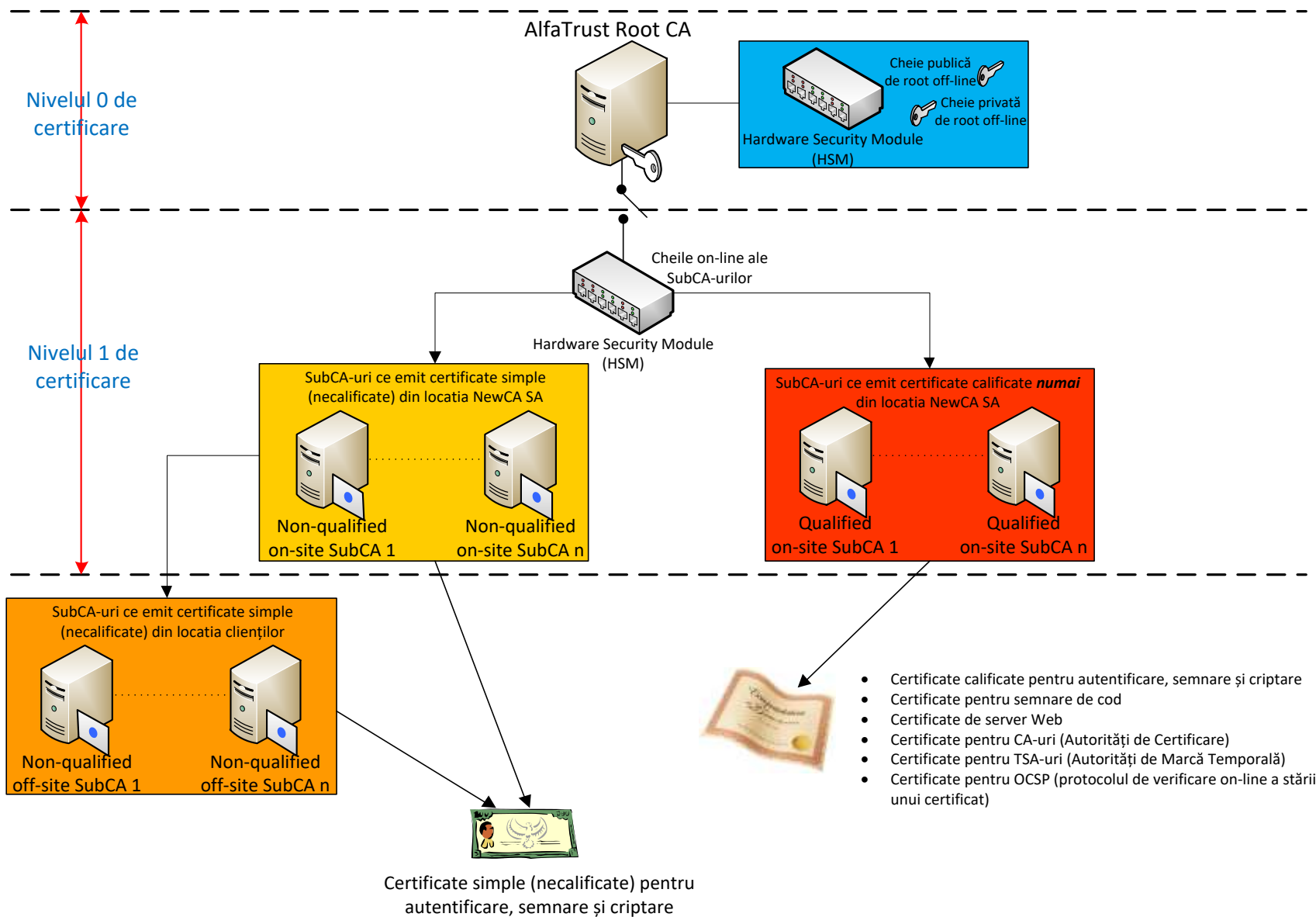
Certificatele asigură identificarea utilizatorului, identificarea realizându-se în principal și în mod tradițional pe baza prezenței fizice a acestuia în fața unei unui reprezentant al AlfaTrust Certification S.A. care îi confirmă identitatea, dar și prin alte forme de de identificare prevăzute de legisție și aprobate de Autoritatea de Supraveghere (ADR), precum, identificare persoanei la distanță utilizând mijloace video.

1.2. Privire de ansamblu asupra infrastructurii de certificare

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

Nivelul 0 este format din AlfaTrust Certification ROOT CA. Autoritățile 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 și 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.



1.3. Sfera de aplicabilitate

1.3.1. Sfera de aplicabilitate a prezentului CPP

Acest CPP se adresează tuturor participanților, incluzând AlfaTrust Certification S.A., distribuitori, utilizatori finali persoane fizice sau juridice, entități partenere și alte părți 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 aplicații de mare securitate care sunt descrise în prezentul CPP.

Certificatele/sigiliile calificate AlfaTrust Certification™ destinate utilizatorilor permit terților (entităților partenere), participanți în procesul de comunicare electronică să verifice semnăturile digitale bazate pe certificatele/sigiliile emise de AlfaTrust Certification.

Supusă legilor în vigoare, o semnătură digitală sau o tranzacție interacționând cu certificatul/sigiliul calificat AlfaTrust Certification™ va fi valid indiferent de locul în care certificatul/sigiliul calificat AlfaTrust Certification™ este emis sau de locul unde semnătura digitală a fost creată sau utilizată și indiferent de locul unde AC-ul sau utilizatorul își desfășoară activitatea.

În mod implicit (serviciul uzual pus la dispoziție), certificatele/sigiliile calificate AlfaTrust Certification™ au scopuri generale. Certificatele/sigiliile 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 piață virtuală.

AlfaTrust Certification S.A. sau ceilalți participanți nu sunt responsabili pentru monitorizarea sau impunerea vreunei restricții în aceste medii.

Cu toate acestea, anumite certificate calificate AlfaTrust Certification™ au funcții limitate. De exemplu, certificatele ACP (Autoritățile de Certificare Primare) nu pot fi utilizate pentru alte funcții decât cele de ACP. Mai mult, certificatele pentru client se supun aplicațiilor clientului și 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/sigiliilor emise de AlfaTrust Certification

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

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

Certificatele emise de AlfaTrust Certification pot fi folosite preponderent pentru autentificare utilizatorului, semnătură electronică și criptare, sau la cererea clientului se pot customiza extensiile astfel încât certificatele 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 și Proceduri sunt definite trei nivele de încredere a certificatelor:

- **Certificate pentru semnături electronice simple** - aceste certificate nu sunt reglementate de eIDAS în mod specific și pot fi utilizate în contexte private, dar nu oferă garanții legale explicite. Se folosesc de obicei pentru autentificare sau semnături simple, unde nu este necesar un nivel înalt de securitate..
- **Certificate pentru semnături electronice avansate** -acestea permit crearea de semnături electronice avansate în sensul art. 26 din Regulamentul (UE) nr. 910/2014 (eIDAS). Semnătura avansată trebuie să îndeplinească cumulativ următoarele cerințe:
 - este legală în mod unic de semnatar;
 - permite identificarea semnatarului;
 - este creată utilizând date de creare a semnăturii pe care semnatarul le poate folosi, cu un nivel ridicat de încredere, sub controlul său exclusiv;
 - este legată de datele semnate în așa fel încât orice modificare ulterioară a acestora să fie detectabilă.

Certificatele pentru semnături avansate pot fi utilizate pentru autentificare, semnătură de documente în medii cu risc moderat, validare de tranzacții interne etc. Nu beneficiază însă de recunoaștere automată la nivel UE

- **Certificate calificate pentru semnături electronice sau sigilii electronice**- aceste certificate permit generarea de semnături electronice calificate în sensul art. 3 pct. 12 și art. 25 din Regulamentul eIDAS. Semnătura calificată:
 - a) are același efect juridic ca o semnătură olografă;;
 - b) efectul său juridic este recunoscută automat în toate statele membre UE;
 - c) este creată cu un dispozitiv calificat și pe baza unui certificat calificat emis de un prestator de servicii de încredere calificat și autorizat ca atare..

Aceste certificate se utilizează în medii cu risc ridicat (tranzacții financiare, contracte importante, documente oficiale) și asigură cel mai înalt nivel de încredere și protecție juridică..

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 și fișierelor, sau autentificarea unui utilizator (de exemplu prin protocolul SSL);

2. **certIFICATE AVANSATE** - permit crearea de semnături electronice avansate, în conformitate cu art. 26 din Regulamentul (UE) nr. 910/2014 (eIDAS). Aceste certificate oferă un nivel mai ridicat de securitate decât certificatele simple și pot fi utilizate pentru semnarea documentelor, autentificare și criptare în contexte unde nu este necesar un certificat calificat.
3. **certIFICATE CALIFICATE** – permit autentificarea utilizatorului, criptarea mesajelor și semnarea documentelor, având cea mai înaltă forță juridică probantă;
4. **certIFICATE PENTRU AUTENTIFICAREA SERVERELOR ȘI SCHIMB DE CHEI SIMETRICE** – sunt folosite de serviciile care operează pe baza protocoalelor SSL/TLS/WTLS;
5. **certIFICATE PENTRU SEMNAREA CODULUI** – folosite de programatori pentru a proteja software-ul împotriva falsificării;
6. **certIFICATE PENTRU AUTORITĂȚILE DE CERTIFICARE** – folosirea lor nu este restricționată la aria definită; aria de aplicabilitate poate fi dată de extensia din certificate ce stabilește 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 conține de asemenea și certificatele operaționale ale Autorităților de Certificare;
7. **certIFICATE PENTRU CONFIRMAREA STĂRII UNUI CERTIFICAT** – sunt emise pentru serverele care funcționează conform protocolului OCSP și care furnizează informații despre starea certificatelor;
8. **certIFICATE PENTRU AUTORITĂȚI 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, semnături electronice etc.) un moment de timp pe baza căruia se poate determina secvențialitatea în timp a datelor.

Certificatele emise în concordanță cu politicile de certificare AlfaTrust Certification pot fi folosite în aplicații ce satisfac cel puțin următoarele condiții:

- gestionează corespunzător cheile publice și private,
- certificatele și cheile publice asociate acestora sunt folosite în concordanță 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 și controlul validității (validitatea semnăturii, data expirării etc.),
- oferă utilizatorului informații corespunzătoare despre certificate și starea acestora.

Lista aplicațiilor recomandate este publicată pe site la adresa: <http://www.AlfaSign.ro> .

Aplicațiile sunt incluse în lista aplicațiilor recomandate pe baza unor declarații scrise ale producătorilor și/sau pe baza testelor făcute de AlfaTrust Certification. AlfaTrust Certification permite fiecărui utilizator final să-și 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 și apoi să livreze utilizatorului final dispozitivul împreună cu cheile. În acest caz, AlfaTrust Certification folosește dispozitive criptografice ce satisfac cel puțin cerințele standardului FIPS PUB 140-2.

1.3.3. Autorități de certificare (AC)

Termenul autoritate de certificare cuprinde toate entitățile care emit certificate respectând propriul CPP, care poate fi același pentru fiecare ACP, sau poate diferi de la un ACP la altul, în funcție de scopul ACP-ului.

Termenul “ACP” se referă la o subcategorie de emitenți numite autorități de certificare primare (ACP), care se comportă ca rădăcini (eng. root). Fiecare ACP este o entitate AlfaTrust Certification™. Subordonate ACP-ului sunt autoritățile de certificare, care emit certificate abonaților-utilizatori finali sau altor AC-uri. Toate ACP-urile AlfaTrust Certification™ ce emit certificate calificate sunt găzduite de centrul de procesare propriu, aflat pe teritoriul României, în locațiile strict securizate.

Autoritatea de Certificare AlfaTrust Certification ROOT CA este o Autoritate de Certificare Primară pentru domeniul AlfaTrust Certification. Toate celelalte Autorități 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 și emite certificate numai Autorităților 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 și emitere de certificat de cheie publică (a se vedea și procedurile descrise în subcapitolul 5.1.1.1). Autoritatea AlfaTrust Certification ROOT CA funcționează pe baza unui certificat autosemnat, emis de ea însăși. Într-un astfel de certificat, extensia **certificatePolicies** lipsește (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 atașat.

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

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

- sine (emite și reînnoiește certificate proprii),
- Autoritățile de Certificare înregistrate în domeniul de certificare AlfaTrust Certification,
- entități ce furnizează servicii de verificare on-line a stării certificatelor și ale entităților ce oferă servicii de non-repudiare (de exemplu, servicii de marcare temporală).

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

- utilizatori care vor să-și asigure securitatea și credibilitatea poștei electronice și a altor servicii (de exemplu, comerț electronic, semnarea codului software) prin intermediul certificatelor,
- entități care oferă servicii de marcare temporală,
- furnizori de servicii din domeniul telecomunicațiilor mobile,
- dispozitive de rețea care realizează conexiuni criptate prin VPN,
- utilizatori în vederea oferiții de servicii pe bază de certificate de chei publice cum ar fi serviciul de verificare on-line a stării certificatelor (OCSP),
- alte Autorități de Certificare.

Orice entitate externă care dorește încheierea unui contract pentru operarea unui CA subordonat AlfaTrust Certification va încheia cu AlfaTrust Certification un contract prin care se obligă să respecte versiunile curente ale CPP și să se supună unui audit pentru verificarea conformității cu legislația în vigoare și cu politicile și procedurile AlfaTrust Certification.

1.3.4. Autorități de înregistrare (AÎ)

AI-ul asistă un AC prin îndeplinirea funcțiilor de confirmare a identității, de aprobare sau respingere a cererilor pentru certificat, de cerere a revocării certificatelor și de aprobare sau respingere a cererilor de reînnoire.

Nivelul de precizie al procesului de determinare a identității clientului este dat de nevoile utilizatorului final și 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 prezența în persoană a solicitantului la Autoritatea de Înregistrare și 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 Autorității 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 abonaților-utilizatori finali sunt găzduite în propriile locații 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 și care nu emite certificate altor entități.

O Entitate Parteneră este o entitate care folosește certificatul unui utilizator final pentru a verifica semnatura electronică a acestuia sau pentru a asigura confidențialitatea informațiilor transmise.

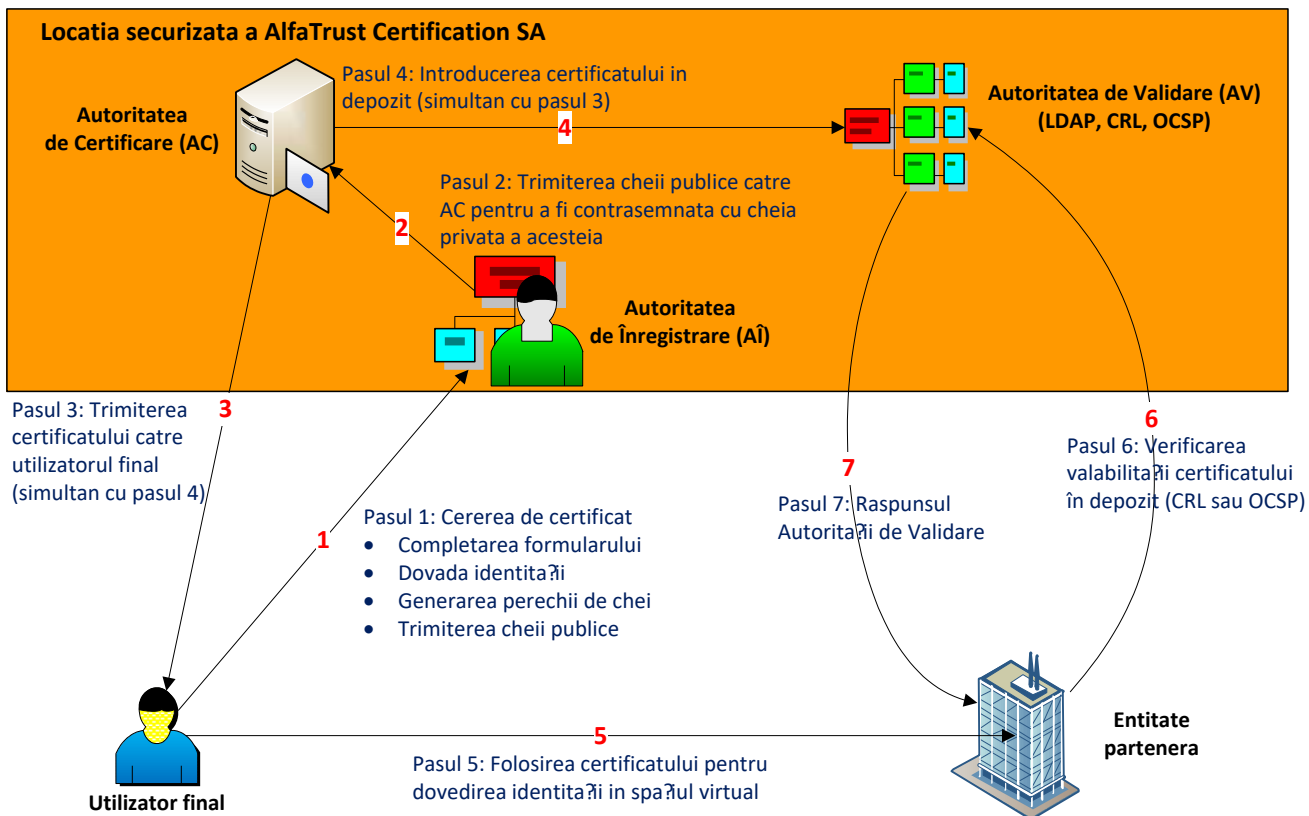
Orice persoană fizică sau juridică, precum și dispozitivele hardware pe care acestea le dețin pot fi utilizatori finali ai serviciilor oferite de AlfaTrust Certification, în condițiile respectării legii. În particular, operatorii Autorității de Înregistrare, ceilalți angajați AlfaTrust Certification și echipamentele indispensabile pentru asigurarea securității infrastructurii AlfaTrust Certification (firewall-uri, routere, servere de autentificare) reprezintă, de asemenea, utilizatori finali.

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

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

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

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



1.4. Detalii de contact

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

S.C. AlfaTrust Certification S.A.

Calea Victoriei 155, bl. D1, tr. 8, etj. 9, sect. 1, București

E-mail: office@AlfaSign.ro

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 și entităților partenere, ambii constituindu-se în părți contractante, obligațiile ambelor părți fiind stipulate clar și fără echivoc în cadrul contractului dintre părți în spiritul prezentului CPP.

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

1. Crearea unui document care să reflecte clar modalitățile de lucru, procedurile aplicabile și aplicate, politica generală a firmei, obligațiile și drepturile părților contractante, etc. - CPP (Codul de Practici și Proceduri) și afișarea lui în mod public (pe Internet) după ce a fost aprobat de persoanele responsabile din cadrul AC-ului;
2. Modul de desfășurare a activității AC-ului să se conformeze strict cu prevederile CPP-ului aprobat;
3. Modalitatea de punere în practică a CPP-ului și a Politicilor de Certificare ale AC-ului să se bazeze pe o infrastructura (de comunicații, software și hardware) fiabilă, capabilă în orice moment de a garanta buna desfășurare a activității AC-ului conform cu politica de funcționare 24x7 impusă nu numai de legile românești în vigoare privind Autoritățile de Certificare ce emit certificate calificate, dar și de realitățile lumii contemporane în ceea ce privește afacerile desfășurate pe Internet;
4. Garantarea faptului că cererile de emiterie de certificate sunt procesate (în sensul identificării persoanei numai pe baza modalităților puse la dispoziție de legile române în vigoare) numai de o AI aflată în legătură contractuală cu AC-ul emitent de certificate (și căruia i se subordonează), și care la rândul ei se conformează cadrului general stabilit de prezentul CPP, în strânsă legătură și 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 obținerii unui certificat digital calificat se desfășoară în litera și spiritul Regulamentului [\(UE\) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date](#) (GDPR);
6. Garantarea faptului că informațiile incluse în certificate sunt valide și conform realității la momentul aprobării certificatului, precum și garantarea menținerii conform Legii 214/2024a actelor ce fac dovada identității persoanelor înregistrate în vederea eliberării certificatului calificat;
7. Garantarea aducerii la cunoștința utilizatorilor a obligațiilor pe care le au în concordanță cu acest CPP, prin prisma faptului că sunt posesori și virtuali utilizatori ai certificatelor digitale calificate, precum și informarea acestora asupra riscului la care se supun prin nerespectarea acestor obligații;
8. Revocarea certificatelor acelor utilizatori în raport de care există indicii și probe rezonabile că au acționat contrar obligațiilor ce revin utilizatorilor, așa cum se desprind ele din acest CPP, cu obligativitatea AC-ului de a anunța utilizatorul despre măsura luată;
9. Serviciile de înregistrare în vederea emiterii de certificate și 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 menține un registru de evidență a certificatelor emise de către toate ACP-urile subordonate, registru ce trebuie actualizat dinamic astfel încât el să reflecte situația la zi a certificatelor emise către abonați;

2.1.2. Obligațiile Autorității de Înregistrare (AÎ)

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

O AI care realizează funcții de înregistrare se va conforma prevederilor acestui CPP aprobat. AC-urile sunt responsabile pentru asigurarea faptului că certificatele sunt generate și administrate în conformitate cu acest CPP și cu Politica de Certificare a AC-ului, și că funcțiile de generare, administrare și retragere a certificatelor sunt realizate numai de cei care înțeleg cerințele politicii de certificare asociate și care sunt de acord să le respecte. Cerințele de securitate impuse AC-urilor sunt asemănătoare celor impuse oricărui AI-uri datorită faptului că AI-urile sunt responsabile pentru informația colectată. AI este responsabilă 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 și/sau certificate către abonați;
6. Trimiterea de cereri către AC pentru eliberarea, revocarea sau reînnoirea certificatelor;
7. Verificarea prealabilă a datelor furnizate de abonați pentru aceste cereri, conform cerințelor din CPP;
8. Asigurarea faptului că PIN-ul și cheia privată ce urmează să se distribuie către abonat nu sunt interceptate de către terțe părți;
9. Transmiterea unui contract („Acordul Părților”) ce urmează a fi semnat, către fiecare utilizator ce urmează a fi deținătorul 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,
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 și 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 aparțin utilizatorilor finali înscrși în certificate, iar utilizatorii și-au dat acordul asupra acestor certificate,

- * să se asigure că certificatele Autorităților de Certificare aparținând domeniului AlfaTrust Certification precum și certificatele utilizatorilor (după aprobarea lor) sunt publicate și arhivate la timp,
- * să asigure publicarea și arhivarea Politicii de Certificare, a Codului de Practici și Proceduri, a listei aplicațiilor și dispozitivelor recomandate,
- * să permită accesul la informațiile despre starea certificatelor prin publicarea de Liste de Certificate Revocate (CRL), prin intermediul serverelor OCSP sau prin interogări HTTP,
- * să asigure accesul permanent la informațiile din depozit pentru Autoritățile de Certificare, Autoritatea de Înregistrare, utilizatori finali și Entitățile Partenere,
- * să publice CRL-urile sau alte informații în timp util și în concordanță cu termenele limită specificate în Politica de Certificare,
- * să asigure accesul sigur și controlat la informațiile din depozit.

2.1.4. Obligațiile utilizatorului final

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

În funcție de relațiile dintre AlfaTrust Certification și un abonat și de nivelul de credibilitate al certificatului solicitat de utilizator, obligațiile pot fi formulate sub forma unui contract între abonat și AlfaTrust Certification.

Prin contract, utilizatorul final se angajează:

- * să fie de acord cu termenii contractului;
- * să probeze fiecare certificat emis pentru el; garanțiile și obligațiile 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 însuși sau de către Autoritatea de Înregistrare) și să stocheze în siguranță cheia privată din cadrul unei perechi de chei (pentru a preveni pierderea, compromiterea, modificarea și folosirea neautorizată a acesteia);
- * să folosească dispozitivele și aplicațiile software recomandate de AlfaTrust Certification în cazul în care utilizatorul își generează singur cheile;
- * să declare date corecte în aplicațiile trimise Autorității de Înregistrare care apoi sunt stocate în baza de date a AlfaTrust Certification și în certificate de chei publice emise; un utilizator trebuie să fie conștient de responsabilitățile ce îi revin pentru daunele directe și indirecte provocate ca urmare a falsificării datelor;
- * să accepte faptul că fiecare semnătură electronică creată prin intermediul unei chei private, aparținând utilizatorului și asociată unui certificat aprobat care conține cheia publică corespunzătoare, reprezintă semnatura utilizatorului și să recunoască faptul că certificatul nu a fost invalid (în afara datei de valabilitate) și nici revocat sau suspendat atunci când a fost creată semnatura;

- * să cunoască în general noțiunile referitoare la certificate, semnături electronice și PKI.

De asemenea, utilizatorul final se angajează:

- să se supună regulilor din prezentul Cod de Practici și Proceduri și Politica de Certificare,
- să genereze cheile criptografice, să gestioneze parolele, cheile publice și private, să schimbe informații cu Autoritatea de Înregistrare și Autoritățile de Validare numai prin intermediul aplicațiilor software recomandate de către AlfaTrust Certification; accesul la acest software, mediile și dispozitivele pe care sunt stocate cheile și 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 Autorității de Înregistrare documentele cerute care să confirme informațiile incluse în aplicația trimisă și identitatea celui ce a transmis cererea sau a entității ce acționează în numele utilizatorului,
- în cazul în care se constată încălcarea securității (sau există suspiciunea de încălcare a securității) cheilor private, să anunțe emitentul certificatului ,
- să folosească certificatele de chei publice și cheile private corespunzătoare numai în scopurile declarate în certificat și în concordanță cu ariile de aplicabilitate și restricțiile stabilite prin Codul de Practici și Proceduri,
- să obțină certificate de chei publice ale Autorităților de Certificare și Autorității de Înregistrare precum și cele corespunzătoare altor servicii oferite de AlfaTrust Certification.

2.1.5. **Obligațiile entităților partenere**

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

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

În funcție de relațiile dintre o entitate parteneră și AlfaTrust Certification sau un abonat și de nivelele certificatelor acceptate de o entitate parteneră, obligațiile entităților partenere sunt stabilite în cadrul unui contract încheiat între AlfaTrust Certification și entitatea parteneră.

Prin contract, Entitatea Parteneră se angajează:

- * să fie de acord și să respecte termenii și condițiile din contract. Drepturile și obligațiile părților încep să își producă efectele începând cu data încheierii contractului.
- * să verifice cu atenție fiecare semnătură electronică de pe un certificat sau document recepționat. Pentru a verifica semnatura, entitatea parteneră trebuie:
 - i. să specifice calea de certificare ce conține toate certificatele Autorităților de Certificare care fac posibilă verificarea semnăturii 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) și până la o Autoritate de Certificare pe care se bazează verificarea semnăturii,
 - iii. să verifice că nici unul din certificatele din calea de certificare, aparținând AlfaTrust Certification, nu se află în listele de certificate revocate sau suspendate,
 - iv. să verifice că toate certificatele din calea de certificare aparțin unor Autorități de Certificare și că acestea sunt autorizate să semneze alte certificate,
 - v. (opțional) să specifice data și 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 semnăturii electronice i s-a asociat o marcă temporală imediat după semnarea documentului; o astfel de verificare permite implementarea de servicii de non-repudiare sau se poate folosi pentru rezolvarea disputelor,
 - vi. să verifice, folosind o cale de certificare definită, credibilitatea certificatului semnatarului documentului sau mesajului și autenticitatea semnăturii,
- * să efectueze corect operațiile criptografice, folosind aplicații software și dispozitive având un nivel de securitate corespunzător nivelului de sensibilitate al certificatului procesat și nivelului de credibilitate al certificatelor folosite,
- * să considere o semnătură 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 își 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 și
 - 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 concordanță cu scopul declarat și corespund ariilor de aplicabilitate specificate de entitatea parteneră, de exemplu, printr-o politică de semnătură,
 - 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 condițiile pe care un certificat de cheie publică și o semnătură electronică trebuie să le îndeplinească pentru a fi considerate valide; aceste condiții pot fi formulate, de exemplu, sub forma unor politici de certificare acceptate și apoi publicate.

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

Entitatea parteneră trebuie să ia la cunoștință prevederile Codului de Practici și Proceduri și Politica de Certificare (garanții și responsabilități).

2.2. Responsabilitate

2.2.1. Responsabilitatea Prestatorului de Servicii de Încredere (FSC)

Răspunderea AlfaTrust Certification S.A. ca prestator de servicii de încredere calificat este reglementată de lege în sensul că, în art. 27 alin. (2) din Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea, se prevede că prestatorii de servicii de încredere răspund pentru prejudiciile cauzate oricărei persoane fizice sau juridice ca urmare a nerespectării prevederilor Regulamentului (UE) nr. 910/2014 și ale prezentei legi, de către terții de verificare a identității care îi deservesc:

- a) în ceea ce privește exactitatea, în momentul eliberării certificatului, a tuturor informațiilor pe care le conține;
- b) în ceea ce privește asigurarea că, în momentul eliberării certificatului, semnatarul identificat în cuprinsul acestuia deține datele de generare a semnăturii corespunzătoare datelor de verificare a semnăturii menționate în respectivul certificat;
- c) în ceea ce privește asigurarea că datele de generare a semnăturii corespund datelor de verificare a semnăturii, în cazul în care prestatorului de servicii de încredere le generează pe amândouă;
- d) în ceea ce privește revocarea certificatului, în cazurile și cu respectarea condițiilor prevăzute la art. 17 din Legea 214/2024;
- e) în privința îndeplinirii tuturor obligațiilor prevăzute la art. 11 și 12 din Legea 214/2024, cu excepția cazurilor în care prestatorul de servicii de încredere probează că, deși a depus diligența necesară, nu a putut împiedica producerea prejudiciului.

De asemenea, AlfaTrust Certification S.A. ca prestator de servicii de încredere poate să indice în cuprinsul unui certificat calificat restricții ale utilizării acestuia, precum și limite ale valorii operațiunilor pentru care acesta poate fi utilizat, cu condiția ca respectivele restricții să poată fi cunoscute de terți.

AlfaTrust Certification S.A. ca prestator de servicii de încredere nu va fi răspunzătoare pentru prejudiciile rezultând din utilizarea unui certificat calificat cu încălcarea restricțiilor prevăzute în cuprinsul acestuia (art. 15 alin. (2) teza a II -a din Legea nr. 214/2024).

Garanțiile și limitele responsabilității dintre o AI și AC care asistă emiterea certificatelor pe de o parte, și utilizatorul respectiv, pe de altă parte, se supun și sunt guvernate de către acordurile dintre aceștia cu respectarea legilor în vigoare.

1.2.1.1. *Garanțiile Furnizorului de Servicii de Certificare*

AlfaTrust Certification S.A. ca furnizor de servicii de încredere calificat, dispune de resurse financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul prestării serviciilor de încredere. În acest sens, asigurarea s-a realizat prin subscrierea unei polițe de asigurare la o societate de asigurări.

Suma asigurată este conform celei stipulate de către Ministerul Comunicațiilor și Societății Informaționale, în calitate de autoritate de reglementare și supraveghere specializată în domeniu. (art. 12 alin. (6) din Legea nr. 214/2024).

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

- Nu există interpretări greșite ale entităților care aprobă cererile pentru certificat sau care emit certificatul,
- Nu există erori privind informațiile referitoare la certificat, făcute de entitățile care răspund de aprobarea cererii pentru certificat, aceleași care răspund și de emiterea certificatului,
- Certificatele utilizatorilor satisfac toate cerințele acestui CPP,
- Serviciile de revocare și utilizarea depozitului (sau registrului) conform cu acest CPP în toate aspectele importante.

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

- Toate informațiile din sau incorporate într-un astfel de certificat sunt precise;
- În cazul certificatelor apărute în registrul AlfaTrust Certification S.A., certificatul a fost emis pentru o persoană fizică sau companie și utilizatorul a acceptat certificatul în concordanță cu specificațiile prezentului CPP;
- Entitățile care aprobă cererile pentru certificat și emit certificate au respectat acest CPP atunci când au emis certificatele.

1.2.1.2. Forța majoră

În măsura limitelor legale, serviciile AlfaTrust Certification S.A. și acordurile părților contractante includ o clauză de forță majoră care protejează părțile.

2.2.2. Responsabilitatea utilizatorului

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

- * Fiecare semnătura digitală creată prin utilizarea cheii private corespunzătoare cheii publice din certificat este semnătura digitală a utilizatorului și că certificatul a fost acceptat și este operațional (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 informațiile furnizate de utilizator și conținute de certificat sunt adevărate;
- * Certificatul este folosit exclusiv pentru scopul declarat, în concordanță cu CPP;
- * Utilizatorul este un utilizator final, nu un AC și nu folosește 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 obligați 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 cunoștința unui terț neautorizat;
- informațiile esențiale cuprinse în certificat nu mai corespund realității.

2.2.3. Responsabilitatea părților contractante

Părțile contractante admit că au informații suficiente pentru a lua o decizie în măsura în care au ales să se bazeze pe informațiile dintr-un certificat, că sunt singurii responsabili pentru decizia de a se baza sau nu pe astfel de informații, și că vor suporta consecințele legale în cazul nerespectării obligațiilor de către părți, conform capitolului 2.1.5. din prezentul CPP.

2.3. Responsabilități financiare

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

1. Furnizarea de informații false/eronate în cererea pentru certificate;
2. Furnizarea eronată a unei informații importante în cererea pentru certificat, dacă relatarea eronată sau omisiunea a fost făcută din neglijență sau cu intenția de a înșela una dintre părți;
3. Neprotejarea cheii private sau neluarea măsurilor de protecție 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 terț.

AlfaTrust Certification S.A. va acoperi prejudiciile pe care le-ar putea cauza cu prilejul desfășurării activității de certificare persoanelor care își întemeiază conduita pe efectele juridice ale certificatelor calificate, până la concurența 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 obligații prevăzute de lege.

2.4. Legea aplicabilă și soluționarea litigiilor

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

În situația apariției unei neînțelegeri între părțile contractante, acestea vor încerca soluționarea acestora în termen de 30 de zile de la notificarea transmisă de către o parte către cealaltă parte (perioadă de negociere inițială) și, în cazul în care părțile nu ajung la o soluție acceptată de comun acord, acestea se pot adresa instanței de judecată competente.

2.5. Prețul serviciilor prestate

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

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

- a) **servicii de încredere individuale** – prețul este stabilit pentru fiecare serviciu în parte, de exemplu, pentru fiecare certificat vândut sau un număr mic de certificate,
- b) **pachete de servicii de încredere** – prețul este stabilit pentru pachete de servicii prestate unei singure entități,
- c) **servicii prestate pe baza de abonament** – prețul este stabilit pentru servicii prestate lunar; valoarea sumelor plătite depinde de tipul și numărul serviciilor accesate și este utilizat în special (dar nelimitându-se la acestea) pentru serviciile de marcare temporală și de verificare a stării certificatelor prin intermediul protocolului OCSP,
- d) **servicii indirecte** – prețul este stabilit pentru fiecare serviciu oferit clienților săi de un partener AlfaTrust Certification S.A., care își 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 preț pentru fiecare certificat emis de Autoritatea de Certificare respectivă.

Plățile se vor face în numerar, prin ordin de plată, inclusiv folosind carduri bancare pe baza de factură, conform reglementărilor legale în vigoare.

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

- * vânzarea de dispozitive criptografice de orice tip, în funcție de nevoile utilizatorului,
- * generarea cheilor pentru Autoritățile de Certificare sau utilizatori,
- * testarea aplicațiilor și includerea lor în lista aplicațiilor recomandate,
- * vânzarea de licențe,
- * activități de proiectare, implementare și instalare,
- * activități de consultanță și audit în domeniul securității informației,
- * vânzarea de copii tipărite ale Codului de Practici și 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 mulțumită de serviciile oferite, pot solicita revocarea certificatului și rambursarea sumelor plătite în 30 de zile de la data emiterii certificatului. După această perioadă, utilizatorul are dreptul de a solicita revocarea certificatului și rambursarea sumelor aferente perioadei rămase până la expirarea certificatului dacă AlfaTrust Certification S.A. nu-și îndeplinește obligațiile și îndatoririle specificate în Codul de Practici și 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 interfață publică către următoarele informații:

- * versiunea curentă și cea anterioară a Politicii de Certificare și a Codului de Practici și Proceduri,

- * Modelele de contract cu utilizatorii finali și Entitățile Partenerere,
- * Declarația AlfaTrust Certification S.A. cu privire la asigurarea confidențialității informațiilor recepționate și procesate,
- * Registrul electronic de evidență a certificatelor disponibil permanent pentru consultare, inclusiv în regim on-line (în accepțiunea art. 14 din Legea 214/2024) care face mențiuni despre:
 - data și ora exactă la care certificatul a fost eliberat;
 - data și ora exactă la care expiră certificatul;
 - dacă este cazul, data și ora exactă la care certificatul a fost suspendat sau revocat, inclusiv cauzele care au condus la suspendare sau la revocare.
- * certificatul AlfaTrust Certification ROOT CA, precum și certificatele tuturor Autorităților de Certificare care aparțin sau sunt legate la domeniul AlfaTrust Certification,
- * certificatele utilizatorilor finali (entități fizice și juridice, inclusiv angajații AlfaTrust Certification S.A. și mașinile / aplicațiile software deținute de aceștia și care sunt indispensabile pentru serviciile PKI) conform Legii 214/2024.

În plus, în Depozit se găsesc informații legate de funcționarea certificatelor, cum ar fi:

- * Listele de certificate Revocate (CRL); CRL-urile sunt disponibile în așa numitele puncte de distribuție a CRL-urilor, a căror adresă este specificată în fiecare certificat emis de AlfaTrust Certification; locația principală de distribuție a CRL-urilor este în depozit la adresa: <http://www.AlfaSign.ro>,
- * Alte informații ce se modifică frecvent sau în timp real,

Conținutul depozitului este disponibil prin Internet la adresa: <http://www.AlfaSign.ro/depozit>

2.6.2. Frecvența publicării

Informațiile publicate de AlfaTrust Certification sunt actualizate cu următoarea frecvență:

- Politica de Certificare și Codul de Practici și Proceduri – la aprobarea inițială și ori de câte ori se modifică,
- certificatele Autorităților de Certificare din cadrul AlfaTrust Certification – după emiterea unui nou certificat,
- certificatul Autorității de Înregistrare – după emiterea unui nou certificat,
- certificatele Abonaților – după fiecare emiteră a unui nou certificat,
- Lista certificatelor Revocate – vezi Capitolul “frecvența de emiteră a CRL-ului”,
- Rapoartele de audit efectuate de instituțiile autorizate – în momentul în care AlfaTrust Certification intră în posesia lor,
- Informațiile suplimentare – după fiecare actualizare.

2.6.3. Controlul accesului la informații

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

AlfaTrust Certification a implementat mecanisme logice și fizice de protecție împotriva adăugării, ștergerii și modificării informațiilor publicate în depozit.

În momentul descoperirii unor breșe ce afectează integritatea informațiilor din depozit, AlfaTrust Certification va lua măsurile corespunzătoare pentru a restabili integritatea informațiilor, va trage la răspundere pe cei vinovați și va notifica entitățile afectate.

2.7. Auditul de conformitate

Auditurile au ca obiectiv verificarea consistenței acțiunilor AlfaTrust Certification sau a entităților delegate de aceasta cu declarațiile și procedurile acestora (inclusiv Politica de Certificare și Codul de Practici și Proceduri).

Auditurile desfășurate de AlfaTrust Certification urmăresc în principal centrele de procesare a datelor și procedurile de gestiune a cheilor. De asemenea, aceste audituri au în vedere și Autoritățile 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 desfășurate de AlfaTrust Certification pot fi efectuate de echipe interne (audit intern) sau de organizații independente (audit extern). În ambele cazuri, auditul se desfășoară la cererea și sub supravegherea administratorului de securitate.

2.7.1. Frecvența auditului de conformitate

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

2.7.2. Identitatea/calificarea auditorului

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

- * angajeze personal având cunoștințe și experiență tehnică corespunzătoare (să dispună de documente care să certifice acest lucru) în domeniul infrastructurilor de chei publice, tehnologiilor și dispozitivelor de securitate informatică și de auditare a securității sistemelor,
- * fie organizație sau societate înregistrată și de renume.

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

2.7.3. Ariile supuse

Auditurile interne și externe se desfășoară conform regulilor și procedurilor acceptate pe plan internațional pentru Autoritățile de Certificare și vizează:

- securitatea fizică a AlfaTrust Certification,
- procedurile de verificare a identității utilizatorilor,
- serviciile de încredere și procedurile de furnizare a serviciilor,
- securitatea aplicațiilor software și a accesului la rețea,
- securitatea personalului AlfaTrust Certification,
- jurnalele de evenimente și procedurile de monitorizare a sistemului,
- arhivarea și restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru CA-uri,
- înregistrările referitoare la analizele și verificările efectuate pentru aplicațiile software și dispozitivele hardware.

2.7.4. Acțiuni acceptate ca rezultat al neconformităților

Rezultatele auditurilor interne și 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 neconformitățile sesizate și va propune un plan de acțiune și termene de rezolvare, pentru închiderea neconformităților. Informațiile referitoare la modul de închidere a neconformităților vor fi trimise auditorului.

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

2.8. Confidențialitate

Toate informațiile pe care le deține AlfaTrust Certification S.A. au fost obținute, păstrate și procesate în concordanță cu legile în vigoare, în mod special cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și cu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice. Relațiile dintre un utilizator, o entitate parteneră și AlfaTrust Certification se bazează pe încredere.

O terță parte poate avea acces doar la informațiile disponibile public în certificate. Celelalte date furnizate în aplicațiile trimise către AlfaTrust Certification nu vor fi dezvăluite în nici o circumstanță vreunei terțe părți, în mod voluntar sau intenționat (cu excepția situațiilor prevăzute de lege).

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

1. cererilor de generare și 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 informații confidențiale, dacă:

- a) informația era cunoscută părții contractante înainte ca ea să fi fost primită de la cealaltă parte contractantă;

sau

- b) informația a fost dezvăluită după ce a fost obținut acordul scris al celeilalte părți pentru asemenea dezvăluire;

sau

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

Dezvăluirea oricărei informații față de persoanele implicate în îndeplinirea obligațiilor, se va face confidențial și se va extinde numai asupra acelor informații necesare în vederea îndeplinirii obligațiilor.

2.8.1. Tipuri de informații confidențiale

AlfaTrust Certification S.A., angajații acesteia precum și entitățile afiliate care participă în procesul de furnizare a serviciilor de încredere sunt obligate să păstreze secretul informațiilor, atât pe durata, cât și după încetarea contractului de muncă, în cazul angajaților.

Sunt catalogate drept informații private sau confidențiale:

- * informațiile furnizate de utilizatori, în plus față de informațiile ce trebuie transmise reevaluate pentru efectuarea serviciilor de încredere; în celelalte cazuri, dezvăluirea informațiilor primite necesită în prealabil o aprobare scrisă din partea proprietarului informației sau în alte condiții prevăzute de lege,
- * informațiile furnizate de, sau către utilizatori (de exemplu, conținutul contractelor încheiate cu utilizatorii finali sau Entitățile Partenere, conturi bancare, aplicațiile de înregistrare, emitere, reînnoire, revocare certificate – cu excepția informațiilor incluse în certificate sau din depozit, conform prezentului Cod de Practici și Proceduri); o parte din informațiile menționate mai sus poate fi dezvăluită doar cu aprobarea și în scopul menționat de proprietarul informațiilor (de exemplu, utilizatorul),
- * înregistrările corespunzătoare tranzacțiilor din sistem (toate tipurile de tranzacții, precum și datele pentru controlul tranzacțiilor, așa numitele loguri ale tranzacțiilor din sistem),
- * înregistrările corespunzătoare evenimentelor (loguri) ce țin de serviciile de încredere, păstrate de către AlfaTrust Certification,
- * rezultatele auditurilor interne și externe, dacă acestea reprezintă o amenințare pentru securitatea AlfaTrust Certification,
- * planurile în caz de urgență,

- * informațiile referitoare la măsurile luate pentru protecția dispozitivelor hardware și aplicațiilor software, informațiile referitoare la modul de administrare a serviciilor de încredere și a regulilor de înregistrare planificate.

Obligația de confidențialitate nu se răsfrânge și asupra faptului că AlfaTrust Certification a oferit servicii de încredere unei părți. Persoanele responsabile de păstrarea confidențialității informațiilor și care se supun regulilor referitoare la modul de gestiune a informațiilor poartă răspunderea penală conform legislației în vigoare.

2.9. Drepturi de proprietate intelectuală

Toate mărcile, patentele, siglele, licențele, imaginile grafice etc. folosite de către AlfaTrust Certification S.A. sunt și vor rămâne proprietatea intelectuală a deținătorilor legali ai acestora. AlfaTrust Certification S.A. se obligă să specifice acest lucru conform cerințelor impuse de deținători.

Toate mărcile, patentele, siglele, licențele, imaginile grafice etc., aparținând AlfaTrust Certification S.A. sunt și rămân proprietatea acesteia, indiferent dacă sunt însoțite sau nu de patente, modele de utilitate, copyright sau altele asemenea și nu pot fi reproduse sau furnizate unei terțe părți 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 excepția certificatelor utilizatorilor persoane juridice, caz în care proprietarul este persoană juridică.

3. Identificare și autentificare

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

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

3.1. Înregistrarea inițială

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

Înregistrarea presupune un număr de proceduri care permit unei Autorități 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 dispoziție de un utilizator, acesta este inclus pe lista utilizatorilor autorizați ai serviciilor AlfaTrust Certification și i se acordă un certificat de cheie publică.

Fiecare utilizator care solicită servicii specifice infrastructurilor de chei publice și 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 și să furnizeze Autorității de Înregistrare dovada deținerii unei chei private; opțional, 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 și să trimită un formular de înregistrare care conține o cheie publică și dovada posesiei cheii private corespunzătoare acesteia,
- să se prezinte, opțional, la Autoritatea de Înregistrare și 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 Autorității de Înregistrare în legătură cu furnizarea serviciilor de către AlfaTrust Certification; prezentul Cod de Practici și 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 poștă, e-mail, site-uri Web etc.

3.1.1. Tipuri de nume

CertIFICATELE emise de AlfaTrust Certification respectă standardul X.509 v3. Aceasta înseamnă că emitentul de certificate și Autoritatea de Înregistrare care acționează în numele emitentului aprobă numele utilizatorului, conform standardului X.509 (cu referire la recomandările seriei X.500). Numele de bază ale utilizatorilor și ale emitenților de certificate plasați în certificatele AlfaTrust Certification sunt în concordanță cu Numele Distinctive – ND – (cunoscute și ca nume directoare), create respectând recomandările X.500 și 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 și DNS simultan. Această opțiune 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 conțină adresa de e-mail a utilizatorului, în concordanță cu recomandările RFC 822.

Numele directoarelor unde sunt reținute certificatele, CRL-urile și Politica de Certificare, ca și numele punctelor de distribuție 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 și verificat de o Autoritate de Înregistrare, depinde de tipul utilizatorului.

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

- **câmpul C** – abrevierea internațională pentru numele țării (RO pentru România),
- **câmpul S** – județul / sectorul în care locuiește utilizatorul,
- **câmpul L** – orașul 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 instituției 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** – funcția utilizatorului,
- **câmpul SN** – numele de familie al utilizatorului,
- **câmpul G** – prenumele utilizatorului,
- **câmpul P** – pseudonimul utilizatorului pe care acesta îl folosește în mediul său, sau pe care dorește să îl folosească pentru a nu-și 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 semnăturii electronice.

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

- **câmpul C** – abrevierea internațională pentru numele țării (RO pentru România),
- **câmpul O** – numele instituției,
- **câmpul OU** – numele departamentului organizației,
- **câmpul S** – județul / sectorul în care funcționează organizația,
- **câmpul L** – orașul în care utilizatorul locuiește sau are domiciliu,
- **câmpul CN** – numele instituției,
- **câmpul Phone** – numărul de telefon,

Numele utilizatorului trebuie confirmat de un operator al Autorității de Înregistrare și 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 concordanță cu profilele de certificate descrise în Profilul certificatelor și al CRL-urilor (Capitolul 6). În crearea și interpretarea ND-ului se face apel la recomandările specificate în subcapitolul 3.1.2.

Identificarea fiecărui deținător 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 concordanță cu cerințele generale specificate în subcapitolul 3.1.1 și 3.1.2, un operator al Autorității de Înregistrare acceptă temporar sugestia. Dacă operatorul Autorității de Înregistrare are acces la baza de date cu ND-uri, acesta va verifica și 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 Autorității de Certificare.

Dacă un ND sugerat de utilizator încalcă drepturile altor entități 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 îndreptățit 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 Autoritățile de Certificare și numele utilizatorului este ND-ul câmpului *Subject* din certificat.

Valorile ultimelor două câmpuri sunt extrase din certificat.

Dacă un utilizator renunță 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 aparțin unui utilizator nu pot fi folosite în cererile sale de certificat. AlfaTrust Certification nu verifică dacă un utilizator este îndreptățit să folosească numele menționat în cererea de înregistrare și nici nu intenționează să-și 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 îndreptățită să respingă sau să suspende cererea unui utilizator fără a-și asuma vreo responsabilitate în acest sens. AlfaTrust Certification este de asemenea îndreptățită să ia toate deciziile cu privire la sintaxa numelui unui utilizator și 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 deține o cheie privată când cere emiterea unui certificat, Autoritățile de Certificare și Autoritatea de Înregistrare care funcționează în cadrul AlfaTrust Certification se vor asigura că entitatea deține o cheie privată corespunzătoare cheii publice furnizate.

Verificarea posesiei cheii private se face pe baza așa 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 deținută în mod exclusiv de utilizator.

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

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

Cerința 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 deține un token la momentul generării și importului cheii, sau token-ul poate fi furnizat entității după procesul de generare de cheie. În ultimul caz, AlfaTrust Certification garantează că token-ul și cheia vor ajunge în mod sigur, direct la entitatea respectivă (vezi subapitolul 5.1.1.1.2).

3.1.6. Autentificarea identității persoanelor juridice

Autentificarea identității unei persoane juridice se realizează pentru a dovedi că, la momentul procesării cererii, persoana juridică stipulată în cerere există; de asemenea, este necesar să se dovedească că o persoană fizică solicitantă a unui certificat în numele societății, sau care-l primește este autorizată de către această persoană juridică să o reprezinte.

Procedurile de autentificare a identității persoanelor juridice sunt inițiate dacă entitatea:

- se comportă ca un utilizator și însărcinează o Autoritate de Certificare cu orice serviciu de încredere,
- cere emiterea unui certificat pentru un dispozitiv hardware sau pentru o aplicație (software) deținută de această entitate,
- se comportă ca o entitate care cere includerea sa în lista Autorităților de Certificare din subordinea AlfaTrust Certification,
- dorește să presteze alte servicii de încredere, cum ar fi: Autoritate de Marcă Temporală, OCSP etc.

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

Reprezentanții autorizați ai instituției, indiferent de nivelul certificatului pe care îl cer, sunt obligați să prezinte, la cererea unui reprezentant al Autorității de Înregistrare, următoarele documente:

- * copie certificată „conform cu originalul” după certificatul de înmatriculare al societății;
- * copie factura de utilități (telefonie, altele) emisă pe numele societății;
- * documente care să confirme identitatea solicitantului (cartea de identitate sau pașaportul) și autorizația prin care reprezintă compania;
- * cerere de achiziție;
- * declarație tip a titularului de domeniu (în cazul certificatelor WEB, când solicitantul certificatului nu este proprietarul domeniului ce se dorește a fi securizat).

Procedura de verificare la AÎ a identității persoanei juridice și a identității reprezentantului său autorizat constă în:

- * verificarea documentelor furnizate de utilizator,

- * verificarea cererii, care constă în:
 - i. verificarea conformității datelor menționate în cerere cu cele din documentele furnizate,
 - ii. (opțional) verificarea dovezii posesiei cheii private (dacă cererea implică o pereche de chei pentru crearea unei semnături electronice) și măsura în care Numele Distinctiv este cel potrivit,
- * verificarea autorizației și identității reprezentantului persoanei juridice care trimite cererea (inclusiv cereri de acreditare ca Autoritate de Certificare) în numele acestei entități,
- * verificarea în 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 autorizația de utilizare a domeniului solicitantului,
- * verificarea contului de mail care apare în cererea de certificat este controlat de către abonat. Cererea de certificat nu poate fi făcută/validată în aplicația software AÎ dacă abonatul nu își validează contul de email.

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

Dacă verificările sunt încheiate cu succes, un operator autorizat al Autorității 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 și trimite această confirmare la Autoritatea de Certificare,
- face copii tuturor documentelor și certificatelor folosite de operator pentru verificarea identității persoanei juridice și identitatea reprezentantului său care acționează în numele acesteia,
- în numele Autorității 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 Autorității de Certificare care verifică dacă aceasta a fost emisă de o Autoritate de Înregistrare autorizată.

Procesul de autentificare este înregistrat. Tipul informațiilor înregistrate și acțiunile depind de nivelul de încredere al certificatului ce face obiectul cererii și privesc:

- identitatea operatorului Autorității de Înregistrare care verifică identitatea solicitantului,
- trimiterea declarației operatorului (semnată de mână) prin care se atestă faptul că acesta a verificat identitatea solicitantului în concordanță cu cerințele prezentului Cod de Practici și Proceduri,
- data verificării,
- identificatorul operatorului și 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),
- declarația solicitantului (semnată de mână) cu privire la corectitudinea datelor incluse în cerere, în concordanță cu cerințele prezentului Cod de Practici și Proceduri,

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

3.1.7. Autentificarea identității persoanelor fizice

Autentificarea identității persoanelor fizice (entități private) are două scopuri. Autentificarea trebuie să dovedească

- 1) că datele dintr-o cerere se referă la o entitate privată existentă și
- 2) că solicitantul este într-adevăr entitatea privată menționată în cerere.

Autentificarea persoanelor fizice se realizează pe baza documentelor personale (carte de identitate sau pașaport) care confirmă identitatea solicitantului, și dacă utilizatorul dorește să includă datele unei instituții (persoană juridică) pentru care lucrează:

- a) autorizația scrisă, cu aprobarea explicită a companiei privind includerea datelor sale în certificatul persoanei fizice,
- b) extrasul valid de la Registrul Comerțului din România,
- c) alte documente.

Procedura pentru persoanele fizice realizată în fața Autorității de Înregistrare constă în:

- * verificarea documentelor furnizate de utilizator (carte de identitate sau pașaport în original sau copie legalizată), inclusiv bazele de date ale AC sau ale altor instituții,
- * verificare cererii înaintate:
 - verificarea consecvenței datelor din cerere cu cele din documente,
 - (opțional) verificarea dovezii posesiei unei chei private și a gradului de potrivire a ND-ului.
- * verificarea setului de informații din cerere folosind alte surse (Registrul Comerțului din România, Registrul de Evidență a Populației etc.),
- * verificarea faptului ca contul de mail care apare în cererea de certificat este controlat de către abonat. Cererea de certificat nu poate fi făcută/validată în aplicația software AÎ dacă abonatul nu își validează 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 și autorizațiile dispozitivului (în cazul în care acestea trebuie specificate în certificat),

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

Verificarea informațiilor care se înregistrează depinde de nivelul de încredere al certificatului. Sunt două metode de autentificare a originii unui dispozitiv și a integrității 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 concordanță cu cerințele stipulate în Capitolul 3.1.7.

3.2. Autentificarea identității la reînnoirea sau modificarea certificatului

Pentru a păstra continuitatea certificatului, înainte de expirarea sa, utilizatorul trebuie să solicite un nou certificat. Noul certificat poate conține aceeași cheie (reînnoire) dacă se respectă condiția ca durata de viață a cheilor să nu depășească o durată de două ori mai mare decât durata maximă de viață a unui certificat. În 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 și numai o singură dată.

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

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

3.2.1. Reînnoirea unui certificat

Un utilizator sau o Autoritate de Certificare folosește reînnoirea dacă deține deja un certificat și o cheie privată asociată acestuia și dorește să continue să folosească aceeași pereche de chei. Noul certificat, creat ca rezultat al înnoirii, constă într-o nouă pereche de chei, același nume și restul informațiilor care se preiau din certificatul anterior, dar perioada de valabilitate, numărul serial și semnatura emitentului sunt diferite față de datele din certificatul anterior.

Reînnoirea se aplică numai certificatelor a căror perioadă de validitate nu a expirat, nu au fost revocate și informațiile conținute de acestea sunt intacte.

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

3.2.2. Modificarea unui certificat

Modificarea certificatului se referă la crearea unui nou certificat pe baza certificatului deținut în prezent de utilizator. Un nou certificat are o cheie publică diferită, un nou număr serial, dar diferă prin cel puțin un câmp (prin conținut sau prin apariția unui câmp complet nou) față de certificatul pe baza căruia este emis.

Modificarea poate fi necesară, de exemplu, în cazul schimbării poziției în cadrul companiei sau al schimbării numelui, cu condiția ca aceste date să fi fost menționate inițial în certificat, sau dacă trebuie adăugate. Dacă datele, verificate pe baza unor documente în concordanță 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 și al căror nume al utilizatorului și alte caracteristici nu au fost schimbate.

3.3. Autentificarea identității la revocarea unui certificat

Cererile de revocare pot fi trimise prin e-mail direct emitentului certificatului sau indirect, Autorității de Înregistrare. Se pot trimite cereri și 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 identității utilizatorului. Cererea de revocare poate să vizeze mai multe certificate. Autentificarea și identificarea utilizatorului la Autoritatea de Înregistrare se realizează ca și la înregistrarea inițială (vezi Capitolul 3.1).

Autentificarea utilizatorului la Autoritatea de Certificare constă în verificarea autenticității 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 conțină informațiile 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 valabilității certificatelor.

Programul de lucru

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

Dacă cererea trimisă conține o cheie publică, cheia trebuie pregătită în așa fel încât să lege criptografic cheia publică cu alte date stipulate în cerere, în special cu datele de identificare ale utilizatorului. O cerere poate conține, în loc de o cheie publică, solicitarea utilizatorului final de a genera o cheie asimetrică în 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 comunicație 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 entități și pot viza certificate a căror aplicabilitate depinde de nevoile entității:

- * 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 și un certificat și, 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 reprezentanți sau angajați ai organizației care delegă acestora autorizarea respectivă,
- * certificate pentru dispozitive (care se aplică, de exemplu, serverelor) sau certificate ale aplicațiilor deținute de persoane fizice (angajați ai organizației sau reprezentanți ai lor) autorizate să folosească acest dispozitiv sau aplicație.

4.1.1. Cererea de înregistrare

O cerere de înregistrare este trimisă de către un utilizator final către Autoritatea de Înregistrare și conține cel puțin următoarele informații:

- i. numele complet al instituției sau numele și 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 identității utilizatorului final (vezi Capitolele 3.1.8 și 3.1.9) și după primirea confirmării Autorității de Înregistrare, cererea este trimisă unei Autorități de Certificare.

4.1.2. Cererea de reînnoire sau modificare certificat

O cerere de modificare sau reînnoire certificat, trebuie să conțină cel puțin:

- 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

Informațiile 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 parțiale sau complete incluse în cererea de mai sus trebuie autentificate prin semnatura electronica, dacă utilizatorul deține 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 Autorității de Înregistrare anunță utilizatorul final în legătură cu acest lucru.

4.2. Tratarea cererilor pentru furnizarea serviciilor de încredere

AlfaTrust Certification acceptă cereri înaintate individual sau colectiv. Cererile pot fi trimise on-line și 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 instrucțiunilor de pe site) un formular de cerere și 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 încredere (FSC), caz în care se completează și se semnează de mână cererea, se semnează contractul cu privire la prestarea serviciilor de încredere și se generează o parolă cu ajutorul căreia utilizatorul va putea face managementul certificatului sau se generează un cod PIN pentru accesul securizat la dispozitivul criptografic ce conține cheile și certificatele,
- * Prin trimiterea prin poștă a cererii și a copiilor documentelor (conform subcapitolelor 3.1.6 și 3.1.7) necesare verificării identității 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 conține cheile și 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 Autorității de Înregistrare și procesate în grup.

4.2.1. La Autoritatea de Înregistrare (AÎ)

Fiecare cerere scrisă pe hârtie este procesată după cum urmează:

1. operatorul Autorității de Înregistrare primește cererea solicitantului,
2. operatorul verifică datele din cerere, cum ar fi datele personale ale solicitantului (vezi subcapitolele 3.1.6 și 3.1.7) și verifică existența dovezii posesiei cheii private (vezi subcapitolul 3.1.5),
3. ca urmare a verificării, operatorul confirmă identitatea dintre datele declarate și cele cuprinse în cerere; dacă cererea conține date neconforme este respinsă,
4. cererea confirmată este trimisă la Autoritatea de Certificare,
5. Autoritatea de Înregistrare mai verifică și 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 și procesarea unei cereri (vezi capitolele 4.1 și 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 și de categoria utilizatorului final și 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 conține 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,
- * dacă procedurile sunt încheiate cu succes, serverul emite un certificat și însărcinează modulul hardware de securitate cu semnarea certificatului; certificatul este stocat în baza de date a Autorității de Certificare,
- * Autoritatea de Certificare pregătește răspunsul conținând certificatul emis (dacă a fost emis) și 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 folosește două metode de bază pentru anunțarea unui utilizator final despre emiterea unui certificat:

- prima metodă presupune folosirea poștei sau a poștei electronice și constă în trimiterea (la adresa furnizată de utilizator) a informațiilor ce permit utilizatorului să-și ridice certificatul. Această metodă este folosită și când este necesară anunțarea tuturor utilizatorilor finali ai unei anumite Autorități de Certificare despre emiterea unui nou certificat pentru autoritatea respectivă;
- A doua metodă constă în emiterea unui certificat și plasarea acestuia (de obicei împreună cu o cheie privată) pe un dispozitiv criptografic și trimiterea certificatului (prin poștă) 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 Entități 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 acuratețea datelor trimise în cerere și de modul de cooperare dintre AlfaTrust Certification și 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 dispoziția Autorității de Înregistrare în termen, sau este necesară o completare a documentației, termenul de emitere a certificatului va fi prelungit.

La eliberarea fiecărui certificat calificat se vor emite două copii de pe acesta, pe suport hârtie, dintre care un exemplar este pus la dispoziție titularului, iar celălalt este păstrat de către AlfaTrust Certification pe o perioadă de 10 ani.

4.2.4. Respingerea cererii de certificat

AlfaTrust Certification poate refuza în condiții bine precizate emiterea unui certificat oricărui solicitant fără a-și asuma vreo obligație 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 excepția cazului în care solicitantul a menționat date false în cererea sa.

Refuzul emiterii de certificat poate surveni în următoarele situații:

- * 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 și 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.

Informațiile privind decizia refuzului de emitere de certificat și 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 conținutul acestuia, în special corectitudinea datelor și complementaritatea cheii publice cu cea privată pe care o deține. Dacă certificatul are nereguli sau greșeli ce nu pot fi acceptate de utilizator, acesta din urmă va sesiza imediat Autoritatea de Înregistrare a Furnizorului de Servicii de Încredere, în vederea revocării certificatului.

Certificatul este considerat acceptat în ipoteza apariției 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) conținând 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 și este accesibil publicului. Acceptarea certificatului este o decizie unilaterală a solicitantului, anterior utilizării lui în efectuarea oricărei operații criptografice, prin care se consideră că a acceptat termenii și condițiile stipulate în prezentul Cod de Practici și Proceduri, Politica de Certificare și Contractul de prestări servicii de încredere. 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 și Proceduri și a Politicii de Certificare și subscrie să respecte prevederile contractul încheiat cu AlfaTrust Certification S.A.

4.2.6. Folosirea certificatelor și a cheilor

Abonații trebuie să folosească cheia privată și certificatele:

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

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

Entitățile Partenere, trebuie să folosească cheile publice și certificatele:

- în concordanță cu scopul lor declarat în prezentul Cod de Practici și Proceduri și în concordanță cu conținutul certificatului (câmpurile *keyUsage* și *extendedKeyUsage*),
- în concordanță cu prevederile contractului dintre entitatea parteneră și AlfaTrust Certification S.A.,
- numai după verificarea stării acestora și verificarea semnăturii Autorității de Certificare care a emis acel certificat.

4.3. Revocarea certificatelor

Revocarea unui certificat are o influență semnificativă asupra utilizării acestuia și asupra obligațiilor unui utilizator care deține un astfel de certificat. Imediat după revocarea certificatului unui utilizator final, certificatul trebuie considerat invalid (în stare de revocare). Similar, în cazul certificatului Autorității de Certificare – anularea validității unui certificat de acest tip semnifică retragerea drepturilor de emisie de certificate pentru proprietarul său și revocarea tuturor certificatelor emise de aceasta.

Revocarea nu afectează tranzacțiile făcute înainte de revocare și nici obligațiile care rezultă din respectarea prezentului Cod de Practici și Proceduri.

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

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

4.3.1. Circumstanțele revocării certificatului

Certificatul se revoca atunci când:

- * informația conținută de certificat s-a schimbat,
- * o cheie privată, asociată unei chei publice, conținută în certificat sau pe dispozitivul de stocare, a fost compromisă sau există un motiv serios pentru a suspecta ca a putut fi compromisă,
- * părțile 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 însuși nu cere revocarea, Autoritatea de Certificare sau un reprezentant al instituției la care este angajat utilizatorul, au dreptul să o facă,
- * Abonatul, deținătorul unei chei publice, cere revocarea,
- * poate fi revocat de emitent (Furnizorul de Servicii de încredere), dacă un utilizator nu respectă Politica de Certificare, Codul de Practici și Proceduri sau contractul, ori alte documente emise de Furnizorul de Servicii de încredere,
- * Furnizorul de Servicii de încredere își 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 Autorității de Certificare,
- * Utilizatorul întârzie sau nu plătește contravaloarea serviciilor prestate de către Furnizorul de Servicii de încredere,
- * cheia privată sau securitatea unei Autorități de Certificare a fost compromisă într-un mod în care pune în pericol credibilitatea certificatelor,
- * Abonatul, angajat al unei organizații, nu a returnat dispozitivul criptografic folosit pentru stocarea certificatului și a cheii private corespunzătoare, la încheierea contractului de muncă,
- * în alte cazuri în care utilizatorul final nu se conformează regulilor acestui Cod de Practici și 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 acces s-a petrecut,
- pierderea cheii private sau apariția unui motiv de a suspecta o astfel de pierdere,
- furtul cheii private sau apariția unui motiv de a suspecta un astfel de furt,
- ștergerea accidentală a cheii private.

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

Cererea de revocare trebuie să conțină informații care să permită autentificarea sigură a utilizatorului final de către Autoritatea de Înregistrare, în concordanță cu prevederile subcapitolelor 3.1.6 și 3.1.7. Dacă autentificarea identității utilizatorului final nu se realizează cu succes, Autoritatea de Înregistrare respinge cererea de revocare și suspendă certificatul până când cererea de revocare va fi examinată în detaliu.

4.3.2. Cine poate solicita revocarea

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

- * utilizatorul însuși, cu condiția să fie proprietarul certificatului,
- * Furnizorul de Servicii de Încredere,
- * un reprezentant al utilizatorului 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 informații 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 utilizatorului final despre revocare, sau despre inițierea procesului de revocare.

Fiecare cerere va fi trimisă trimisă:

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

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 inițiată numai la cererea utilizatorului final; această metodă se aplică în situațiile 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 utilizatorului final, cu condiția 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 ștampilă și o semnatura de mână a unei persoane recunoscute de AlfaTrust Certification; o cerere făcută prin telefon este îndeplinită numai după ce se trimit și documentele de autentificare a solicitantului; după verificarea cu succes a cererii, Autoritatea de Înregistrare pregătește confirmarea electronică a cererii de revocare și o înaintează Autorității de Certificare.

Informațiile 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 conțină motivele pentru care se cere revocarea și trebuie să fie autentificată.

Procedura de revocare a unui certificat se desfășoară 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 și corectitudinea certificatului atașat cererii; cererea făcută pe hârtie necesită autorizarea solicitantului; o astfel de confirmare poate fi obținută prin telefon, fax sau prin prezentarea în persoană a utilizatorului final la un reprezentant autorizat al Autorității de Înregistrare (sau invers);
- * dacă cererea este verificată cu succes, Autoritatea de Certificare plasează informațiile despre revocarea certificatului în Lista certificatelor Revocate (CRL), împreună cu informații privind motivele de revocare (vezi subcapitolul 6.2.1);
- * Autoritatea de Înregistrare notifică, electronic sau prin poștă, 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 privința revocării certificatului, sau inițierii 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 șters în condiții de maximă securitate. Această operație se îndeplinește de către posesorul dispozitivului criptografic – o persoană fizică sau juridică (un reprezentant al unei astfel de entități). Deținătorul dispozitivului criptografic trebuie să-l păstreze astfel încât să prevină furtul sau utilizarea neautorizată a sa până la distrugerea fizică sau la ștergerea cheii private.

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

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

În momentul revocării certificatului, operatorii Autorității de Înregistrare și utilizatorii implicați sunt informați automat despre această revocare. Informații despre starea curentă a certificatului sunt

disponibile prin serviciul de verificare a stării certificatelor imediat după perioada de grație declarată. Acest serviciu poate fi cerut, de exemplu, de către o Entitate Parteneră, care verifică validitatea unei semnături electronice aplicate unui document primit de la utilizatorul final.

4.3.4. Frecvența de emiteră 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 și se actualizează zilnic.

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

În cazul revocării certificatului unei autorități 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 corespunde cheii private a utilizatorului, folosită pentru crearea de semnături 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 frecvența perioadelor de emiteră a CRL-ului, declarată de AlfaTrust Certification, nu poate aduce daune serioase sau pierderi pentru Entitatea Parteneră. În alte cazuri, o Entitate Parteneră este obligată 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 securității cheii private,
- iii. **cACompromise** – compromiterea securității Autorității de Certificare,
- iv. **cessationOfOperation** – încetarea serviciilor asociate cheii private,

Decizia finală asupra credibilității 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 obțină date mai exacte (în comparație cu folosirea exclusivă a CRL-ului) despre starea unui certificat.

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

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

Serviciul OCSP este disponibil oricărui utilizator final și 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 informațiilor din baza de date a AlfaTrust Certification și conține informații mai noi decât cele din CRL-ul publicat.

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

4.3.7. Revocarea certificatului Autorității de Certificare (AC)

Certificatul aparținând unei Autorități de Certificare poate fi revocat de către autoritatea emitentă. O astfel de revocare poate să apară în următoarele situații:

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

4.4. Schimbarea cheii unei Autorități de Certificare (AC)

Procedurile de schimbare a cheii (*key changeover*) se aplică cheilor Autorităților de Certificare afiliate la AlfaTrust Certification și descriu modul în care se face schimbarea cheilor certificatelor autorităților, 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 deține vechiul certificat al autorității să-l obțină pe cel nou iar noilor utilizatori care au deja noul certificat al autorității să-l obțină pe cel vechi pentru verificarea datelor curente. Fiecare schimbare de cheie a Autorității de Certificare este anunțată în avans prin intermediul paginilor de web ale AlfaTrust Certification

și difuzată prin poșta electronică către fiecare utilizator al Autorității de Certificare a cărei cheie urmează a fi schimbate. În plus, în cazul schimbării cheii AlfaTrust Certification ROOT CA, informațiile despre acest eveniment vor fi publicate prin intermediul mass-media cu o luna înainte de momentul expirării perioadei de valabilitate a cheii private. Frecvența schimbării cheilor unei Autorități de Certificare afiliată la AlfaTrust Certification este dată de perioada de valabilitate a certificatului autorității.

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

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

Obligațiile prezentate mai jos sunt stabilite pentru a minimiza efectele negative asupra utilizatorilor finali și Entităților Partenere, ce pot apărea ca urmare a deciziei unui Furnizor de Servicii de Încredere de a-și înceta activitatea și se referă la obligațiile de a notifica în prealabil toți utilizatorii că își încetează activitatea și transferarea responsabilităților (servicii oferite utilizatorilor finali, baza de date, etc.), conform reglementărilor în vigoare, unui alt Furnizor de Servicii de Încredere.

4.5.1. Transferul responsabilității

Înainte ca un Prestatorul de servicii de încredere să-și înceteze activitatea, este obligat să:

1. anunțe Autoritatea de Certificare care a emis certificatul său despre intenția de a-și înceta activitatea ca Prestator de servicii de încredere; notificarea trebuie făcută cu 90 de zile înainte de data stabilită pentru încetarea efectivă a activității,
2. să anunțe (cu cel puțin 30 de zile înainte) utilizatorii săi care au certificate active (neexpirate și nerevocate) emise de autoritatea respectivă despre decizia de a-și înceta activitatea,
3. să revoce toate certificatele care rămân active (neexpirate și nerevocate) în momentul declarat al încetării activității, indiferent dacă utilizatorul a trimis sau nu o cerere în acest sens,
4. să anunțe toți utilizatorii Prestatorul de servicii de încredere despre încetarea activității,
5. să depună toate eforturile pentru a minimiza efectele negative asupra intereselor utilizatorilor și persoanelor juridice angajate în procese de verificare a semnăturilor electronice folosind certificate digitale emise de FSC-ul care își încheie activitatea,
6. să propună încheierea unui contract (de exemplu cu un alt Prestator de servicii de încredere) prin care să se garanteze protecția datelor,
7. să plătească compensații (care să nu depășească taxele de emisie și depozitare a certificatelor) utilizatorilor al căror certificat neexpirat și nerevocat va fi revocat înainte de data expirării.

4.5.2. Emiterea certificatelor de către succesori

Pentru a asigura continuitatea serviciilor de emisie de certificate pentru utilizatorii finali, Prestatorul de Servicii de Încredere care își 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 își încheie activitatea.

Prin emiterea unui certificat care să-l înlocuiască pe cel vechi, succesorul Prestator de Servicii de Încredere care își încetează activitatea preia drepturile și obligațiile acestei autorități în ceea ce privește 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 și structurilor de protecție a informațiilor care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice și de comunicații și al altor sisteme electronice, împotriva amenințărilor și a oricăror acțiuni care pot aduce atingere confidențialității, integrității, disponibilității, autenticității și non-repudierii informațiilor, precum și afectarea funcționării sistemelor informatice, indiferent dacă acestea apar accidental sau intenționat.

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

În sensul celor de mai sus definim și:

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

5.1. Controale ComSEC

5.1.1. Controale de securitate criptografică (cryptosecurity)

Acest capitolul descrie procedurile de generare și management a perechilor de chei criptografice a Prestatorului de Servicii de Încredere și a utilizatorul final, inclusiv cerințele tehnice asociate.

5.1.1.1. Generarea și folosirea perechii de chei

Procedurile de management a cheii se referă la păstrarea și folosirea în siguranță de către proprietar a cheilor sale. O atenție deosebită se acordă generării și protecției cheii private a AlfaTrust Certification ROOT CA, care influențează funcționarea în siguranță a întregului sistem de certificare a cheilor publice.

Autoritatea de Certificare AlfaTrust Certification ROOT CA deține cel puțin un certificat autosemnat. Cheia privată corespunzătoare cheii publice conținută de certificatul autosemnat este folosită exclusiv în scopul semnării cheilor publice ale Autorităților de Certificare direct subordonate (de pe nivelul 1 de certificare), prin semnarea certificatelor operaționale și a Listei de certificate Revocate, necesare pentru funcționarea autorităților respective.

Perechile de chei deținute de fiecare Autoritate de Certificare de pe nivelul 1 de certificare (SubCA-urile) permit semnarea de certificate și 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 combinație cu rezumatul criptografic SHA-1, SHA-256, SHA-384 sau SHA-512.

5.1.1.2. Generarea perechilor de chei

Cheile Autorităților de Certificare de pe nivelul 1 de certificare (SubCA-urile), precum și ale altor autorități subordonate acestora sunt generate în cadrul locației AlfaTrust Certification, în prezența unui grup de persoane de încredere (administratorul de securitate și administratorul Autorității de Certificare sunt membri ai acestui grup).

Perechile de chei pentru Autoritățile de Certificare care funcționează în cadrul AlfaTrust Certification sunt generate la anumite stații de lucru autentificate și conectate la module hardware de securitate (HSM), conforme cu cerințele FIPS 140-2 Nivel 3. Ele sunt menținute în permanență criptate pe aceste dispozitive.

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

Operatorii Autorității de Înregistrare dețin numai chei pentru autentificarea tuturor acțiunilor lor. Aceste chei sunt generate de operator (în prezența administratorilor de secrete) prin intermediul unei aplicații software autentificată, furnizată de Autoritatea de Certificare și conectată la un modul hardware de securitate conform cu cerințele FIPS 140-2 Nivel 2.

În general, fiecare utilizator final își generează singur perechea de chei. Pentru aceasta se va folosi de aplicația disponibilă pe site-ul web al AlfaTrust Certification, în momentul creării cererii. Aplicația permite crearea cheilor atât pe dispozitive securizate (tokenuri, smart carduri), cât și 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 Autorității de Înregistrare, să genereze o pereche de chei și să o trimită în siguranță utilizatorului final. În astfel de cazuri sunt folosite aplicații și dispozitive criptografice conforme cu FIPS 140-2 Nivel 2.

Procedurile de generare a cheilor inițiale ale Autorității de Certificare Primară

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

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

După generarea perechii de chei pentru semnarea de certificate și CRL-uri, activarea cheii private în modulul hardware de securitate, cheile pot fi folosite în operațiile 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 viață limitată; dacă această perioadă a expirat, cheile trebuie actualizate.

Actualizarea perechii de chei folosite pentru semnarea de certificate și 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 siguranță la utilizarea noului certificat; noii utilizatori care posedă deja noul certificat pot să obțină în siguranță certificatul expirat, care poate fi necesar la verificarea datelor semnate în trecut.

Pentru a obține 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 și invers (o cheie publică veche este autentificată cu o cheie privată nouă). Aceasta înseamnă că, drept rezultat al actualizării certificatului Autorității de Certificare, AlfaTrust CertificationS ROOT CA, în afară de certificatul nou, mai sunt create încă două certificate.

După actualizarea cheii, sunt create patru certificate pentru semnarea de certificate și 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 nouă) și
- 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 și CRL-uri, se desfășoară astfel:

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

După generarea și 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 toți utilizatorii obțin noul certificat (noua cheie publică) a AlfaTrust Certification ROOT CA (acesta trebuie obținută înaintea datei de expirare a vechiului certificat).

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

Perioada de validitate a certificatului *NewWithOld* începe din momentul generării noii perechi de chei și expiră în momentul în care toți utilizatorii finali vor obține 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 și expiră la cel puțin 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 și CRL-uri cu cel puțin 180 de zile înainte de data expirării certificatului corespunzător acestei chei private.

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

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

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

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

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

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

5.1.1.3. 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 și sunt livrate personal utilizatorului final, sau printr-o scrisoare poștală recomandată; datele pentru activarea cardului (codul PIN) sau pentru decriptarea cheii (parola) sunt trimise separat de mediul de stocare care conține perechile de chei; cardurile emise sunt personalizate și înregistrate de Prestatorul de Servicii de încredere.

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

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

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

Cererile trimise unei Autorități 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 Autorității de Înregistrare, de către Autoritatea de Certificare, care emite simultan un certificat pentru perechea de chei generată.

Cheile publice ale unei Autorități 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 Autorității de Certificare AlfaTrust Certification ROOT CA, certificatele sunt autosemnate.

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

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

În cazul schimbării (actualizării) cheii Autorității de Certificare AlfaTrust Certification-ROOT CA, depozitul va conține toate certificatele autosemnate sau certificatele emise ca urmare a execuției procedurii descrise în subcapitolul 5.1.1.1.1.

5.1.1.5. Dimensiunea cheilor

Dimensiunea cheilor folosite de Autoritățile de Certificare, operatorii Autorității de Înregistrare și utilizatorii finali sunt :

- * AlfaTrust Certification ROOT CA = 2048 biți/4096 biți;
- * AlfaTrust Certification SubCA-uri = 2048 biți/4096 biți;
- * Operatorii Autorității de Înregistrare = 1024 biți/2048 biți/4096 biți;
- * Persoane (fizice sau juridice) și dispozitivele hardware ale acestora = 1024 biți/2048 biți/4096 biți.

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

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

Acesta trebuie să verifice:

- posibilitatea de a efectua operații de criptare și decriptare, inclusiv creare de semnături electronice și 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 și DSA).

5.1.1.7. Generarea cheilor hardware și/sau software

Metodele permise pentru generarea de chei depind de Politica de Certificare aplicată și 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 Autorităților de Certificare, cheile sunt generate prin intermediul modulelor hardware de securitate care respectă prevederile prezentate în subcapitolul 5.1.1.2.1.

Cheile operatorilor Autorității 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 și software.

5.1.1.8. 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 aplicația utilizatorului final care face managementul certificatelor.

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

- a. **digitalSIGNature**: certificat pentru verificarea de semnături electronice,
- b. **nonRepudiation**: certificat pentru furnizarea de servicii de non-repudiare către persoane fizice, cât și pentru alte scopuri decât cele descrise la punctele f) și g). Bitul de non-repudiare poate fi setat numai într-un certificat de cheie publică cu care se intenționează verificarea semnăturilor electronice și nu trebuie combinat cu cele descrise la punctele c) - e) și în legătură cu asigurarea confidențialității,
- c. **keyEncipherment**: folosit pentru a cripta cheile pentru algoritmi simetrici, oferind confidențialitatea datelor,
- d. **dataEncipherment**: folosite pentru criptarea datelor utilizatorului, altele decât cele de la punctele c) și e),
- e. **keyAgreement**: folosit în protocoale de schimb de chei,
- f. **keycertSIGN**: cheia publică este folosită pentru verificarea semnăturii electronice în certificatele emise de entități care oferă servicii de încredere,
- g. **cRLSign**: cheia publică este folosită pentru verificarea semnăturilor electronice de pe listele de certificate revocate și suspendate emise de entitățile care oferă servicii de încredere,
- 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.

5.1.2. Protecția cheii private

Fiecare utilizator, operator al Prestatorului de Servicii de încredere și Autoritate de Certificare generează și 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 utilizatorului final, trebuie să o livreze acestuia în siguranță și să impună utilizatorului protejarea cheii sale private.

5.1.2.1. Standarde pentru modulele criptografice

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

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

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

- **în așteptare pentru activare (pregătită)** – cheia a fost deja generată, dar nu este utilizabilă (data curentă nu este încă aceeași cu data începerii perioadei de validitate a certificatului),
- **activă** – cheia poate fi folosită în operațiile criptografice (de exemplu pentru crearea de semnaturii electronice), data curentă este în cadrul perioadei de validitate a certificatului, cheia nu a fost revocată,
- **inactivă** – cheia aflată în această stare poate fi folosită numai pentru verificarea de semnaturii electronice sau pentru operații 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 informației); data curentă este în afara perioadei de validitate a certificatului.

5.1.2.2. Controlul dual al accesului cheii private

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

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

Pentru operațiuni de tipul: inițierea modulului criptografic hardware (HSM), transferul cheilor private ale Autorităților de Certificare, se implementează scheme prag de acces (de forma k din n) prin distribuire de secrete partajate. Numărul acceptat de secrete partajate și 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** și numărul necesar de secrete care permit restaurarea cheii private este **3**.

Procedura de transfer a secretului partajat implică prezența deținătorului de secret pe timpul procesului de generare a cheii și a distribuirii sale, acceptarea secretului dat și a responsabilităților care reies din păstrarea sa.

5.1.2.2.1. Acceptarea păstrării secretului de către deținători

Fiecare deținător de secret partajat, înainte de a primi partea sa de secret, trebuie să asiste personal la împărțirea secretului, să verifice corectitudinea secretului creat și distribuția sa.

Fiecare parte a secretului partajat trebuie transferată deținătorului pe un card criptografic protejat de un cod PIN, ales de deținător și știut numai de el. Primirea secretului partajat și crearea sa sunt confirmate printr-o semnătură de mână pe un formular, a cărui copie este păstrată în arhivele Autorității de Certificare și de către deținătorul de secret.

5.1.2.2.2. Protecția secretului partajat

Deținătorii secretului partajat trebuie să protejeze partea lor împotriva dezvăluirii. Deținătorul declară că:

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

5.1.2.2.3. Disponibilitatea și ștergerea (transferul) secretului partajat

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

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

5.1.2.2.1. Responsabilitățile deținătorului de secret partajat

Deținătorul de secret partajat trebuie să-și îndeplinească îndatoririle și obligațiile conform cerințelor acestui Cod de Practici și Proceduri, în mod responsabil în orice situație posibilă. Un deținător de secret partajat trebuie să anunțe emitentul secretului în cazul furtului, pierderii, dezvăluirii neautorizate sau compromiterii securității secretului, imediat după incident. Un deținător de secret partajat nu este responsabil pentru neîndeplinirea îndatoririlor/obligațiilor sale din cauza unor motive ce sunt imposibil de controlat de către acesta, dar este responsabil pentru dezvăluirea inoportună a secretului sau pentru neglijarea obligațiilor de a notifica emitentul secretului despre dezvăluirea inoportună sau violarea securității secretului ca urmare a greșelilor, neglijenței sau iredponsabilității deținătorului.

5.1.2.3. Back-up-ul cheilor private

Autoritățile de Certificare care operează în cadrul AlfaTrust Certification creează o copie de siguranță a cheii lor private. Copiile sunt folosite în cazul punerii în aplicare a procedurilor standard, sau de urgență (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 Autorității de Certificare. Copiile cheilor private ale utilizatorilor sunt create numai la cererea utilizatorului final și în conformitate cu Codul de Practici și Proceduri și Politicile de Certificare.

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

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

5.1.2.4. Arhivarea cheii private

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

5.1.2.5. Introducerea cheii private în modulul criptografic

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

- * când cheile sunt generate în afara modulului criptografic; această situație 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 operație similară de introducere a cheii într-un modul criptografic poate fi îndeplinită de un utilizator când cheile sunt livrate sub formă criptată și necesită stocare locală pe un dispozitiv criptografic,
- * în cazul creării copiilor de siguranță 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 operațional folosit pentru operații standard ale entității, pe un alt modul; situația poate apărea în cazul defectării modulului sau în cazul necesității distrugerii acestuia.

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

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

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

5.1.2.6. Metoda de activare a cheii private

Metodele de activare a cheii private, deținute de diverși 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 (și dezactivare) a unei chei private depinde de tipul entității care deține cheia respectivă (utilizator final, Autoritate de Înregistrare, Autoritate de Certificare, dispozitiv hardware etc.), de sensibilitatea datelor protejate de cheie și de intervalul de timp în care cheia trebuie să rămână activă (pe timpul unei singure operațiuni, sesiuni sau pentru o perioadă nelimitată).

Toate cheile private ale Autorităților 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 ștergerea 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 deținut de operator. După introducerea cardului în modulul criptografic și folosirea codului PIN, cheia privată rămâne în stare activă până la scoaterea cardului din modul.

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

Activarea cheii private a unui utilizator final se face în mod similar cu procedura de activare a cheii private a operatorilor Autorității de Certificare, indiferent dacă sunt stocate pe un card criptografic sau sub formă criptată, ca fișier pe o dischetă sau orice alt mediu de stocare. În cazul utilizatorilor finali persoane juridice (organizații, instituții etc.) activarea trebuie să se facă de către o persoană autorizată a utilizatorului.

5.1.2.7. 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 Autorității de Înregistrare, dezactivarea cheii private de semnatura se face imediat după încheierea sesiunii (la ieșire din aplicație). Dacă în timpul executării operației criptografice, cheia privată a fost stocată în memoria aplicației, aplicația trebuie să prevină refacerea neautorizată a cheii private. Dacă o cheie privată este deținută 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 ofițerul 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 activitățile sistemului. Dezactivarea unei chei private se face prin scoaterea cardului din modul.

5.1.2.8. Metoda de distrugere a cheii private

Ștergerea cheii private a unui utilizator sau operator al Autorității de Înregistrare presupune ștergerea ei de pe mediul de stocare (dischetă, card criptografic, memorie, modul hardware de securitate etc.). Dacă o

cheie privată aparține 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.

5.1.3. Alte aspecte cu privire la managementul perechilor de chei

Cerințelor din acest capitol se referă la procedurile de arhivare a cheii publice și la perioada de validitate a cheilor publice și private ale fiecărui utilizator, inclusiv ale Autorităților de Certificare.

5.1.3.1. Arhivarea cheilor publice

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

Arhivarea cheilor publice presupune arhivarea certificatelor care conțin aceste chei.

Fiecare autoritate care emite certificate arhivează cheile publice ale utilizatorilor către care au fost emise certificatele. Cheile publice ale Autorității 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 aplicațiile folosite (de exemplu, sistemele de poștă electronică).

Arhivele cheilor publice trebuie protejate în așa fel încât să se prevină adăugarea, inserarea, modificarea și ștergerea neautorizată de chei din arhivă. Protecția este realizată prin autentificarea entității care face arhivarea și autorizarea cererilor.

Administratorul de securitate verifică lunar integritatea arhivelor de chei publice. Scopul acestei verificări este de a asigura faptul că nu sunt goluri în arhive și că certificatele din arhive nu au fost modificate. Mecanismul de verificare a integrității arhivelor ține 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.

5.1.3.2. 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, și o perioadă de validitate a cheii private. Perioada maximă de utilizare a cheilor utilizatorilor nu poate depăși de 2 ori durata de viață a unui certificat. Valorile standard ale perioadei maxime de folosire a certificatelor Autorității de Certificare și a certificatelor utilizatorilor finali 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 și a cheilor private corespunzătoare poate fi mai scurtă în cazul revocării unui certificat.

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

5.1.4. 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 entităților și pentru a controla accesul la cheia privată.

5.1.4.1. Generarea și instalarea datelor de activare

Datele de activare sunt folosite în două situații principale:

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

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

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

Fraza de autentificare menționată mai sus trebuie generată în concordanță cu cerințele FIPS-112.

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

5.1.4.2. Protecția datelor de activare

Protecția 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 informațiilor 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 și 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 protecție trebuie să fie același cu cel al datelor pe care le protejează prin folosirea cardului criptografic. Mai multe încercări nereușite 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.

5.1.4.3. 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.

5.2. Măsuri de securitate fizică, procedurală, de personal și a documentelor

Acest capitol descrie cerințele generale privind securitatea fizică, procedurală și a documentelor, precum și activitatea personalului AlfaTrust Certification în activitatea de generare de chei, verificarea autenticității entităților, emiterea și publicarea certificatelor, revocarea certificatelor, audit și crearea de copii de siguranță.

5.2.1. Controale de securitate fizică

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

5.2.1.1. Accesul fizic

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

Sediul AlfaTrust Certification și Autoritatea de Înregistrare sunt accesibile publicului în fiecare zi lucrătoare între 10:00 și 16:00. În restul timpului (inclusiv în zilele nelucrătoare), accesul este permis numai persoanelor autorizate de către conducerea AlfaTrust Certification. Vizitatorii locațiilor aparținând AlfaTrust Certification trebuie să fie însoțiți 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 mișcare, efracție și incendiu. Accesul în această zonă este permis numai personalului autorizat, de exemplu, administratorul de securitate, administratorul Autorității de Certificare și administratorul de sistem. Monitorizarea drepturilor de acces se face folosind carduri și cititoare,

montate lângă punctul de acces. Fiecare intrare și ieșire 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 și administratorilor,
- zona de dezvoltare și testare,
- zona de depozitare a echipamentelor informatice, de comunicații sau criptografice.

Controlul accesului în zona operatorilor și administratorilor se face prin intermediul cardurilor și a cititoarelor de carduri. Deoarece toate informațiile sensitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor și 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 angajații AlfaTrust Certification și persoanele autorizate; ultimilor nu le este permisă prezența în zonă neînsoțiți.

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

- * **Zone administrative** – în această categorie intră orice alte zone din locația Prestatorului de Servicii de încredere 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.

5.2.1.2. Energie și climatizare

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

5.2.1.3. Expunerea la apă

AlfaTrust Certification și-a luat precauții deosebite pentru a minimiza impactul expunerii la apă a sistemelor AlfaTrust Certification.

5.2.1.4. Prevenirea și protecția împotriva incendiilor

AlfaTrust Certification și-a luat precauții deosebite pentru a preveni și a stinge focul sau alte expuneri la flacără sau fum. Măsurile AlfaTrust Certification de prevenire și protecție împotriva focului au fost stabilite pentru a respecta reglementările cu privire la prevenirea și stingerea incendiilor și siguranța la foc.

5.2.1.5. Mediile de stocare

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

5.2.1.6. Aruncarea lucrurilor nefolositoare

Documentele și materialele sensibile sunt distruse (tocate) înainte de a fi aruncate. Mijloacele folosite pentru a strânge sau a transmite informațiile 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 concordanță cu îndrumările anterioare ale producătorului. Alte lucruri nefolositoare sunt aruncate, ținând cont de cerințele AlfaTrust Certification.

5.2.1.7. Depozitarea backup-urilor în afara locației

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

Stocarea în afara locației se aplică și în cazul arhivelor, copiilor curente ale informațiilor procesate de sistem și kit-urilor de instalare ale aplicațiilor AlfaTrust Certification. Acest lucru permite refacerea de urgență a oricărei funcții a AlfaTrust Certification în 48 de ore, în locația principală a AlfaTrust Certification, sau în locația auxiliară.

5.2.2. Controale procedurale

Acest capitol prezintă rolurile ce pot fi atribuite personalului aparținând AlfaTrust Certification, Autorității de Înregistrare, utilizatorilor finali și entităților partenere. De asemenea, tot în acest capitol sunt descrise responsabilitățile și sarcinile specifice fiecărui rol.

5.2.2.1. Funcții de încredere

Printre persoanele de încredere se numără toți angajații, furnizorii și consultanții care au acces la sau controlează operațiile de autentificare și criptare și care pot influența:

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

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

- Personalul de la serviciu clienți,
- Personalul care se ocupa de operațiile criptografice ale activității,

- 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 și procedurilor de securitate. În plus poate aproba/revoca/suspenda certificate;
 - ✓ inițiază instalarea, configurarea și managementul aplicațiilor software și hardware (inclusiv resursele de rețea) ale AlfaTrust Certification;
 - ✓ inițiază și suspendă serviciile oferite de AlfaTrust Certification;
 - ✓ coordonează administratorii, inițiază și supraveghează generarea de chei și secrete partajate;
 - ✓ atribuie drepturi din punct de vedere al securității și privilegiilor de acces ale utilizatorilor;
 - ✓ creează conturile pentru utilizatorii AlfaTrust Certification;
 - ✓ atribuie parole pentru conturile utilizatorilor noi;
 - ✓ verifică jurnalele de evenimente;
 - ✓ supervizează auditurile interne și externe;
 - ✓ primește și răspunde la rapoartele de audit;
 - ✓ supervizează eliminarea deficiențelor constatate în urma auditului;
 - ✓ supraveghează operatorii Prestatorului de Servicii de încredere;
 - ✓ configurează sistemele și rețeaua, activează și configurează mecanismele de protecție a rețelei;
 - ✓ verifică log-urile de sistem;
 - ✓ verifică respectarea Politicii de Certificare și a Codului de Practici și Proceduri;
 - ✓ generează secrete partajate și chei;
 - ✓ administrează Lista de Certificate Revocate;
 - ✓ creează copiile de siguranță;
 - ✓ modifică numele și adresele serverelor.
- * **Administratorul de secrete** = își desfășoară activitatea la nivelul Autorităților de Certificare și Autorității de Validare;
 - ✓ supervizează și transferă secretele (cheile criptografice și alte date protejate) către operatorii Autorității de Înregistrare;
 - ✓ ia parte la activarea modulului criptografic și la încărcarea cheilor operatorilor (în prezența acestora);

- ✓ transferă și activează cardurile de identitate ale operatorilor (dacă aceste carduri sunt blocate);
- ✓ mediază contactele dintre Autoritatea de Înregistrare și Autoritățile de Certificare;
- * **Administratorul de sistem** = Autorizat să instaleze, configureze și să întrețină sistemele de încredere ale Furnizorului de Servicii de Certificare AlfaTrust Certification pentru înregistrarea, generarea de certificate, inițializarea dispozitivelor și gestiunea revocărilor de certificate;
 - ✓ Instalează dispozitivele hardware și sistemele de operare;
 - ✓ instalează și configurează echipamentele de rețea;
 - ✓ instalează programe;
 - ✓ configurează sistemul și aplicațiile;
 - ✓ activează și configurează resursele de securitate;
 - ✓ creează conturi și parole pentru operatori;
 - ✓ creează copii de siguranță și arhivează datele;
 - ✓ verifică jurnalele de evenimente (log-uri) și (împreună cu operatorul Autorității de Înregistrare), la ordinul administratorului de secrete, șterge datele în exces.
- * **Operatorul de sistem** = Responsabil de operarea zilnică a sistemelor de încredere ale Furnizorului de Servicii de Certificare AlfaTrust Certification;
 - ✓ autorizat să execute operațiile de backup și restaurare a sistemului;
 - ✓ are acces la certificatele utilizatorilor finali;
 - ✓ revocă certificatele utilizatorilor;
 - ✓ asigură continuitatea copiilor de siguranță și arhivelor bazelor de date și a creării log-urilor de sistem;
 - ✓ administrează bazele de date;
 - ✓ are acces la informații confidențiale despre utilizatori, dar nu poate accesa fizic nici o altă resursă a sistemului;
 - ✓ transferă copiile de siguranță ale arhivei și ale datelor curente în afara locației 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 și corectitudinea cererilor primite;
 - ✓ emit confirmări ale cererilor pe care le trimit Autorității de Certificare;
 - ✓ generează cheile și iau parte la generarea certificatelor, trimițând informațiile din cerere la o Autoritate de Certificare;
 - ✓ arhivează (sub formă de documente pe hârtie) cererile și confirmările emise, care fac obiectul ștergerii, la ordinul administratorului de secrete și în prezența acestuia,
- * **Auditorul de sistem** = autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale Prestatorului de servicii de încredere AlfaTrust Certification. Responsabil de efectuarea de

audituri interne pentru respectarea Codului de Practici și Proceduri și a Politicilor de Certificare de către Prestatorul de servicii de încredere; această responsabilitate se extinde și asupra Autorității 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 responsabilitățile auditorului.

- * **Administratorul depozitului** = își desfășoară activitatea la nivelul Autorității de Validare și administrează directoarele AlfaTrust Certification disponibile publicului, creează și actualizează conținutul directoarelor din depozit, creează paginile web și administrează legăturile (link-urile).

5.2.2.2. Numărul de persoane necesare pentru fiecare sarcină

Procesul de generare de chei – pentru semnarea certificatelor și al CRL-urilor – este una din operațiile ce necesită o atenție deosebită. Generarea necesită prezența a cel puțin două persoane: un administrator de securitate și un administrator de sistem. Procesul de generare a cheii Autorității de Certificare poate fi de asemenea observat de către posesori de secrete partajate care păstrează partea lor de cheie în locații sigure.

Prezența administratorului de securitate, a administratorului Autorității de Certificare și a unui număr corespunzător de posesori de secrete partajate este necesară și la încărcarea cheii criptografice a Autorității de Certificare în modulul hardware de securitate (HSM). Încărcarea cheii criptografice a Autorității de Înregistrare în modulul hardware de securitate (daca este cazul) necesită prezența administratorului de secrete și a unui operator al Autorității de Înregistrare.

Orice altă operațiune 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.

5.2.2.3. Identificarea și autentificarea pentru fiecare rol

Personalul AlfaTrust Certification este supus identificării și autentificării în următoarele situații:

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

Fiecare cont desemnat:

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

5.2.3. Controale de personal

AlfaTrust Certification garantează că se asigură că persoana care îndeplinește responsabilitățile funcției, conform cu rolul atribuit în cadrul unei Autorități de Certificare, Validare sau Înregistrare:

- ✓ a absolvit cel puțin liceul,
- ✓ este cetățean român,
- ✓ a semnat un contract care descrie rolul și responsabilitățile sale în cadrul sistemului,
- ✓ a beneficiat de un stagiu de pregătire avansată în conformitate cu obligațiile și sarcinile asociate funcției sale,
- ✓ a fost instruit cu privire la protecția datelor personale și informațiilor confidențiale sau private,
- ✓ a semnat un contract ce conține clauze referitoare la protejarea informațiilor sensitive (din punctul de vedere al securității AlfaTrust Certification) și a datelor confidențiale și private ale utilizatorilor finali,
- ✓ nu îndeplinește sarcini care pot genera conflicte de interese între Autoritatea de Certificare și Autoritatea de Înregistrare care acționează în numele acesteia.

5.2.3.1. Cerințe privind calificările și experiența

Personalul care dorește să se numere printre persoanele de încredere din AlfaTrust Certification trebuie să prezinte dovada îndeplinirii cerințelor referitoare la calificări și experiență, necesare pentru a îndeplini în mod competent și satisfăcător responsabilitățile postului respectiv. Verificarea informațiilor cu privire la personal se repetă la cel puțin 5 ani pentru personalul care ocupă poziții de încredere.

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

- * Confirmarea locului de muncă anterior;
- * Verificarea referințelor profesionale;
- * Confirmarea celei mai înalte sau relevante instituții de învățământ urmate;
- * Solicitarea cazierului judiciar;
- * Solicitarea rapoartelor financiare;
- * Solicitarea rapoartelor privind permisul de conducere;
- * Solicitarea rapoartelor privind asistența socială.

În măsură în care, oricare dintre cerințele impuse de această secțiune, nu poate fi satisfăcută din cauza unei interziceri sau limitări din legea locală sau din cauza altor circumstanțe, AlfaTrust Certification S.A. va folosi o tehnică de investigație care este permisă de lege și care furnizează informații asemănătoare, inclusiv, dar nu limitându-se la, obținerea unei verificări a trecutului, realizată de agenția guvernamentală adecvată.

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

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

Rapoartele care conțin astfel de informații sunt evaluate de personalul de la resurse umane și securitate, care determină cursul potrivit al acțiunii, în funcție de tipul, importanța și frecvența comportamentului dezvăluit de verificarea trecutului. Aceste acțiuni pot include măsuri care pot ajunge la anularea ofertelor de angajare pentru candidații la funcții de răspundere sau la scoaterea din funcție a persoanelor de încredere.

Folosirea informațiilor găsite prin verificarea trecutului pentru a întreprinde astfel de acțiuni este supusă reglementarilor în vigoare din România.

5.2.3.2. Cerințe de pregătire

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

Programele de pregătire ale AlfaTrust Certification S.A. sunt realizate ținând cont de responsabilitățile individuale și includ următoarele:

- ✓ Concepte de bază despre infrastructura cheii publice (PKI);
- ✓ Responsabilitățile funcției;
- ✓ Politicile și procedurile de securitate și operaționale ale AlfaTrust Certification S.A.;
- ✓ Folosirea și funcționarea hardware-ului și software-ului existent;
- ✓ Raportarea și tratarea cazurilor de incident și compromis;
- ✓ Procedurile de recuperare în caz de dezastru și de continuare a activității.

5.2.3.3. Cerințele și frecvența cursurilor de perfecționare

AlfaTrust Certification S.A. furnizează cursuri de perfecționare și de actualizare pentru personal, în măsura și cu frecvența care permit asigurarea menținerii nivelului necesar pentru îndeplinirea competentă și satisfăcătoare a responsabilităților de serviciu. Se asigură periodic pregătire de securitate.

5.2.3.4. Sancțiuni pentru acțiuni neautorizate

Se iau măsuri disciplinare adecvate pentru acțiunile neautorizate sau pentru alte violări ale politicilor și procedurilor AlfaTrust Certification S.A. Acțiunile disciplinare pot include măsuri care duc până la încetarea contractului și sunt luate în funcție de frecvența și severitatea acțiunilor.

5.2.3.5. Cerințe pentru contractarea personalului

În circumstanțe limitate, se pot folosi contractanți sau consultanți independenți pentru a ocupa funcții de încredere. Orice astfel de contractant sau consultant este menținut după aceleași criterii funcționale și de securitate care se aplică și în cazul angajaților AlfaTrust Certification, care se află într-o poziție asemănătoare.

Contractanții și consultanții independenți care nu au desăvârșit procedurile de verificare a trecutului specificate la punctul 5.1.2.3.1 pot accesa locațiile securizate ale AlfaTrust Certification numai dacă sunt escortați și supravegheați direct de persoane de încredere.

5.2.3.6. Documentație furnizată personalului

Personalul AlfaTrust Certification implicat în funcționarea serviciilor infrastructurii cheii publice ale AlfaTrust Certification trebuie să citească, să înțeleagă și să-și însușească acest cod de practici și proceduri și politica de securitate a AlfaTrust Certification. AlfaTrust Certification S.A. oferă angajaților săi pregătirea necesară și altă documentație necesară pentru a îndeplini competent și satisfăcător responsabilitățile funcției.

5.3. Controale CompuSEC

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

5.3.1. Cerințele de securitate specifice

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

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

- ✓ autentificarea obligatorie la nivelul sistemului de operare și al aplicațiilor,
- ✓ control discreționar al accesului,
- ✓ posibilitatea de a fi auditate din punct de vedere al securității,
- ✓ calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în AlfaTrust Certification ,
- ✓ separarea sarcinilor, conform rolului în cadrul sistemului,
- ✓ identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- ✓ prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,

- ✓ protecția criptografică a schimburilor de informații și protecția bazelor de date,
- ✓ arhivarea istoricului operațiunilor executate pe un calculator și a datelor necesare auditării,
- ✓ o cale sigură ce permite identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- ✓ metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicațiilor și a sistemului de operare,
- ✓ mijloace de monitorizare și alertare în cazul accesului neautorizat la resursele de calcul.

5.3.2. Evaluarea securității calculatoarelor

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

5.3.3. Controale pentru managementul securității informației

Scopul controalelor pentru managementului securității este acela de a superviza funcționalitatea sistemelor AlfaTrust Certification, garantând astfel că acestea operează corect și în concordanță cu configurarea acceptată și implementată.

Configurația curentă a sistemelor AlfaTrust Certification, precum și orice modificare și actualizare a acestora, este înregistrată și controlată.

Controalele aplicate sistemelor AlfaTrust Certification permit verificarea continuă a integrității aplicațiilor, versiunii și autentificarea și verificarea originii dispozitivelor hardware.

Fiecare aplicație, înainte de a fi folosită în producție de AlfaTrust Certification, este instalată astfel încât să se permită controlul versiunii curente și 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 așa fel încât să poată fi urmărită și 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 și de încredere.

5.3.4. Controale de securitate a rețelei

Serverele și stațiile de lucru de încredere aparținând AlfaTrust Certification sunt conectate prin intermediul unei rețele locale (LAN), divizate în mai multe subrețele, 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 și a filtrelor de trafic aplicate la nivelul ruterelor și serviciilor Proxy.

5.4. Înregistrarea evenimentelor și procedurile de auditare

Pentru a gestiona eficient sistemele AlfaTrust Certification și pentru a putea audita acțiunile utilizatorilor și personalului AlfaTrust Certification, toate evenimentele care apar în sistem sunt înregistrate. Informațiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente și trebuie păstrate în așa fel încât să permită Entităților Partenerere să acceseze informațiile corespunzătoare și necesare rezolvării disputelor, sau să detecteze tentativele de compromitere a securității 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 păstrată și dezvăluită atunci când se desfășoară un audit.

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

5.4.1. Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securității AlfaTrust Certification este înregistrată în logurile de evenimente și 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 conțin înregistrări ale tuturor activităților generate de componentele software din cadrul sistemului. Aceste înregistrări sunt împărțite în trei categorii separate:

- ✓ *înregistrări de sistem* – conțin informații despre cererile clienților și răspunsurile serverului (sau invers) la nivelul protocolului de rețea (de exemplu http, https); datele concrete care se înregistrează sunt: adresa IP a stației sau a server-ului, operațiunile executate (de exemplu: căutare, editare, scriere etc.) și rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- ✓ *erori* – conține informații despre erori la nivelul protocoalelor de rețea și la nivelul modulelor aplicațiilor,
- ✓ *audit* – conțin informații specifice serviciilor de încredere, de exemplu: cererea de înregistrare și de certificare, acceptarea certificatului, emiterea de certificat și CRL etc.

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

Fiecare înregistrare, automată sau manuală, conține următoarele informații:

- tipul evenimentului,
- identificatorul evenimentului,
- data și ora apariției evenimentului,
- identificatorul persoanei responsabile de eveniment.

Conținutul înregistrărilor se refera la:

- * alertele firewall-urilor și IDS/IPS-urilor,

- * operațiile asociate înregistrării, certificării, înnoirii, revocării, suspendării etc.,
- * modificări ale structurii hard sau soft,
- * modificări ale rețelei și conexiunilor,
- * înregistrările fizice în zonele securizate și violările de securitate,
- * schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,
- * accesul reușit și nereușit la baza de date AlfaTrust Certification și la aplicațiile serverului,
- * generarea de chei pentru AC, AÎ, AV etc.,
- * fiecare cerere primită și decizia emisă în format electronic schimbate între utilizator și AÎ/AC,
- * istoria creării copiilor de backup și a arhivelor cu înregistrări.

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

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

5.4.2. Frecvența analizei jurnalelor de evenimente

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

Procesul de verificare a jurnalului include verificarea unor eventuale falsificări, sau modificări și verificarea fiecărei alerte sau anomalii consemnate în log-uri. Orice acțiune executată ca rezultat al funcționării defectuoase detectate este înregistrată în jurnal.

5.4.3. Perioada de retenție a jurnalelor de evenimente

Înregistrările evenimentelor sunt stocate în fișiere 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 depășirea spațiului alocat, jurnalele sunt păstrate în arhive și pot fi accesate numai off-line, de la o anumită stație de lucru.

Jurnalele arhivate sunt păstrate cel puțin 2 ani.

5.4.4. Protecția jurnalelor de evenimente

Săptămânal, fiecare înregistrare din jurnale face obiectul arhivării pe bandă magnetică. După depășirea numărului acceptat de înregistrări pentru un jurnal, conținutul 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 așa fel încât:

- ✓ numai entitățile de mai sus au dreptul să citească înregistrările jurnalului,

- ✓ numai administratorul de securitate poate arhiva sau șterge fișiere (după arhivarea acestora) care conțin evenimentele înregistrate,
- ✓ este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conțin goluri sau falsuri,
- ✓ nici o entitate nu are dreptul să modifice conținutul unui jurnal.

În plus, procedurile de protecție a jurnalului sunt implementate în așa fel încât, chiar și după arhivarea jurnalului, este imposibil să ștergi înregistrări, sau să ștergi jurnalul înaintea expirării perioadei de retenție a jurnalului.

5.4.5. 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 locații auxiliare ale AlfaTrust Certification.

5.4.6. Notificarea entităților responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente și sesizează automat activitățile suspecte sau pe cele care au ca scop compromiterea securității. În cazul activităților care au influență asupra securității sistemului, sunt notificați automat administratorul de securitate și administratorul de sistem. În celelalte cazuri, notificarea este direcționată numai către administratorul de sistem. Transmiterea informațiilor către persoanele autorizate despre situațiile critice – din punctul de vedere al securității sistemului – se face prin alte mijloace de comunicare, protejate corespunzător, de exemplu, pager, telefon mobil, poșta electronică. Entitățile notificate iau măsurile corespunzătoare pentru a proteja sistemul față de amenințarea detectată.

5.4.7. Analiza vulnerabilităților

Autoritățile de Certificare, Autoritatea de Înregistrare și Autoritatea de Validare fac o analiză a vulnerabilităților pentru fiecare procedură internă, aplicație și sistem informatic. Cerințele de analiză pot, de asemenea, să fie stabilite de către o instituție 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, activitățile executate în cazul apariției unei amenințări și conformitatea cu Codul de Practici și Proceduri.

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

5.5. Arhivarea înregistrărilor

Este necesar ca toate datele și fișierele referitoare la informațiile despre securitatea sistemului, cererile trimise de utilizatori, informațiile despre utilizatori, certificatele emise și CRL-urile, cheile folosite de Autoritățile de Certificare și Înregistrare, și toată corespondența dintre AlfaTrust Certification și utilizatorii finali să fie arhivate.

Depozitul on-line conține certificatele active și poate fi folosit pentru efectuarea unor servicii externe ale Prestatorului de Servicii de Încredere, de exemplu verificarea validității unui certificat, publicarea certificatelor pentru proprietarii acestora (restaurarea certificatelor) și entitățile autorizate.

Arhivele off-line conțin certificate (inclusiv certificatele revocate) expirate cu până la 10 ani înainte de data curentă. Arhiva certificatelor revocate conține informații despre certificatul identificat, motivul revocării, dacă și 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 siguranță care sunt ținute în afara locației AlfaTrust Certification.

5.5.1. Tipurile de date arhivate

Următoarele date sunt incluse în procesul de arhivare:

- informațiile rezultate în urma examinării și evaluării (ca urmare a unui audit) măsurilor de protecție logice și fizice ale unei Autorități de Certificare, Autorității de Înregistrare și Autorități de Validare,
- cererile primite și deciziile emise, în formă electronică, trimise de, sau către un utilizator sub formă de fișiere sau mesaje electronice,
- baza de date cu utilizatorii finali,
- baza de date cu certificate,
- Listele de Certificate Revocate emise,
- istoria cheii Autorității 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 Autorității de Certificare.

5.5.2. Frecvența arhivării datelor

Arhivarea datelor se realizează pe mai multe nivele, astfel:

- * baza de date cu certificate și 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 șaptelea an (la șase ani după emiterea de certificatului) toate informațiile despre utilizatori și certificatele acestora sunt stocate pe CD-uri și sunt disponibile off-line,
- * CRL, corespondența electronică și cererile trimise de utilizatori precum și deciziile emise sunt arhivate în același mod și cu aceeași frecvență ca și bazele de date cu certificate și utilizatori,
- * cheile Autorităților de Certificare, Înregistrare și Validare sunt stocate – după expirarea certificatelor asociate – pe medii ce nu pot fi suprascrise și criptate cu cheia controlată de administratorul de securitate; cheile astfel arhivate sunt disponibile numai off-line.

5.5.3. Perioada de păstrare a arhivelor

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

5.5.4. Cerințele pentru marcarea temporală a înregistrărilor

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

5.5.5. Procedurile de acces și verificarea informațiilor arhivate

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

5.6. Procedura de backup și restaurare

Copiile de siguranță permit restaurarea completă (dacă este necesar, de exemplu, după distrugerea sistemului) a datelor esențiale pentru activitatea AlfaTrust Certification. Pentru a realiza acest lucru, sunt copiate următoarele aplicații și fișiere:

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

Metoda de creare a copiilor de backup are o influență deosebită asupra timpului și costului restaurării sistemelor Furnizorului de Servicii de Certificare după defectarea, sau distrugerea sistemului. AlfaTrust Certification folosește atât back-up-uri totale (săptămânale), cât și back-up-uri incrementale (zilnice), toate copiile sunt clonate și clonele sunt păstrate în altă locație, în aceleași condiții de securitate ca și cele din locația primară.

Procedura de restaurare va fi verificată cel puțin o dată la 3 luni, pentru a se verifica utilitatea back-up-ului, în caz de dezastru. Se verifică dacă datele salvate pe bandă sunt suficiente pentru restaurarea sistemului în cel mai scurt timp posibil. Concluziile testelor vor fi înregistrate.

5.7. Compromiterea securității cheii și recuperarea în caz de dezastru

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

5.7.1. **Compromiterea resurselor de calcul, a aplicațiilor software și/sau datelor**

Politica de securitate a AlfaTrust Certification ia în considerare următoarele amenințări ce pot influența disponibilitatea și continuitatea serviciilor oferite:

- distrugerea fizică a sistemului de calcul al AlfaTrust Certification, inclusiv a resurselor de rețea – această amenințare se referă la distrugerile provocate de situațiile de urgență,
- funcționarea defectuoasă a aplicațiilor, având ca efect imposibilitatea accesării datelor - aceste deteriorări se referă la sistemul de operare, aplicațiile utilizatorilor și executarea de aplicații periculoase, cum ar fi virușii, viermii, cii troieni,
- pierderea unor servicii de rețea importante pentru activitatea AlfaTrust Certification . Acestea se referă în primul rând la căderile de tensiune și distrugerea legăturilor de rețea,
- distrugerea unei părți din Intranetul folosit de AlfaTrust Certification pentru a furniza servicii – acest lucru poate duce la obstrucționarea clienților și refuzul (neintenționat) serviciilor.

Pentru a preveni sau limita efectele amenințărilor de mai sus:

- * Politica de securitate a AlfaTrust Certification include un Plan de continuitate a afacerii și recuperare în caz de dezastru,
- * În cazul apariției unui eveniment ce blochează funcționarea AlfaTrust Certification, în maxim 48 de ore, va fi activată locația auxiliară ce poate substitui toate funcțiile importante ale unei Autorității de Certificare până la restaurarea locației principale. Distanța dintre locația primară și cea secundară este suficientă pentru ca majoritatea potențialelor dezastruri care pot afecta locația primară să nu afecteze în același timp și locația secundară,
- * Instalarea de versiuni noi ale aplicațiilor software în producție 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 aplicații pentru crearea copiilor de backup pe baza cărora se poate face în orice moment restaurarea sistemului și auditarea acestuia. Copiile de siguranță includ toate datele relevante din punct de vedere al securității.

5.7.2. **Compromiterea sau suspiciunea compromiterii cheii private a unei Autorități de Certificare**

În cazul compromiterii cheii private a unei Autorități 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 și un nou certificat,
- ✓ toți utilizatorii de certificate sunt informați imediat despre compromiterea cheii private prin intermediul mass-media sau poștei electronice,
- ✓ 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 acționa în conformitate cu Planul de continuitate a afacerii și 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 și al Listei de Certificate Revocate (CRL) respectă formatul descris în standardul ITU-T X.509 v.3, în timp ce profilul OCSP respectă cerințele RFC 2560. Informațiile de mai jos descriu semnificația câmpurilor din certificat, CRL și OCSP, standardul aplicat și extensiile folosite de AlfaTrust Certification.

6.1. Profilul certificatelor

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

- corpul certificatului (***tbcertificate***),
- informații despre algoritmul folosit pentru semnarea certificatului (***signatureAlgorithm***),
- semnatura electronica propriu-zisă a Autorității de Certificare (***signatureValue***).

6.1.1. Conținutul certificatului

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

Extensiile definite într-un certificat conform normelor permit adăugarea de atribute suplimentare specifice utilizatorului final și cheii publice și 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.

3.1.1.1. 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 Autorității de Certificare,
- * **signatureAlgorithm:** identificatorul algoritmului de semnatura folosit de Autoritatea de Certificare emitentă, poate fi, după caz:
 - sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) sau
 - sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
- * **Issuer:** numele distinctiv (ND) al Autorității de Certificare,

- * **Validity:** perioada de validitate, descrisă prin intermediul unei date de începere (**notBefore**) și a unei date de expirare (**notAfter**) a certificatului, în baza sistemului universal de referință temporală (Universal Time Coordinated). AlfaTrust Certification posedă un ceas controlat de Atomic Frequency Standard,
- * **Subject:** numele distinctiv (ND) al utilizatorului final care este subiectul certificatului. Numele distinctiv respectă cerințele standardului X.501. Valorile unora dintre atributele acestor câmpuri sunt opționale,
- * **SubjectPublicKeyInfo:** valoarea cheii publice împreună cu identificatorul algoritmului criptografic folosit. Criptat în conformitate cu RFC 3280, poate conține informații despre cheile publice RSA, DSA sau ECDSA (identificatorul cheii, mărimea cheii în biți și valoarea cheii publice).

3.1.1.2. Extensiile standard ale certificatelor

Rolul fiecărei extensii este definit de valoarea standard a identificatorului de obiect folosit (Object Identifier - OID). Extensia, funcție de opțiunea autorității emitente, poate fi critică sau non-critică. Dacă o extensie este definită ca fiind critică, aplicația care folosește certificatul trebuie să respingă orice certificat care conține 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 Autorității 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 semnături electronice,
 - *nonRepudiation (1)* – cheie asociată cu serviciile de ne-repudiare,
 - *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,
 - *decipherOnly (8)* – cheie numai pentru decriptare.
- ✓ **ExtKeyUsage:** definește restricțiile cu privire la folosirea cheii (RFC 3280 și predecesorii) - extensia nu este critică. Acest câmp definește unul sau mai multe domenii de utilizare posibilă a certificatului, adițional domeniilor standard, definite de câmpul *KeyUsage*. Acest câmp trebuie înțeles ca o restrângere a scopurilor permise definite în câmpul *KeyUsage*. AlfaTrust Certification emite certificate care pot conține una dintre următoarele valori sau o combinație de astfel de valori în câmpul *ExtKeyUsage*:
 - *serverAuth* – autentificarea severelor web SSL/TLS; *KeyUsage* are setați biții pentru:

- *digitalSignature, keyEncipherment* sau *keyAgreement*;
- *clientAuth* – autentificarea clienților web SSL/TLS; *KeyUsage* are setați biții pentru:
 - *digitalSignature* și /sau *keyAgreement*;
- *codeSigning* – semnarea codurilor executabile; *KeyUsage* are setat bitul pentru
 - *digitalSignature*;
- *emailProtection* – protecția e-mail-ului; *keyUsage* are setați biții pentru:
 - *digitalSignature, nonRepudiation* și/sau (*keyEncipherment* sau *keyAgreement*),
- *ipsecEndSystem* – protocolul de autentificare și/sau criptare IPSec,
- *ipsecTunnel* – protocolul IPSec Tunnelling,
- *ipsecUser* – protocolul de protecție IPSec al aplicațiilor utilizatorului,
- *timeStamping* – legarea rezumatului (digest) cu timpul furnizat de sursa de încredere; *KeyUsage* are setați biții pentru:
 - *digitalSignature, nonRepudiation*.
- *ocspSigning* – asignează dreptul de a emite confirmări privind starea certificatului în numele AC-ului; *KeyUsage* are setați biții 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 setați biții pentru:
 - *digitalSignature, nonRepudiation, keyCertSign, cRLSign*.
- *EncryptedFileSystem* – permite folosirea certificatului pentru criptarea sistemului de fișiere (EFS); este cerut obligatoriu de anumite aplicații de acest gen (ex. EFS);
- *SmartCardLogon* – permite utilizarea certificatului pentru operația 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* – informații (identificatorul, adresa electronica) despre o politică de certificare aplicată. Această extensie nu este critică.

Certificate emise de către Autoritățile de Certificare AlfaTrust Certification includ și calificatori recomandați de RFC 3280:

- * **PolicyMapping**: map-area politicii – acest câmp nu este critic; acest câmp conține una sau mai multe perechi de OID, definind echivalența 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 și lungimea maxim admisă pentru lanțul de certificate – acest câmp este critic,
- * **CRLDistributionPoints**: punctul de distribuire a Listei Certificatelor Revocate – acest câmp nu este critic; extensia definește adresa din rețea la care se află CRL-ul curent al Autorității emitente a certificatului în cauză,

- * **AuthorityInfoAccessSyntax**: accesul la informațiile despre Autoritatea de Certificare – acest câmp nu este critic; câmpul indică metoda de informare și furnizare a serviciilor de către emitentul certificatului,
- * **OCSPNoCheck**: dacă este prezentă în cadrul unui certificat al unui responder OCSP, clienții 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 și este definită de standardul RFC 2560,
- * **NetscapeCertType**: această extensie limitează utilizarea certificatului numai la anumite aplicații specificate de valoarea extensiei. Dacă nu este prezentă, certificatul poate fi folosit pentru orice aplicație cu excepția aplicațiilor de *ObjectSigning*. Extensia este necritică, iar valoarea să poate fi o combinație 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 clienți de mail securizat S/MIME,
 - *ObjectSigning* (bit 3) - certificatul poate fi folosit pentru semnarea obiectelor cum ar fi appleturi 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,

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

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

6.1.2. Identificatorul algoritmului de semnare

Câmpul **signatureAlgorithm** conține identificatorul algoritmului criptografic folosit pentru semnarea electronica a certificatului de către Autoritatea de Certificare. În cazul AlfaTrust Certification este folosit algoritmul RSA, în combinație cu funcția hash SHA-1 sau SHA-256.

6.1.3. Câmpul ce conține semnătura electronică

Valoarea câmpului **signatureValue** este rezultatul aplicării funcției de hash asupra tuturor câmpurilor certificatului (*tbscertificate*) și a algoritmului de semnare a rezumatului obținut, folosind cheia privată a autorității.

6.2. Profilul listei de certificate revocate (CRL)

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

- primul câmp (**tbscertList**) conține informații despre certificatele revocate,

- al doilea (**signatureAlgorithm**) - informații despre identificatorul algoritmului folosit pentru semnarea listei,
- al treilea (**signatureValue**) conține semnatura electronică a Autorității de Certificare.

Câmpul *tbscertList* este o secvență de câmpuri obligatorii și opționale. Câmpurile obligatorii identifică emitentul CRL-ului în timp ce câmpurile opționale conțin informații despre certificatele revocate și extensiile CRL-ului.

Conținutul câmpurilor obligatorii și opționale dintr-un CRL sunt următoarele:

- ✓ **Version**: versiunea formatului de CRL,
- ✓ **Signature**: identificatorul algoritmului folosit de Autoritatea de Certificare pentru a semna CRL-ul; autoritățile AlfaTrust Certification semnează CRL-urile folosind algoritmul **sha1WithRSAEncryption** sau **sha256WithRSAEncryption**,
- ✓ **Issuer**: numele Autorității 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); informația constă din trei sub-câmpuri:
 - *usercertificates* – numărul serial al certificatului revocat,
 - *revocationDate* – data revocării certificatului,
 - *crlEntryExtensions* – conține informații suplimentare despre certificatele revocate - opțional.
- ✓ **crlExtensions**: informații suplimentare despre Lista de Certificate Revocate (câmp opțional). Dintre extensiile posibile, cele mai importante sunt următoarele:
 - *AuthorityKeyIdentifier* - care permite identificarea cheii publice corespunzătoare cheii private folosită pentru semnarea listei și
 - *cRLNumber*, care conține un număr serial incrementat monoton al listei emise de Autoritatea de Certificare (prin intermediul acestei extensii, utilizatorul are posibilitatea de a determina dacă a fost publicat un nou CRL).

6.2.1. Extensiile acceptate în intrările din CRL

Rolul și semnificația extensiilor este aceeași ca în cazul extensiilor de certificat. Extensiile dintr-o intrare CRL (*crlEntryExtensions*) acceptate de AlfaTrust Certification conțin următoarele câmpuri:

- * **ReasonCode**: codul motivului revocării certificatului. Acest câmp nu este critic și permite determinarea motivului revocării unui certificat. Sunt permise următoarele motive de revocare:
 - ✓ *unspecified* – nespecificat;
 - ✓ *keyCompromise* – compromiterea cheii;
 - ✓ *cACompromise* – compromiterea cheii Autorității 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 Autorităților de Certificare afiliate. Serverul OCSP, care emite confirmări ale stării certificatelor, folosește o pereche specială de chei, generată exclusiv pentru acest scop.

Certificatul serverului OCSP trebuie să conțină extensia *ExtKeyUsage*, descrisă în RFC 3280. Această extensie trebuie declarată ca fiind non-critică și 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 (aparținând utilizatorilor acestei autorități).

De asemenea, certificatul serverului OCSP conține extensia *OCSPNoCheck*, descrisă de RFC 2560. Această extensie trebuie declarată ca fiind non-critică și semnifică faptul că un client de OCSP care primește 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 primește 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).

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

Informațiile 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 și a fost revocat
- ✓ **UNKNOWN** – indică faptul că nu există suficiente informații pentru determinarea stării certificatului respectiv.

6.3.3. Extensiile standard acceptate

În concordanță 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 **OCSRequest** și repetat în câmpul *responseExtensions* al **OCSResponse**.

7. Managementul Codului de Practici și Proceduri

Fiecare versiune a Codului de Practici și Proceduri este în vigoare până în momentul aprobării și publicării noii sale versiuni. O nouă versiune este dezvoltată de către AlfaTrust Certification și publicată pentru comentarii cu mențiunea spre aprobare (dacă este cazul). După primirea și includerea comentariilor, Codul de Practici și Proceduri intră în procedura de aprobare internă. 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 întreținerea Codului de Practici și Proceduri este managerul departamentului care asigură furnizarea serviciilor de încredere. După terminarea procedurii de aprobare, noua versiune a CPP este transmisă Autorității de Reglementare și Supraveghere și apoi, în termen de 10 zile, este publicată și marcată ca fiind în starea validă. Regulile și cerințele descrise mai jos, cu privire la managementul Codului de Practici și Proceduri guvernează și managementul Politicii de Certificare.

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

7.1. Procedura de modificare a CPP

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

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

Modificările introduse pot fi în general împărțite în două categorii: una care nu necesită consultarea utilizatorilor și entităților partenere și una care cere (de obicei în avans) consultarea acestora. Prima categorie include modificări de urgență sau modificări neesențiale.

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

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

7.2. Publicarea CPP-ului

O copie a Codului de Practici și Proceduri este disponibilă în formă electronică 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 confidențiale de AlfaTrust Certification, nu se dezvăluie publicului. În această categorie intră și regulamentele interne, ce nu vor fi făcute publice.